Protéger la vie privée pour prévenir l'homicide conjugal

État des lieux des besoins en maisons d'hébergement de 2e étape et recommandations aux fournisseurs de services et d'outils numériques

Lise Chovino (CDÉACF), Anne-Sophie Letellier (Lab 2038), Amélie Tremblay (Lab 2038), Fanny Tan Therrien (Lab 2038), Hayfa Ben Miloud (Alliance MH2)

2023

CDEACF
Centre de documentation
sur l'éducation des adultes et la condition féminine

Lab 2038

Alliance MH2

Protéger la vie privée pour prévenir l'homicide conjugal

État des lieux des besoins en maisons d'hébergement de 2e étape et recommandations aux fournisseurs de services et outils numériques

Auteures :

Lise Chovino, CDÉACF
Anne-Sophie Letellier, Lab 2038
Amélie Tremblay, Lab 2038
Fanny Tan Therrien, Lab 2038
Hayfa Ben Miloud, Alliance MH2

Publié par :

Centre de documentation sur l'éducation des adultes et la condition féminine (CDÉACF)
469, rue Jean-Talon O, Bureau 229
Montréal QC H3N 1R4
Téléphone : 514 876-1180
Sans frais : 1 866 972-1180
Courriel : info@cdeacf.ca
Site internet : www.cdeacf.ca

Montréal, mars 2023

ISBN de la version électronique : 978-2-922995-63-3

Disponible sur internet : https://cdeacf.ca/proteger-vie-privee-victimes-pour-prevenir-lhomicide-1

CC BY-NC-SA 4.0

Éléments administratifs

Le présent rapport a été rédigé dans le cadre du projet ***Protéger la vie privée pour prévenir l'homicide conjugal***.

La reproduction du présent document, en tout ou en partie, est autorisée à la condition d'en mentionner la source et de ne pas l'utiliser à des fins commerciales. Pour plus d'informations, voir plus bas la méthode de citation suggérée.

Ce projet a été financé par le Commissariat à la protection de la vie privée du Canada (CPVP); les opinions exprimées ici sont celles de l'auteur et ne reflètent pas nécessairement celles du CPVP.

- **Vous avez besoin d'aide ou de ressources sur la violence conjugale?**

SOS Violence conjugale : sosviolenceconjugale.ca | 1 800 363-9010 (ligne d'aide ouverte 24h sur 24h tous les jours)

9-1-1 : ligne d'urgence

Interligne : interligne.co | 1 888 505-1010 (ligne d'écoute, clavardage et messages texte)

Alliance des maisons d'hébergement de 2e étape pour femmes victimes de violence conjugale : alliancemh2.org

Regroupement pour femmes et enfants victimes de violence conjugale : maisons-femmes.qc.ca

Fédération des maisons d'hébergement pour femmes : fmhf.ca

Femmes Autochtones du Québec : faq-qnw.org

- **Présentation des organismes partenaires**

Le partenariat

Depuis 2017, le CDÉACF, les membres du Lab 2038 et l'Alliance des maisons de 2e étape, notamment, ont mis en place un partenariat pour adresser les impacts du numérique dans le continuum de la violence conjugale et développer des outils de sensibilisation et des formations permettant aux intervenantes d'acquérir des connaissances de base des outils numériques qu'utilisent les résidentes. Ces outils ont été largement diffusés dans l'ensemble des réseaux de maisons d'hébergement d'urgence.

Le comité exécutif

Le projet a été mené par un comité exécutif composé de 3 organismes.

Le **Centre de documentation sur l'éducation des adultes et la condition féminine (CDÉACF)** œuvre depuis près de 40 ans auprès des groupes d'alphabétisation et de femmes de la francophonie canadienne. Reconnu comme un organisme de formation par le ministère de l'Éducation, il fournit aux groupes du matériel, de la formation et de l'accompagnement sur différents thèmes (compétences parentales, alpha-francisation, connaissance de soi, budget, intégration socioprofessionnelle, santé et bien-être, sécurité et confidentialité numériques, compétences TIC, éthique numérique, etc.). Le CDÉACF réalise sa mission dans une perspective de transformation sociale basée sur des valeurs de justice sociale, d'éthique numérique et de démocratisation des connaissances.

L'**Alliance des maisons de 2e étape pour femmes et enfants victimes de violence conjugale** compte 34 maisons membres qui offrent un hébergement sécuritaire et des services psychosociaux spécialisés en violence conjugale post séparation. Les résidentes sont admises au sortir des maisons d'urgence (MH1) sur le critère de dangerosité du conjoint, ce qui représente 8% des femmes hébergées en première étape. La durée moyenne de séjour de 8,5 mois permet une connaissance intime des enjeux numériques de nos résidentes concernant l'impact direct et immédiat de ces outils technologiques sur leur sécurité. De plus l'Alliance co-préside **Hébergement Femmes Canada**, qui regroupe 520 maisons d'hébergement canadiennes, et y anime le Comité de travail sur les MH2.

Le **Lab 2038** : Le Lab-2038 est un organisme à but non lucratif qui a pour mission de défendre et promouvoir les droits, les libertés et la justice

sociale dans l'espace numérique. Ses membres travaillent, de par leur expertise en recherche, en sécurité de l'information et en informatique, à rendre les technologies et leurs usages plus sécuritaires, équitables et respectueux de la vie privée de tous les citoyen-nes.

- **Remerciements**

Le comité exécutif tient à remercier les membres du comité de pilotage, soit :

- le **Professeur Normand Landry, professeur à la TELUQ directeur de la Chaire de recherche en éducation aux médias et droits humains**,
- **Alexandre Plourde** de l'organisme Option-Consommateur,

ainsi que **toutes les travailleuses de maisons d'hébergement de 2e étape, les résidentes des maisons d'hébergement de 2e étape** et **les fournisseurs de services** qui ont contribué à ce travail.

- **Questions et corrections**

Pour toute question concernant le présent rapport ou concernant le projet, veuillez contacter Lise Chovino à chovino@cdeacf.ca.

- **Citation suggérée**

Veuillez citer ce rapport en utilisant la notice bibliographique suivante, créée d'après la norme APA :

Chovino, L., Ben Miloud, H., Letellier, A.-S., Tremblay, A., & Tan Therrien, F. (2023). *Protéger la vie privée pour prévenir l'homicide conjugal : État des lieux des besoins en maisons d'hébergement de 2e étape et recommandations aux fournisseurs de services numériques*. Centre de documentation sur l'éducation des adultes et la condition féminine. Consulté le …, à l'adresse https://cdeacf.ca/proteger-vie-privee-victimes-pour-prevenir-lhomicide-1

Table des matières

Éléments administratifs **2**

Liste des acronymes **6**

Introduction **7**

1. Contexte et revue de la littérature **8**

1.1 Synthèse de la revue de littérature 8

1.2 De quoi traite la littérature? 9

1.3 De quelle manière le sujet est-il traité? 10

2. Quels risques et inquiétudes en matière de confidentialité pour les victimes de violence conjugale? **12**

2.1 Méthodologie 12

2.2 Discussion 16

2.3 Conclusion partielle 18

3. Les applications numériques **20**

3.1 Méthodologie 20

3.2 Analyse des résultats 27

3.3 Discussion & conclusion partielle 31

4. Services numériques **33**

4.1 Méthodologie 34

4.2 Analyse des résultats 36

4.3 Discussion et conclusion partielle 40

5. Recommandations **42**

5.1 Découvertes majeures 42

5.2 Recommandations à l'attention des fournisseurs de services et outils numériques 43

6. Conclusion **45**

7. Bibliographie **47**

Annexe 1: Grille d'analyse - analyse de politiques de confidentialité **54**

Annexe 2: Grille d'entretien **56**

Annexe 3: Sondage **58**

Annexe 4: Questionnaire de focus groupe **66**

Liste des acronymes

Alliance MH2 : Alliance des maisons de 2e étape pour femmes victimes de violence conjugale

CDÉACF : Centre de documentation sur l'éducation des adultes et la condition féminine

CPVP : Commissariat à protection de la vie privée

IoT : Internet of Things (traduction : internet des objets)

2FA : double facteur d'authentification

Introduction

Comme le note l'Alliance des maisons d'hébergement de 2e étape pour femmes et enfants victimes de violence conjugale, le risque d'homicide s'élève à 80% pour les femmes victimes de violence conjugale au moment de la séparation. Dans ce contexte, il est donc essentiel de réfléchir à l'impact de la divulgation directe ou indirecte d'informations d'identification qui pourrait survenir par le biais de fournisseurs de services et d'outils numériques.

Les intervenantes en maison d'hébergement assurent déjà un rôle essentiel dans la mise en sécurité physique et psychosociale des femmes hébergées. De même, elles se forment continuellement pour faire face aux menaces émergentes reliées aux outils numériques et aux objets connectés (IoT).

Cependant, elles ne peuvent à elles seules assurer pleinement la sécurité numérique – en plus de la sécurité physique et psychosociale – des résidentes dans une réalité de plus en plus connectée. De plus, en maison de 2e étape, les femmes hébergées gèrent leur quotidien de manière autonome. Il est donc important pour les intervenantes de pouvoir leur fournir un cadre d'épanouissement le plus sécurisé possible à travers des démarches d'autonomisation et de dévictimisation.

Le projet ***Protéger la vie privée pour prévenir l'homicide conjugal***, mené par le CDÉACF, l'Alliance MH2 et le Lab 2038, vise donc à comprendre et documenter la place que doivent occuper la sécurité numérique et la protection des renseignements personnels en ligne dans l'évaluation du filet de sécurité des femmes hébergées dans les maisons de 2e étape.

Ce travail permet d'évaluer les failles de sécurité provenant des pratiques des fournisseurs de services et d'outils numériques, de sonder le sentiment de sécurité des femmes hébergées ayant accès à ces services, et de mieux protéger ces femmes des impacts de la collecte de données.

Ce rapport de recherche présente les résultats d'une analyse croisée de données qui a permis, d'une part, de réaliser un état des lieux actuel des besoins et enjeux des maisons d'hébergement de 2e étape en matière de confidentialité numérique, d'autre part, de dégager des recommandations à destination des fournisseurs de services numériques.

1. Contexte et revue de la littérature

1.1 Synthèse de la revue de littérature

Afin d'identifier les ouvrages pertinents à notre sujet d'étude, nous avons procédé à une recherche par mots-clés dans Google Scholar et dans la base de données universitaire Sofia, qui regroupe les références d'un très grand nombre de revues savantes et révisées par les pairs. Nous y avons cherché des références en français et en anglais qui mobilisent des thématiques liées, d'une part, au champ lexical de la violence conjugale (*domestic abuse*, *domestic violence*, *abusive relationship*, *intimate partner violence/IPV*) et, d'autre part, au champ lexical de la surveillance et de la collecte de données (données électroniques, surveillance électronique, collecte de données, capitalisme de surveillance, données numériques, Internet des objets, *data collection*, digital data, *Internet service providers*, *digital devices*, *digital surveillance*, *surveillance capitalism*, etc.). La recherche opérée n'a donc pas été exhaustive, mais visait à identifier les ouvrages clés portant sur la thématique présentée en phase initiale.

La revue de littérature compile une centaine de références issues du milieu académique (incluant des études provenant majoritairement des disciplines de la sociologie et de la criminologie, lesquelles sont parfois menées de manière conjointe avec des expert-es en sciences informatiques), de la sphère journalistique et du milieu communautaire. Les références anglophones se concentrent principalement sur les contextes états-unien (Chatterjee et al., 2018; Citron, 2015; Grimani et al., 2022; Marganski et Melander, 2018), australien (Douglas et al., 2019; Harris et Woodlock, 2021; Lopes Gomes Pinto Ferreira, 2021; Louie, 2021b), canadien (Bailey et Shayan, 2016; Marques, 2021) et anglais (Barker et Jurasz, 2021; Millman et al., 2017; Tanczer et al., 2021), tandis que la France et le Québec sont représentés dans les sources francophones (Bernier, 2016; Kabassema, 2020; Laguë Maltais, 2021). Les articles se penchant sur les enjeux légaux liés au sujet d'étude rassemblent principalement des cas provenant des États-Unis (Fukuchi, 2011; Hosani et al., 2019) et du Canada (Aikenhead, 2021; Dunn, 2021 ; Dunn et Aikenhead, 2022; Hosani et al., 2019; Thomasen et Dunn, 2021).

1.2 De quoi traite la littérature?

Un premier constat général à retenir : aucune référence repérée abordant les enjeux technologiques de la perpétration de la violence conjugale ne le fait sous l'angle de la collecte des données. Les sources se rapprochant le plus de ce point d'analyse portent sur les enjeux légaux entourant l'impact de cette collecte sur le cyberharcèlement (Fukuchi, 2011; Hosani et al., 2019; Millman et al., 2017). Elles se concentrent toutefois sur le cas des États-Unis et n'abordent pas la question dans un contexte de violence conjugale. Il est à noter que la revue n'ayant pas été systématique, il se peut que certains mots-clés qui auraient permis de trouver des références traitant du lien entre la violence conjugale et la collecte de données n'aient pas été identifiés.

Dans un second temps, il est possible de relever un consensus sur le fait que les technologies offrent de nouveaux moyens de contrôle et de surveillance (Afrouz, 2021; Aghtaie et al., 2018; Bernier, 2016; Citron, 2015; Fraser et al., 2010; Freed et al., 2019; Marganski et Melander, 2021), ce qui donne lieu à de nouvelles formes de violence en plus d'en exacerber d'autres qui étaient déjà présentes (Al-Alosi, 2017; Al-Nasrawi, 2021; Anderson et Wood, 2021; Araújo et al., 2022; Bailey et Shayan, 2016; Cama, 2021; Douglas et al., 2019; Freed et al., 2018; Leitão, 2021; Marques, 2021; Obada-Obieh et al., 2022; Roundy et al., 2020; Salerno-Ferraro et al., 2021). À ce propos, plusieurs formes de violence sont abordées, incluant notamment celles menées via les objets connectés (Internet des objets) (Bowles, 2018 ; Leitão, 2018 ; Lo, 2021; PenzeyMoog et Slakoff, 2021 ; Slupska et Tanczer, 2021 ; Tanczer et al., 2021), la géolocalisation (Chatterjee et al., 2018; Dumont, 2019; PenzeyMoog et Slakoff, 2021), le piratage des mots de passe (Perry, 2012; Tseng et al., 2020) ou l'utilisation d'applications bancaires pour effectuer du contrôle financier (PenzeyMoog et Slakoff, 2021 ; Perry, 2012). Du côté du milieu académique, il s'observe plutôt une surreprésentation des études portant sur l'utilisation de logiciels et d'applications de surveillance (*stalkerware*, *spyware*, *spouseware*) par les agresseurs (Baddam, 2017; Beagle, 2011; Chatterjee et al., 2018; Citron, 2015; Douglas et Burdon, 2018; Freed et al., 2018; Hand et al., 2009; Kabassema, 2020; Roundy et al., 2020).

Dans un autre ordre d'idées, les pratiques des fournisseurs de services et de produits technologiques sont moins étudiées (Kabassema, 2020; Obada-Obieh et al., 2022 ; Tanczer et al., 2021). Une bonne partie des sources compilées offre plutôt des descriptions des manières dont les technologies sont utilisées par les agresseurs pour procéder à des actes de surveillance sur leur victime (Lee et Anderson, 2016; Louie, 2021a;

Slupska et Tanczer, 2021). Lorsqu'il est question des fournisseurs, c'est presque toujours dans un contexte de considérations légales (majoritairement hors Canada) quant aux acteurs qui détiennent une responsabilité dans la gestion des situations de violence en ligne (Cheung, 2021; Coombs, 2021; Dragiewicz et al., 2018). Rien n'a été repéré sur les prises de position de ces fournisseurs quant au rôle de leurs pratiques dans la perpétration de la violence conjugale ni quant aux moyens qu'ils mettent en place pour la contrer. D'ailleurs, une part importante des références retenues aborde les enjeux technologiques de la violence conjugale du point de vue légal (Aikenhead, 2021; Citron, 2015; Douglas et Burdon, 2018; Fetters, 2018; Fraser et al., 2010 ; Lee et Anderson, 2016; Lo, 2021).

1.3 De quelle manière le sujet est-il traité?

D'abord, la plupart des sources retenues abordent le sujet à l'étude du point de vue des victimes de violence conjugale (Dimond et al., 2011; Douglas et al., 2019; Freed et al., 2017; Harris et Woodlock, 2021; Havron et al., 2019; Laguë Maltais, 2021; Leitão, 2021; Louie, 2021a).

Ensuite, il est à noter qu'une grande partie de la littérature, autant celle provenant de la sphère académique (Freed et al., 2019; Southworth et al., 2005) que communautaire (BC Society of Transition Houses, 2019; Centre Hubertine Auclert, s.d.; Chayn, s.d.; Coalition Against Stalkerware, s.d.; Perry, 2012; HACK*BLOSSOM, s.d.; Safety Net Project, s.d.) et journalistique (Cericola et Wells, 2018 ; Dumont, 2019), consiste au partage de solutions concrètes que peuvent appliquer les victimes pour lutter contre les formes de violence en ligne auxquelles elles peuvent faire face. Si cela peut leur être très utile, l'absence quasi totale de critique formulée envers les organisations qui collectent, utilisent et communiquent des renseignements personnels dans le cadre d'activités commerciales (Henry et Witt, 2021; Slupska et Tanczer, 2021) a pour effet d'imputer aux victimes la responsabilité de se défendre contre ces formes de violence.

En ce sens, les objectifs énoncés dans ce projet de recherche visent à combler un vide dans les recherches, notamment académiques, en documentant le rôle des pratiques technologiques des entreprises en matière de protection des données privées. Cela se pose en complément nécessaire aux écrits publiés sur les enjeux d'ordre juridique ainsi que les pratiques de sensibilisation et d'éducation. Les objectifs du projet ont finalement une utilité sociale dans leur visée de documenter et d'attirer l'attention sur les responsabilités qui peuvent incomber aux acteurs qui ne vivent pas cette violence.

En conclusion, la revue de littérature opérée permet de soulever deux constats principaux.

1. Une recherche plus approfondie pourrait être conduite pour cerner avec plus de précision l'étendue des connaissances sur le sujet. Néanmoins, la tendance actuelle nous apparaît claire : la thématique sur laquelle se concentre le présent projet n'est que très marginalement documentée, particulièrement dans le contexte canadien.
2. La littérature nous laisse peu de pistes pour identifier les cas d'études qui devront être opérés dans les prochaines étapes de la recherche. Le groupe focus et le sondage risquent conséquemment d'être des piliers stratégiques pour identifier des cas porteurs, pertinents et riches afin de répondre aux objectifs de la recherche.

2. Quels risques et inquiétudes en matière de confidentialité pour les victimes de violence conjugale?

Dans le cadre du projet, il a été nécessaire de réaliser un état des lieux actuel du sentiment de sécurité ou d'insécurité vécu dans les maisons d'hébergement de 2e étape par rapport aux enjeux de protection des données personnelles confiées à des fournisseurs de services et d'outils numériques. Cet état des lieux a été réalisé en croisant les données recueillies lors de la diffusion d'un sondage et lors de l'animation de sessions d'un groupe focus. Les questionnaires de ces deux activités sont disponibles en annexe de ce rapport.

2.1 Méthodologie

Confidentialité des participantes

Pour assurer la confidentialité des contributrices ayant participé aux activités de recueil des besoins, le présent état des lieux a été rédigé à partir des faits saillants de la compilation des réponses des participantes.

Fournisseurs de services numériques

L'appellation « fournisseurs de services numériques » a été utilisée dans le sondage et le groupe focus pour simplifier le texte en regroupant plusieurs types d'entreprises ou d'organismes offrant des services au public médiés par les technologies numériques et connectées à internet:

- les entreprises qui offrent des services à distance (livraison de repas ou d'épicerie, taxis, etc.),
- les entreprises qui fournissent des logiciels et des plateformes en ligne (logiciels et suites informatiques, comptes connectés, appareils connectés, etc.),

- les sociétés qui font du soutien technique ou informatique.

Méthodes de recueil des besoins

Les besoins des intervenantes et résidentes ont été recueillis de 2 manières :

- grâce à un sondage en ligne envoyé aux intervenantes
- grâce à un groupe focus.

1. **Le sondage**

Dans un premier temps, nous avons réalisé un sondage. Ce sondage a été diffusé sous la forme d'un formulaire disponible en ligne du 26 septembre au 11 octobre 2022. La plateforme utilisée est Framaforms, un outil libre et gratuit développé par Framasoft (**framaforms.org**).

Ce formulaire a été élaboré par le comité exécutif avec l'appui du comité de pilotage, puis diffusé aux maisons d'hébergement par l'Alliance MH2. Les résultats ont été reçus par le CDÉACF via la plateforme Framaforms. Le CDÉACF s'est chargé de compiler les résultats afin d'en faire parvenir une version anonymisée aux comités exécutif et de pilotage, puis de fournir les informations d'identification à l'Alliance MH2 pour ses suivis administratifs.

De plus, le questionnaire a été structuré de manière à obtenir des éléments d'information aussi bien sur la réalité des intervenantes que sur les enjeux rencontrés par les femmes hébergées dans les maisons de 2e étape. Le choix a été laissé libre aux intervenantes d'utiliser l'approche appropriée pour répondre aux questions concernant les résidentes.

Ce questionnaire de sondage a été envoyé dans les 17 maisons d'hébergement de 2e étape qui sont actuellement actives et nous avons obtenu 15 réponses, ce qui dépasse l'objectif annoncé de 80% de taux de réponses.

2. **Le groupe focus**

Une fois les résultats du sondage reçus, nous avons élaboré un questionnaire pour le groupe focus. En effet, cette activité a été pensée comme une manière de bonifier les réponses au sondage à deux niveaux:

- en approfondissant des questions déjà posées afin que les intervenantes puissent étoffer leurs réponses, ces questions sont précédées d'une référence entre crochets au sondage, exemple : **[question 7]**,
- en complétant les questions du sondage par de nouvelles questions qui permettent de pousser la réflexion.

Le groupe focus répondait aussi au besoin de donner un espace pour parler plus largement de la thématique de la confidentialité des données, car répondre au sondage a parfois causé des interrogations et un besoin de parler du vécu et des doutes vis-à-vis de la confidentialité, au-delà des questions déjà posées.

La session de groupe focus s'est tenue le 10 novembre 2022, lors du forum des maisons de 2e étape et a rassemblé 60 intervenantes provenant des différentes régions administratives du Québec, ce qui dépasse l'objectif de 5 à 10 intervenantes prévu en début de projet.

L'activité a été menée en 3 temps :

- un rappel du contexte du projet et une présentation des résultats du sondage en plénière,
- pour faciliter la parole, nous avons réparti les 60 intervenantes en 4 sous-groupes de 15, chaque sous-groupe étant accompagné d'une animatrice et d'une preneuse de notes,
- un retour en plénière pour faire un retour collectif (questions complémentaires, commentaires) et une présentation des prochaines étapes du projet.

L'activité de sous-groupes a été menée sous forme de discussion semi-dirigée. Toutes les animatrices disposaient de la même liste de questions. Elles ont adapté le rythme de l'activité et la précision des questions en fonction de leur groupe, mais devaient tout de même suivre les thématiques générales du questionnaire.

Du fait de l'approche semi-dirigée, la prise de notes des 4 sous-groupes diffère un peu : certaines questions ont été répondues en bloc et pas individuellement, notamment. La compilation générale reportait donc les réponses dans la section où ces réponses ont été notées durant le sous-groupe.

Méthode d'analyse des données

L'analyse des données recueillies a été réalisée en 3 étapes :

- une compilation du sondage
- une compilation des participations au groupe focus
- un dégagement de faits saillants.

Les deux premières étapes d'analyse étaient des compilations. Il s'agissait donc de faire état des réponses tel qu'elles ont été données pour chacune des activités. Le sondage associait des questions qualitatives et des questions quantitatives. De par la nature qualitative de l'exercice de groupe focus, les réponses ont été reportées telles que prises en note durant l'activité, en enlevant les informations éventuelles d'identification des maisons ou intervenantes.

À noter : le sondage contenait une section d'identification intitulée « Présentez-vous ». La section d'identification avait pour unique but de faciliter les suivis administratifs entre l'Alliance MH2 et les maisons ayant répondu au sondage. Cette section n'a donc pas été utilisée pour la compilation ni pour l'analyse des réponses. La compilation a donc commencé à la question numéro 5.

Le troisième temps d'analyse a consisté en un dégagement de concordances et d'éventuelles discordances entre les réponses apportées au sondage et au questionnaire du groupe focus. Cette étape

a permis de dégager une synthèse des besoins utile à la suite du projet, notamment pour identifier les thématiques à aborder dans les outils de sensibilisation et de formation, mais aussi pour identifier les types de fournisseurs à contacter et de pratiques de confidentialité à étudier. La discussion suivante présente les faits saillants dégagés lors de cet exercice de synthèse.

2.2 Discussion

Les services en ligne et les appareils connectés sont très diversifiés, tant pour les travailleuses des maisons que pour les résidentes : stockage de documents (ex : Google Drive, etc.), suite de logiciels (ex : Office 365, etc.), outils de visioconférences (Zoom, Teams, etc.), comptes personnels ou d'organisme sur les réseaux sociaux, commandes de livraison de repas ou d'épicerie, comptes de loisirs (Disney +, Netflix, etc.), fournisseur d'internet, applications de conversation (ex : WhatsApp, Viber, Messenger, etc.), appareils connectés (domotique, jouets connectés, etc.).

La sécurité et la confidentialité des informations en ligne sont des préoccupations très importantes (14) ou plutôt importantes (1) pour les 15 maisons d'hébergement ayant répondu au sondage.

Toutes les maisons notent que l'accès à des informations personnelles en ligne peut avoir un impact négatif probable (6) ou certain (9).

Bien que la majorité des intervenantes pense avoir plus de contrôle sur la sécurité physique que sur la sécurité en ligne des informations personnelles, elles pensent quasi toutes qu'il est tout aussi important de s'intéresser à la confidentialité et la sécurité des infos en ligne qu'à la sécurité physique (14 sur 15).

Les pratiques de confidentialité appliquées par les fournisseurs de services numériques ne sont pas toujours faciles à identifier et à comprendre. À la question « ***Que veut dire pour vous 'pratiques de confidentialité' des fournisseurs? »*** la majorité des répondantes nomme les politiques de confidentialité, des termes et conditions qui ne sont pas lues, le partage

de la localisation, ou encore le rassemblement d'informations sur les réseaux sociaux.

À travers le sondage et le groupe focus, les répondantes indiquent majoritairement que les pratiques de confidentialité sont une notion qui est difficile à comprendre, donc qu'il est difficile de prendre des décisions éclairées. Ainsi, 14 des 15 répondantes au sondage indiquent qu'elles ne choisissent pas leurs fournisseurs de services numériques en fonction de ce critère – soit parce qu'elles n'ont pas le choix (2), parce qu'elles n'avaient pas pensé à la question (2), ou parce que « c'est compliqué de savoir quelles sont les pratiques de confidentialité de toutes les entreprises » (3) – ou qu'elles font leur sélection en fonction de ce critère quand elles peuvent (7). Une seule réponse au sondage fait état d'une sélection systématique des fournisseurs en fonction de leurs pratiques de confidentialité. Des répondantes indiquent, lors du groupe focus, avoir été amenées à bannir certains outils ou services numériques des maisons à cause des risques de sécurité liés à la difficulté de comprendre et de maîtriser leurs pratiques de confidentialité.

La majorité des répondantes indique que leur maison d'hébergement fait appel à une ressource externe ponctuelle (3) ou habituelle (9) pour assurer la maintenance des appareils et plateformes numériques.

Au total, une vingtaine d'incidents et de préoccupations basées sur l'expérience des maisons et des résidentes en lien avec la confidentialité numérique a été reportée durant les deux activités.

Plusieurs répondantes ont nommé le besoin d'être mieux informées sur les questions de confidentialité numérique, indiquant que cela permettrait aux femmes, d'une part, de bien comprendre ce qui est en leur pouvoir, d'autre part, de pouvoir mieux comprendre les pratiques des fournisseurs avec lesquels elles font affaire.

Les répondantes ont également nommé un besoin de changement de pratiques de la part de certains fournisseurs de services numériques afin d'améliorer la confidentialité, notamment :

- enjeux humains (ex : ne plus localiser ou identifier la maison pour d'autres personnes sans prendre en compte les implications en termes de sécurité liées à cette pratique),
- gestion des dossiers (ex : dossiers traités par plusieurs agents avec peu ou pas de méthode d'identification claire, donc certains ne savent pas qu'il s'agit d'un dossier en violence conjugale et contactent l'ex-conjoint-e),
- besoin de formation et sensibilisation des équipes,
- besoin de rendre plus facile d'accès l'information sur leurs pratiques de confidentialité,
- besoin de procédures adaptées à la violence conjugale pour la gestion des comptes (comptes partagés, notamment).

2.3 Conclusion partielle

Les répondantes ont participé en grand nombre au recueil des besoins ayant rendu possible cet état des lieux. Cela démontre que la thématique de la confidentialité numérique est ancrée dans la réalité des maisons d'hébergement.

En effet, les répondantes identifient les bris de confidentialité comme des incidents pouvant avoir des conséquences directes et graves sur la sécurité des femmes et des équipes des maisons d'hébergement. Ces résultats viennent donc renforcer l'argumentaire en faveur d'une prise en compte de la dimension numérique de la confidentialité dans l'analyse du tissu de sécurité des femmes victimes de violence conjugale.

Les répondantes nomment, certes, le besoin de continuer d'être sensibilisées aux thématiques en lien avec la confidentialité numérique, mais elles formulent aussi la nécessité pour les fournisseurs d'être sensibilisés à leur tour aux enjeux liés à la violence conjugale. Cette double sensibilisation permettrait d'accroitre l'autonomie des femmes, mais aussi de développer des pratiques de confidentialité numériques qui soient adaptées à leur réalité. En recoupant ce besoin de sensibilisation avec la variété d'outils et de services numériques dont font usage les répondantes, et avec le fait que la majorité des maisons d'hébergement contracte des ressources externes en cas de besoins de support

technique, un autre besoin sous-jacent se dessine : les répondantes ont un besoin de confiance envers les fournisseurs de services et d'outils numériques. Il est essentiel pour elles de pouvoir faire des choix éclairés, d'avoir un accès facilité aux pratiques de confidentialité mises en place par les fournisseurs, d'identifier les pratiques manquantes, et de recevoir un service adapté lorsqu'une situation de violence conjugale est signalée au fournisseur.

Ainsi, des pistes d'adaptation des pratiques sont dégagées afin d'élaborer des recommandations concrètes à l'attention des fournisseurs de services et d'outils numériques. Ces recommandations seront présentées à la section 5 du rapport.

3. Les applications numériques

Le terme d'*application numérique* est utilisé pour désigner spécifiquement des entreprises qui fournissent des logiciels et des plateformes en ligne dont les services sont exclusivement consacrés au domaine numérique. Cela peut inclure, par exemple, des plateformes de réseautage social, des systèmes d'opération ou encore des jeux vidéo. Dans le cadre de cette recherche, nous avons identifié des applications numériques, avons analysé leurs politiques de confidentialité et de sécurité en lien spécifiquement avec les enjeux de violence conjugale.

3.1 Méthodologie

Sélection des cas d'étude

Les applications numériques sont extrêmement nombreuses. Ainsi, pour procéder à la sélection des cas d'études, l'équipe de recherche s'est basée sur les résultats ayant émergé du sondage ainsi que du groupe focus menés dans le cadre de la présente recherche. Effectivement, une multitude d'applications et de fournisseurs de service ont été mentionnés par les participantes comme cas de figure où leur utilisation a présenté des enjeux de sécurité pour les femmes et les intervenantes en maisons de 2e étape.

Parmi l'ensemble des cas mentionnés, l'équipe de recherche a basé sa sélection d'étude de cas en fonction de trois critères principaux : la fréquence à laquelle une application a été nommée, la popularité de l'application, la gravité des risques rapportés et une représentativité des catégories d'applications.

Ces critères ont permis la sélection des cinq applications numériques suivantes : TikTok (application de réseau social), Facebook (application de réseau social), Nintendo (console de jeu connectée), Netflix (service de diffusion) et Apple (système d'opération).

Collecte de données

Pour chacune des applications sélectionnées, l'équipe de recherche a mené une analyse de contenu relativement au texte des politiques de confidentialité et de sécurité, ainsi qu'une analyse des fonctionnalités des applications relativement aux paramètres de confidentialité disponibles aux utilisatrices. Les données ont été récoltées dans trois grilles d'analyse :

- Analyse des politiques de confidentialité (analyse de contenu)
- Analyse des politiques et paramètres de sécurité (identification des fonctionnalités et analyse de contenu)
- Analyse des paramètres de confidentialité (analyse des fonctionnalités)

Les différentes catégories d'analyse mobilisées dans ces grilles ont été développées de manière itérative. C'est-à-dire que les applications ont d'abord été analysées en utilisant les catégories analytiques développées par la Fondation Mozilla dans son outil « *Privacy Not Included »[1]. Néanmoins, les grilles d'analyse[2] ont été modifiées en tenant compte des risques, des préoccupations et des besoins spécifiques inhérents au contexte de violence conjugale, tels que soulevés dans le groupe focus et dans le sondage.

Grille 1 : Les politiques de sécurité

Le principal risque en matière de sécurité des applications relève de la gestion des accès. Une des particularités du contexte de violence conjugale est qu'il peut exister un partage des accès à un compte du fait de la vie commune pré ou post séparation. Par exemple : des comptes d'épicerie en commun, des comptes bancaires joints, des comptes en lien avec les enfants, etc. L'analyse ci-dessous s'est concentrée sur la protection des comptes individuels, par opposition aux comptes joints, qui font l'objet d'une approche à différencier et adapter aux cas spécifiques rencontrés. Par comptes individuels, nous faisons référence aux comptes

[1] Mozilla Foundation. "*Privacy Not Included: A Buyer's Guide for Connected Products." Consulté le 14 mars 2023. https://foundation.mozilla.org/en/privacynotincluded/.

[2] Voir l'annexe 2 de ce rapport de recherche.

personnels de l'usagère qu'elle ne souhaite pas partager et dont elle souhaite être la seule à avoir les accès. Il s'agissait donc de voir quelles fonctionnalités étaient disponibles aux utilisatrices ou directement mises en place par le fournisseur pour pouvoir éviter une compromission d'accès de la part d'un acteur de menace. Effectivement, la compromission d'accès – c'est-à-dire la capacité d'un acteur de menace à se connecter à un compte sans l'autorisation explicite de son titulaire – est un risque qui a été soulevé à de multiples reprises dans le groupe focus et qui est également largement documenté dans la littérature portant sur l'utilisation coercitive de la technologie en violence conjugale.

Les éléments d'analyse étaient les suivants :

1. **Utilisation du chiffrement (en transit et au repos) :** ce critère vise à évaluer si un service utilise du chiffrement pour les données en transit (depuis ou vers l'appareil de l'usagère) et au repos (sur les serveurs du fournisseur numérique).

   Le niveau de risque associé à ce critère reste généralement faible à moyen, dans la mesure où l'interception de trafic web permis par du contenu non chiffré demande une connaissance technologique qui ne peut pas être assumée par une majorité des acteurs de menace et correspond moins aux types de compromission d'accès qui sont ressortis des partages d'expérience.

2. **Utilisation de mots de passe robustes :** ce critère vise à évaluer si le service :
   - permet l'utilisation de mots de passe robustes (c'est-à-dire avec un nombre élevé de caractères, et mobilisant des chiffres et caractères spéciaux)
   - a mis en place une interface graphique permettant à l'utilisatrice d'évaluer la robustesse de son mot de passe
   - a mis en place des critères de sécurité minimaux lors de la création d'un mot de passe.

   Le niveau de risque associé à ce critère est considéré comme moyen, dans la mesure où la compromission d'accès est une manière commune pour les acteurs de menace dans le contexte de violence conjugale d'obtenir des informations auxquelles ils n'ont pas accès.

   Néanmoins, la connaissance intime de l'utilisatrice (et potentiellement de ses mots de passe) ne permet pas d'assumer

qu'un mot de passe robuste est une mesure suffisante en soi pour empêcher une compromission d'accès. Pour cette raison, cette fonctionnalité doit être couplée avec la possibilité d'utiliser un second facteur d'authentification et la possibilité de réviser les activités de connexion au compte pour augmenter la sécurisation du compte.

3. **Utilisation d'un second facteur d'authentification :** Ce critère évalue si l'application permet d'activer une authentification à multiples facteurs et, si oui, quelles méthodes sont disponibles pour les utilisatrices.

   Le second facteur d'authentification est un élément clé pour assurer la sécurité des comptes en ligne, dans la mesure où la seule connaissance d'un mot de passe n'est plus suffisante pour se connecter à un compte à partir d'un nouvel appareil. Pour réussir la compromission d'accès, l'acteur de menace devra également avoir en sa possession l'appareil permettant de s'authentifier. La diversité des méthodes de 2FA est également un critère structurant, dans la mesure où différentes méthodes permettent aux utilisatrices de faire des compromis entre le niveau de sécurité désiré (chaque méthode a des avantages et inconvénients différents) et leurs habiletés technologiques (enjeu d'accessibilité et de fractures numériques).

   Pour ces raisons, le fait qu'un service ne dispose pas de possibilités de recourir à des 2FA relève d'un risque élevé.

4. **Révision des activités de connexion :** ce critère fait référence à la fonctionnalité permettant au titulaire d'un compte de pouvoir identifier les différents appareils qui se sont connectés audit compte. Cette fonctionnalité permet, notamment, de détecter les compromissions d'accès et de déconnecter, au besoin, les appareils non-souhaités. Au-delà de la présence de ce critère, nous avons évalué la facilité avec laquelle une utilisatrice peut accéder à ce paramètre en calculant le nombre de clics depuis la page d'accueil de l'application.

   Cette fonctionnalité est centrale à la mitigation de risque lié à la compromission d'accès. Pour cette raison, le fait qu'un service ne dispose pas de celle-ci représente un risque élevé.

Grille 2 : Les politiques de confidentialité

Les détails de la grille d'analyse des politiques de confidentialité est disponible dans l'annexe 1 de ce rapport de recherche. Afin de circonscrire la portée de la recherche et concentrer les efforts d'analyse autour de données significatives, l'analyse des politiques de confidentialité s'est opérée autour de deux types de données considérées comme particulièrement sensibles dans le contexte de violence conjugale.

- **Les données de navigation :** les données de navigation font référence aux données collectées sur les activités de l'utilisatrice sur l'application, sur le navigateur (lorsque la plateforme étudiée collecte par le biais de traceurs ou pixels des informations sur d'autres sites web) ou encore sur l'appareil mobile.

  La collecte de ce type d'informations représente un risque moyen à élevé, dans la mesure où elles peuvent révéler de manière indirecte (par recommandation de contenu, par exemple) ou directe sur la plateforme ou dans le navigateur (par un historique des activités consultable via un compte) des informations confidentielles sur l'utilisatrice.

  Le risque peut donc être élevé si les données de navigation sont rendues accessibles dans un contexte où elles permettraient la surveillance et le contrôle des activités de l'utilisatrice, menant à une éventuelle escalade de la violence (surveillance des changements d'habitude de consommation, surveillance des sites consultés, historique des recherches d'aide).

- **Les données de localisation :** les données de localisation incluent le positionnement GPS, mais également d'autres indicateurs de positionnement géographique comme les adresses IP. Ces informations peuvent être accessibles directement sur la plateforme (cela impliquerait une compromission d'accès de la part de l'acteur de menace) ou encore de manière indirecte, via la personnalisation de contenu (contenu publicitaire ou recommandations d'amis ou de lieux).

  Ce type de données représente un risque élevé, dans la mesure où elles peuvent révéler le lieu de résidence, le lieu d'une maison 2e étape ou encore les lieux fréquemment visités par l'utilisatrice.

Grille 3 : Les paramètres de confidentialité

La grille portant sur l'analyse des paramètres de confidentialité évalue spécifiquement les différentes fonctionnalités qui permettent de contrôler le niveau de confidentialité du contenu publié par l'utilisatrice ou de ses activités sur la plateforme.

Le risque associé à la capacité – ou non – d'une utilisatrice à contrôler ses paramètres de confidentialité est élevé. Effectivement, la surveillance via différentes plateformes numériques est une tactique fréquemment utilisée par les acteurs de menace pour obtenir des informations sur leur cible. Si des informations disponibles publiquement ne constituent pas forcément une compromission d'accès, elles relèvent sans conteste l'importance qu'une utilisatrice soit en mesure de paramétrer ses plateformes afin qu'elles soient en adéquation avec ses attentes en matière de confidentialité. Ainsi, l'utilisatrice devrait être en mesure de choisir quelles informations elle souhaite rendre publiques et quelles informations elle souhaite réserver à une audience limitée. La mise en place d'interfaces intuitives et de paramètres clairement identifiés sont des actions concrètes pouvant être menées par les fournisseurs d'applications numériques pour améliorer la sécurité et la confidentialité de leurs utilisatrices.

En ce sens, les éléments évalués sont les suivants :

1. **Les paramètres de confidentialité sont accessibles :** ce critère est évalué en fonction du nombre de clics nécessaires depuis la page d'accueil pour accéder aux paramètres de confidentialité.
    - 1-2 clics : Très bonne accessibilité
    - 3-4 clics : Accessibilité moyenne
    - 5 clics et plus : Mauvaise accessibilité

    L'évaluation du risque lié à une « mauvaise accessibilité » des paramètres de confidentialité est élevée, dans la mesure où il dissuade les utilisatrices de mettre en place efficacement des éléments pouvant améliorer leur sécurité.

2. **Les paramètres de confidentialité sont simples à comprendre :** ce critère évalue le niveau de langage technique utilisé pour décrire les paramètres de confidentialité ainsi que l'impact sur l'accessibilité des données de l'utilisatrice.
    - Clarté sémantique : les mots utilisés ne sont pas trop techniques et peuvent être compris par des personnes sans grandes connaissances technologiques.

- Utilisation d'icônes : présence d'icônes permettant d'appuyer le texte et de le rendre plus accessible aux personnes ayant différentes capacités de compréhension des textes écrits.
- Nombre de paramètres de confidentialité : plus le nombre de paramètres est élevé, plus leur impact est granulaire et peut engendrer des erreurs de configuration de la part des utilisatrices. Un plus petit nombre de paramètres, en revanche, permet une protection de base plus simple et efficace.

Le niveau de risque associé à des paramètres compliqués à comprendre et à utiliser est également élevé, dans la mesure où cela peut entraîner des erreurs ou un faux sentiment de sécurité de l'utilisatrice face aux informations disponibles.

3. **Les paramètres permettent de rapporter du contenu problématique, de bloquer, restreindre ou mettre en sourdine rapidement des utilisateurs :** Ce critère évalue les fonctionnalités disponibles pour rapporter ou limiter l'accès et l'exposition aux acteurs de menace. Le harcèlement en ligne, la prise de contact répétée et insistante, et la prise de contact non souhaitée sur les réseaux sociaux sont des tactiques rapportées dans la littérature. Plus spécifiquement, les éléments suivants ont été pris en considération :
   - La variété des fonctionnalités disponibles : en fonction des situations, une utilisatrice pourrait préférer restreindre un acteur de menace au lieu de le bloquer afin d'éviter une réaction ou une escalade de violence. Une plus grande variété des fonctions permet un plus grand contrôle de l'utilisatrice.
   - Efficacité : les utilités des fonctionnalités sont explicitées et permettent à l'utilisatrice de poser des actions dont elle comprend les portées et les limites.

   Le niveau de risque associé à ce critère est élevé, dans la mesure où des fonctionnalités limitées ou une mauvaise communication liée à leurs impacts et limites peuvent créer un faux sentiment de sécurité et exacerber la possibilité de bris de confidentialité ou de violence numérique pour les utilisatrices.

3.2 Analyse des résultats

Analyse des paramètres de sécurité

De manière générale, les applications étudiées appliquent d'une manière relativement uniforme de bonnes pratiques de sécurité de base selon les critères identifiés : utilisation du chiffrement, mot de passe, possibilité d'utiliser l'authentification à double facteur.

D'abord, quelques nuances ont été observées entre les applications, notamment en matière d'accessibilité des paramètres d'application. Seule Facebook permet d'accéder aux paramètres de sécurité en moins de deux clics, représentant une bonne accessibilité des paramètres de sécurité. Les autres applications nécessitent toutes entre 3 et 4 clics pour arriver aux paramètres pertinents.

Ensuite, tous les services ne permettent pas la même variété d'options en ce qui a trait au double facteur d'authentification. Dans le cadre de cette recherche, nous n'avons pas établi quelles étaient les méthodes de 2FA privilégiées dans le contexte de la violence conjugale, mais avons identifié qu'une plus grande variété de méthodes permettait de pallier différents niveaux d'aisance technologique et différents modèles de menace. En ce sens, des applications telles que TikTok, Apple ou encore Nintendo ont des offres plus limitées en matières de 2FA, ce qui a le potentiel de pouvoir limiter les options disponibles aux utilisatrices désireuses de sécuriser leurs comptes.

Finalement, si l'ensemble des applications permettent avec une facilité relative (entre 2 et 4 clics) de faire la révision des activités de connexion, les informations affichées lors de cette révision d'activité est intéressante à noter. Effectivement, l'ensemble des applications étudiées affichent les appareils connectés avec leur « nom ». Cette pratique est relativement récente dans la mesure où, dans la dernière année, ces sections affichaient généralement les adresses IP associées aux appareils connectés. Dans le contexte de la violence conjugale, cela pouvait permettre à un acteur de menace ayant compromis le compte de pouvoir avoir une idée approximative du lieu de connexion. Cela représentait donc un risque pour les utilisatrices. Ce changement minimisant les informations disponibles même pour les utilisatrices permet une meilleure protection. Néanmoins, pour certains services (tels que Netflix), un acteur de menace ayant compromis le compte de l'utilisatrice (ou y ayant accès par le partage de compte) peut télécharger les

données personnelles et avoir accès aux adresses IP à partir desquelles des appareils se sont connectés au compte.

Analyse des politiques de confidentialité

En contexte de violence conjugale, les risques associés à la collecte de données par les services numériques se situent au niveau de la compromission de compte (si un acteur de menace obtient l'accès non autorisé au compte d'une utilisatrice, ce dernier peut avoir accès à plusieurs données récoltées à son égard). Cependant, ce n'est pas ce profil de menace dont il sera question dans cette analyse, puisque les mesures de mitigation à ce niveau se rattachent principalement aux paramètres de sécurité. Les risques abordés dans le cadre de cette analyse seront surtout de l'ordre de la personnalisation des contenus ainsi que des recommandations (d'amis ou de contacts).

D'abord, des applications analysées, deux (Facebook et TikTok) se catégorisent comme des réseaux sociaux et ont donc un objectif commercial directement lié à la collecte et à l'analyse d'informations personnelles. Les politiques de confidentialité étudiées soulèvent effectivement la collecte d'informations relatives à la localisation (géolocalisation, mais également adresse IP des appareils connectés), aux activités de l'utilisatrice sur l'application ainsi que sur son navigateur (ex. : page web consultées) par le biais de pixels ou de témoins de connexion. Peu d'informations sont disponibles sur les manières concrètes dont les plateformes utilisent les données récoltées pour faire des recommandations de contenus ou de contacts. Cependant, ce mécanisme représente un risque clair quant à la confidentialité de plusieurs informations de personnes vivant de la violence conjugale. Effectivement, dans la mesure où l'acteur de menace a déjà entretenu une relation significative avec l'utilisatrice, iels peuvent déjà avoir un grand nombre de données en commun : contacts sur la plateforme, fréquentation de lieux communs (tels que l'école des enfants, l'ancienne maison), etc. En ce sens, même si le « lien de relation est rompu », il pourrait être probable que les algorithmes puissent faire des recommandations à un acteur de menace qui dévoilent des informations confidentielles :

- publicité ciblée liée à des recherche ou activités de navigation de l'utilisatrice,
- recommandation de contacts pouvant révéler la prise de contact avec des ressources d'aide,

- recommandation de contacts pouvant révéler un nouveau profil créé par l'utilisatrice,
- recommandation de contenus pouvant suggérer des lieux fréquentés de l'utilisatrice, comme la présence d'une femme à une maison d'hébergement.

Ensuite, un autre service (Apple) peut, à partir des données récoltées, recommander des contacts en fonction des données préalablement enregistrées. Si ces recommandations ne sont pas faites dans une perspective commerciale, celles-ci peuvent tout de même impacter la sécurité des utilisatrices si l'appareil n'est pas configuré de manière optimale.

Finalement, les applications de divertissement (Nintendo et Netflix) représentent un risque plus limité relativement à la collecte de données liée aux différentes activités en ligne à des fins de recommandation de contenus ou de contacts. N'excluant pas les pratiques, déjà rapportées, visant à utiliser de comptes récréatifs pour altérer la sécurité psychosociale d'une utilisatrice (modification des listes de favoris, suppression des contenus, etc.), les éléments de risque directement en lien avec les politiques de confidentialité, pour ces deux plateformes, se situent principalement au niveau de la compromission d'accès.

Analyse des paramètres de confidentialité

Une grande majorité des services étudiés permettent la mise en place de paramètres de confidentialité pour qu'une utilisatrice puisse masquer certains aspects de ses activités à d'autres personnes utilisatrices de la plateforme. Une seule exception est à noter, celle de la plateforme Netflix. La plateforme permet, certes, d'ajouter un code PIN pour limiter l'accès à son profil afin de masquer des données des autres personnes partageant un compte, sur les appareils applicables, mais des données de localisation (adresses IP) peuvent être accessibles lorsqu'un utilisateur fait la demande de télécharger les informations personnelles.

Ensuite, un autre élément soulevé dans les autres applications (particulièrement Facebook, TikTok et Apple) est le caractère extrêmement granulaire des paramètres de confidentialité offerts aux utilisatrices. Cela peut être expliqué par le besoin d'affaires des compagnies à favoriser l'engagement et la connexion. Néanmoins, cette granularité peut rendre plus complexes les activités de paramétrage et

engendrer des erreurs des utilisatrices qui pourraient nuire à leur sécurité et favoriser la violence numérique de la part d'un acteur de menace.

De plus, notre analyse des paramètres de confidentialité (et des fonctions de blocage et de mise en sourdine) de l'application Facebook a souligné que, devant les nombreux services offerts par la plateforme (Marketplace, Facebook Dating, Messenger, etc.), il peut être particulièrement complexe de pouvoir ajuster efficacement les paramètres en fonction de la situation. Par exemple, un usager bloqué dans l'application Messenger ne le sera pas automatiquement sur Facebook; un utilisateur bloqué sur Facebook peut tout de même voir les activités de l'utilisatrice sur MarketPlace ou Facebook Dating. En bref, cette analyse démontre que les fonctionnalités, surtout lorsqu'elles sont fragmentées de la sorte peuvent représenter un risque substantiel.

Finalement, deux services numériques ont développé un « assistant de configuration » pour accompagner leurs usagers dans les étapes de configuration les plus importantes. Les interfaces d'assistance présentent des fonctionnalités distinctes, particulièrement lorsqu'analysées sous l'angle de la violence conjugale :

- Facebook : l'interface d'assistance rendue disponible par l'application permet de réviser les paramètres de confidentialité en fonction de différentes thématiques (sécurité du compte, qui peut voir certaines publications, etc.). Cette fonctionnalité semble conçue pour accompagner les utilisateurs dans l'ajustement sommaire des paramètres de sécurité et de confidentialité et ne présente pas un vocabulaire ou des énoncés spécifiques pour faire référence à la violence conjugale. Il s'agit donc d'une configuration standardisée, mais qui élude certains détails importants pour réduire les risques de violence numérique dans le contexte de violence conjugale.
- Apple : la fonctionnalité « contrôle de sécurité » semble avoir été développée avec le contexte de violence conjugale en tête. Effectivement, des indices permettent de déduire l'intention derrière cette interface de configuration, notamment dans le vocabulaire utilisé (à travers la mention: « quelqu'un pourrait remarquer l'interruption de votre partage ») ainsi que la présence de la fonctionnalité « Quitter rapidement » qui permet de retourner rapidement sur l'écran d'accueil et d'éliminer les traces de l'opération. La fonctionnalité « Contrôle de sécurité » guide l'utilisatrice dans les différents paramètres de sécurité pour révoquer des accès ou faire une réinitialisation d'urgence.

Contrairement à l'interface de configuration mise de l'avant par Facebook, celle d'Apple sélectionne les paramètres utiles à ajuster dans les cas qui peuvent s'apparenter à de la violence conjugale. Cela permet à l'utilisatrice de concentrer ses efforts et de réduire les risques d'erreur occasionnés par une granularité des paramètres et l'absence d'accompagnement à travers les menus.

3.3 Discussion & conclusion partielle

Différents éléments d'intérêt se dégagent de l'analyse des paramètres de sécurité et de confidentialité ainsi que des politiques de confidentialité mises de l'avant par les applications numériques.

D'abord, les éléments de sécurité et de confidentialité qui sont les mieux observés sont ceux dont les risques ne sont pas spécifiques à la violence conjugale. Effectivement, la mise en place de mots de passe robuste, la possibilité de réviser les activités de connexion ainsi que la possibilité d'activer un second facteur d'authentification sont des mesures de sécurité qui répondent à des modèles de menace largement répandus (cybercriminalité, par exemple) et qui ont, indirectement, une efficacité dans le domaine de la violence conjugale.

Un autre point d'importance à soulever concerne l'opacité des entreprises (majoritairement des réseaux sociaux). Effectivement, tel que noté dans l'analyse, les recommandations de contenus et de contacts peuvent représenter un risque de divulgation d'informations confidentielles dans le contexte de violence conjugale. L'opacité des algorithmes responsables d'organiser le contenu et d'effectuer les recommandations, doublée d'un certain laisser-aller règlementaire, limite significativement les informations disponibles sur les mécanismes de recommandations, et donc les suggestions et les analyses pouvant être faites pour adresser les enjeux de confidentialité dans le contexte de violence conjugale et, plus largement, concernant les enjeux d'intérêt public.

La fragmentation des services et des paramètres représente un risque dans la mesure où elle tend à compliquer les opérations permettant d'avoir une meilleure confidentialité en ligne. Des paramètres plus simples et englobants, pour leur part, ont l'avantage d'être plus faciles à opérationnaliser et tendent ainsi à minimiser les risques.

Enfin, les deux assistants de configuration démontrent en quoi le développement d'une interface de configuration ne garantit pas nécessairement en soi la réduction du risque en sécurité lié à la violence conjugale. Au contraire, le développement d'un outil d'assistance pensé avec les enjeux de violence conjugale en tête permet d'adresser de manière plus simple, efficace et ciblée des enjeux de sécurité et de confidentialité préalablement identifiés, au lieu de remettre le fardeau et la charge mentale sur les utilisatrices.

4. Services numériques

Le terme *service numérique* est utilisé pour désigner les entreprises et organisations dont seulement une partie des activités se fait sur un support numérique. Contrairement aux applications numériques – dont la collecte et l'analyse de données est centrale au modèle d'affaires et aux activités commerciales – les services numériques se caractérisent par le fait qu'ils collectent principalement des « données de service », c'est-à-dire des données qu'une entreprise doit posséder pour offrir un service à un individu. Dans son ouvrage Data and Goliath (2015), Bruce Schneier décrit ces données de services comme des informations qu'une personne divulgue à une entreprise afin de recevoir un service (des exemples de données collectées seraient une adresse postale, un numéro de téléphone, une adresse courriel, etc.). Ces données de services sont souvent, pour des raisons de commodité, stockées numériquement par les entreprises et accessibles aux commis de service à la clientèle.

Les deux types de services se distinguent donc à quelques niveaux :

- Par le contexte et les objectifs entourant la collecte de données : la collecte de données numériques pour les applications se fait dans une perspective commerciale alors que les services numériques récoltent des données nécessaires pour fournir un service précis (électricité, Internet, assurances, etc.).
- Par la présence fréquente de comptes partagés : effectivement, plusieurs services offrent la possibilité de partage de comptes à des fins de convenance. Il n'est donc pas rare que des informations personnelles soient stockées sur un compte accessible à plusieurs personnes. En ce sens, dans un contexte de violence conjugale, plusieurs éléments peuvent s'avérer problématiques comme la séparation d'un compte, mais aussi les informations qui peuvent toujours être accessibles à un acteur de menace.
- Par la présence d'un service à la clientèle : contrairement aux applications numériques, les services numériques sont dotés de service à la clientèle permettant aux utilisateurs et utilisatrices de parler à des employé-es en cas de problème. Dans le contexte de

violence conjugale, un acteur de menace peut tenter d'accéder à des informations personnelles en convainquant un-e employé-e à partir d'informations qu'il possède déjà sur le compte en question ainsi que sur la victime.

En ce sens, la prochaine section visera exclusivement à analyser les pratiques de protection des données personnelles mises en place par les fournisseurs de services numériques, en gardant en tête ces spécificités. Nous aborderons donc la méthodologie employée pour analyser ces services et détaillerons les principales trouvailles faites dans le cadre de la recherche.

4.1 Méthodologie

Sélection des cas

Les résultats du groupe focus et du sondage ont permis d'identifier des services qui provoquaient des enjeux de sécurité auprès des femmes et des intervenantes en maison de 2e étape. L'équipe de recherche a sélectionné les services en fonction de trois critères : la fréquence à laquelle un service était nommé, la gravité des risques rapportés et une représentativité des catégories de services. Ce processus a mené à la sélection de cinq cas d'études.

Méthode de collecte de données

L'analyse de politiques de confidentialité ainsi que l'entrevue semi-dirigée ont été les deux approches méthodologiques mobilisées pour collecter les données d'analyse. Initialement, l'équipe de recherche a lancé une procédure de recrutement pour des entretiens semi-dirigés auprès de la sélection de services dont les types de services fournis correspondaient à ceux ayant émergé du sondage et du groupe focus comme pouvant provoquer des enjeux de sécurité pour les femmes et les intervenantes en maisons de 2e étape.

Les tentatives de prises de contact avec les fournisseurs de services sélectionnés ont finalement abouti à la conduite d'un entretien. L'équipe

de recherche a effectué une analyse des politiques de confidentialité des autres fournisseurs à partir des catégories d'analyse élaborées dans la grille d'entretien (disponible en annexe).

Les résultats des analyses seront présentés sous forme anonymisée. L'objectif de cette recherche étant d'identifier tant les bonnes pratiques que les facteurs de risques, l'anonymisation des entreprises et organisations analysées était une condition essentielle à l'obtention de données de qualité.

Catégories d'analyse

En contraste avec les catégories d'analyse présentées pour les applications numériques, la collecte de données a été structurée de manière à récolter des informations à propos de trois catégories d'analyse.

La première renvoie aux capacités du fournisseur de service à reconnaître les cas de violence conjugale et de harcèlement. L'objectif est plus précisément de cerner les connaissances détenues sur les besoins en matière de confidentialité et sur les données traitées susceptibles d'être ciblées dans un contexte de violence conjugale.

La deuxième catégorie d'analyse porte sur les mesures mises en place par le fournisseur de service afin d'identifier et de gérer les cas où des clientes sont en situation de violence conjugale. Ces mesures peuvent prendre des formes variées, notamment : formation et sensibilisation des employé-es, mise en place de procédures internes en cas d'incident ou lorsqu'une personne rapporte être victime de violence conjugale, fonctionnalités mises à disposition des clients permettant de mieux protéger ses données personnelles.

Finalement, la troisième catégorie d'analyse cible la perception organisationnelle de la menace. Cette catégorie renvoie à la conception interne du rôle qu'occupe le fournisseur de service dans la prévention de la violence conjugale et des difficultés rencontrées pour remplir ce rôle.

4.2 Analyse des résultats

D'emblée, il importe de mentionner que nous avons été en mesure d'identifier des processus spécifiquement dédiés à répondre aux enjeux de confidentialité des informations personnelles inhérentes à la violence conjugale dans seulement une entreprise/organisation étudiée. En ce sens, les éléments figurant dans les prochains paragraphes reflètent les éléments soulevés dans ce cas d'étude.

Cette section aborde les résultats dans leur ensemble pour assurer l'anonymat des organisations.

A) Perception organisationnelle de la menace

Cette catégorie analytique identifie les données étant perçues comme confidentielles par les entreprises dans le contexte spécifique de la violence conjugale.

Tout d'abord, aucun élément des politiques de confidentialité n'aborde spécifiquement les enjeux de violence conjugale. Les informations personnelles ou confidentielles sont donc abordées sous l'angle juridique inhérent à ces politiques.

L'entreprise disposant d'une procédure spécifique aux cas de violence conjugale a identifié certaines données spécifiques comme étant particulièrement à risque : le numéro de téléphone (particulièrement si ce dernier a été mis à jour), l'adresse courriel et, surtout l'adresse physique, laquelle peut être déclinée en adresse de facturation, adresse de correspondance ou adresse domiciliaire. En somme, il s'agit de toute information permettant le « retraçage » d'une personne par un acteur de menace.

Ces éléments identifiés par l'organisation sont en adéquation avec les données récoltées dans les étapes précédentes de cette recherche.

B) Mesures en place

Comme mentionné plus haut, aucune entreprise étudiée dans le cadre de cette recherche ne rend disponibles des informations relatives à des mesures spécifiques de protection de renseignements personnels en contexte de violence conjugale dans la politique de confidentialité disponible sur le site web. Les manières de prévenir les accès non autorisés ainsi que la divulgation d'informations se restreignent donc à des mesures relativement standard comme la mise en place de mots de passe pour accéder au compte en ligne, l'option d'un double facteur d'authentification (sur le compte en ligne), ou encore la reconnaissance vocale ou des méthodes similaires pour les services téléphoniques. Bien que ces méthodes soient des barrières essentielles, leurs mises en place ne sont pas suffisantes pour limiter l'accès à un acteur de menace qui dispose d'une connaissance intime de sa victime.

Une entreprise a mentionné avoir des mesures en place pour répondre aux besoins spécifiques de la violence conjugale, spécifiquement en ce qui a trait aux opérations du service à la clientèle. Les mesures en place mentionnées dans le cadre d'une entrevue semi-dirigée se déclinent en deux initiatives.

D'abord, une procédure spéciale est enclenchée lorsqu'un-e employé-e du service à la clientèle dispose d'un doute raisonnable permettant de croire que la personne au téléphone vit de la violence conjugale. Cette procédure est généralement déclenchée si une personne mentionne explicitement être victime, ou si des questions soulevant des « drapeaux rouges » sont énoncées. Par exemple « est-ce que c'est possible que mon ex ait accès à mes données? ». Dans ces cas, c'est l'employé-e du service à la clientèle qui est invité à utiliser son « gros bon sens » pour mettre en place une opération dérogatoire pour offrir des mesures de sécurité supplémentaires, isolant ainsi le dossier de tout acteur de menace. L'entreprise a également mentionné avoir publié des informations de sensibilisation disponibles aux employé-es dans leur intranet.

Ensuite, l'entreprise a également mis en place un projet pilote permettant d'établir une ligne dédiée à la violence conjugale dans les opérations de services à la clientèle. Ce projet pilote a été élaboré en collaboration avec l'Alliance MH2. Sommairement, cette mesure vise à créer une ligne

de service à la clientèle uniquement accessible aux refuges pour femmes – question de pouvoir créer un canal de communication direct et de confiance pour adresser les enjeux. Dans le cadre de ce projet pilote, il a été question de former un nombre restreint d'employé-es au contexte de violence conjugale. De cette manière, les femmes en maison d'hébergement utilisant cette ligne spéciale ont accès uniquement à des employé-es sensibilisé-es à leur situation et connaissant finement les processus dérogatoires mis en place pour assurer leur protection.

Ce projet pilote, récemment mis en place, a demandé la mobilisation d'une multitude de départements et a dû être accompagné d'ateliers de sensibilisation pour les employé-es concernés. Il démontre, d'une part, les éléments spécifiques qui doivent être mis en place pour répondre efficacement aux enjeux soulevés par la violence conjugale et, d'autre part, dans quelle mesure la mise en place de ces bonnes pratiques en sécurité demande un effort concerté d'un grand nombre de départements au sein d'une entreprise.

Dans l'ensemble des cas étudiés dans le cadre de cette recherche, aucune entreprise n'a mis en place de guide ou de documentation permettant à des victimes de violence d'être mises au courant de processus dérogatoires ou d'activer certains paramètres de sécurité dédiés pouvant être bénéfiques à la protection de leurs renseignements personnels.

C) Capacité de reconnaître les cas

Lorsqu'une organisation détient une procédure dérogatoire de protection des renseignements personnels adaptée à la violence conjugale, le « nerf de la guerre » revient à ce que les employé-es soient adéquatement outillé-es pour reconnaître ces cas de violence conjugale. Dans le cas étudié, quelques éléments intéressants permettent d'amorcer une réflexion sur les différentes manières de pouvoir reconnaître efficacement des cas, ainsi que sur les opportunités et limites que ces mécanismes peuvent également poser.

Dans un premier temps, l'utilisation d'une ligne – et surtout un processus ainsi que des ressources – dédiée aux maisons d'hébergement est une

manière extrêmement efficace de simplifier et de rendre plus efficientes les mesures de protection et d'accommodement tout en permettant d'éviter une trop grande victimisation des femmes. Cette mesure, même si elle a la limite de ne pas pouvoir toucher l'ensemble des femmes victimes de violence conjugale, promet de rendre le processus plus efficace pour celles qui sont considérées comme étant grandement à risque d'homicide conjugal. Le numéro de la ligne en question est uniquement connu des maisons d'hébergement, réduisant par la même occasion le risque de mauvais usage.

Ensuite, en ce qui a trait aux cas qui doivent être identifiés à travers le processus standard de service à la clientèle (c'est-à-dire, les femmes qui n'ont pas accès à la ligne dédiée), l'identification de cas relève certainement d'une certaine subjectivité des employé-es. Effectivement, les victimes ne vont pas toujours mentionner explicitement la situation dans laquelle elles se trouvent. En ce sens, la capacité des individus à reconnaître un cas de violence conjugale dépend tant d'éléments subjectifs dans l'interaction avec la cliente que du niveau de sensibilisation des employé-es du service à la clientèle.

Finalement, nos données révèlent que, dans ces interactions, les employé-es du service à la clientèle sont limités dans ce qu'iels peuvent demander au client-es dans la mesure où « la loi ne veut pas non plus qu'on pose des questions sur la vie personnelle [des client-es] comme : '*Est-ce que vous déménagez dans un contexte de violence conjugale*?' On n'est pas autorisé à faire ça en téléphonie ». En ce sens, outre les services liés à la ligne dédiée auxquels une victime peut accéder si elle est hébergée en maison, la reconnaissance doit être déclenchée par des informations exprimées par la victime, et reconnues par l'employé-e au service à la clientèle.

En ce sens, nos données démontrent que la reconnaissance optimale des cas semble passer par trois éléments clés :

- la mise en place de ressources dédiées et facilement accessibles à une population visée,
- la communication efficace des manières dont une cliente peut demander un service adapté aux risques associés à la violence conjugale,

- une formation adéquate des employé-es pour être en mesure de reconnaître efficacement les cas, et de les rediriger vers des ressources appropriées.

4.3 Discussion et conclusion partielle

L'analyse des fournisseurs de services nous permet de soulever de nombreux enjeux. D'abord, que la mise en place de stratégies de protection de données personnelles adaptées au contexte de la violence conjugale semble être marginale dans les cas étudiés (1 sur 5 a mis en place des stratégies adaptées). Or, nos données démontrent non seulement un besoin de procédures spécifiques pour protéger les victimes, mais de manière plus importante, elles démontrent l'incapacité des « procédures » standard à répondre aux risques présentés par des acteurs de menace motivés, persistants, violents et connaissant intimement leur victime.

Nous notons également une absence de publicisation (notamment sur les sites web des entreprises étudiées ainsi que dans leurs politiques de confidentialité) des potentielles mesures mises en place pour protéger la confidentialité des informations personnelles des victimes de violence conjugales. Des données d'entrevue soulèvent à ce titre des enjeux ainsi qu'une prudence institutionnelle à divulguer ce genre d'informations. Parmi les enjeux soulevés ayant dissuadé la promotion de ces procédures adaptées dans les espaces publics, nous pouvons noter, par exemple, la crainte qu'une campagne publicitaire puisse être « un couteau à double tranchant » ou encore être perçue comme une manière de faire « du gain politique ». Cette situation peut être exacerbée par le fait que très peu d'organisations canadiennes semblent offrir ce type de services adaptés.

Finalement, nous relevons que les initiatives permettant une meilleure protection adaptée des informations personnelles des victimes de violence conjugale sont importantes et extrêmement utiles. Néanmoins, elles dépendent exclusivement de la bonne foi d'entreprises / organisations plutôt que sur une réponse concertée, structurante et systémique des enjeux de confidentialité uniques et urgents du contexte de violence conjugale.

Peu de modèles sont disponibles à ce jour, mais nous notons tout de même une initiative australienne « The National Plan to End Violence against Women and Children 2022-2032 » qui mobilise des approches novatrices. Celles-ci encouragent notamment les entreprises – notamment des institutions publiques et parapubliques – à se doter de « Family Violence Policy ». Effectivement, ce type de politiques se retrouvent (comme pour les politiques de confidentialité) sur les sites web d'organisations / entreprises australiennes et y détaillent les mesures mises en place pour identifier, répondre et protéger « les clients et employés affectés par des formes de violence familiale » (Traduction libre: EnergyAustralia, 2020). Entre autres choses, ces politiques définissent la notion de violence conjugale et familiale, identifient sur leur site web public les mesures pouvant être mises en place pour sécuriser les données de comptes et énoncent les mesures de sensibilisation en place dans l'entreprise ou l'organisation pour que les employé-es soient efficacement outillés pour répondre à ce type de demandes.

5. Recommandations

5.1 Découvertes majeures

Les personnes aux prises avec la violence conjugale sont confrontées à un modèle de menace absolument unique en ce qui a trait à la protection des renseignements personnels et à la sécurité de l'information. Effectivement, ces personnes sont confrontées à des acteurs de menace motivés, persistants et, parfois, disposant de connaissances poussées en informatique. De plus, ce qui distingue les risques propres à la violence conjugale des modèles de menace plus traditionnels est le fait que les acteurs de menace sont également des personnes qui disposent d'une connaissance détaillée et intime de leur victime.

Les mesures de sécurité et de confidentialité envisagées lors de la conception de services numériques restent souvent orientées vers une conception relativement standardisée des acteurs de menace comme provenant de l'externe et de personnes inconnues. Or, dans le contexte de violence conjugale, la situation est inverse. Les résultats de nos études de cas permettent de dégager quelques constats :

- pour une majorité des services numériques étudiés, les mesures de protection liées aux renseignements personnels et à la sécurité de l'information sont appliquées, en toute apparence, de manière relativement standardisée. C'est-à-dire que ces services ne semblent pas considérer spécifiquement des préoccupations liées à la violence conjugale dans l'établissement de politiques, de processus ou de paramètres;
- les mesures de protection de la confidentialité et de la sécurité, lorsqu'appliquées de manière standardisée, sont mal adaptées aux besoins et préoccupations inhérents aux situations de violence conjugale. Cela limite la potentielle efficacité des mesures de sécurité et de confidentialité et tend à mettre à risque accru des utilisatrices déjà en état de vulnérabilité;
- En contraste, quelques cas étudiés démontrent une volonté et un intérêt de la part de certains fournisseurs de services numériques de vouloir développer des mesures qui adressent les enjeux et risques spécifiques à la violence conjugale. Bien que le contexte de cette recherche ne permette pas d'en mesure l'efficacité, la présente recherche démontre que ces mesures répondent à un besoin exprimé et documenté des femmes victimes de violence conjugale et des maisons d'hébergement de 2e étape.

5.2 Recommandations à l'attention des fournisseurs de services et outils numériques

Le regroupement d'analyses réalisé au long de ce rapport nous permet de dégager des recommandations afin d'offrir aux fournisseurs de services et d'outils numériques des pistes d'action concrètes à explorer pour adapter leurs pratiques en matière de protection de la vie privée spécifiquement en contexte de violence conjugale. Étant donné :

- que la recherche a permis de démontrer le caractère essentiel de l'implication des fournisseurs de services dans le renforcement du tissu de sécurité des résidentes et travailleuses de MH2,
- que les intervenantes ont formulé le besoin, ancré dans des situations de risque tangibles, de pouvoir faire appel à des ressources techniques de confiance et de pouvoir accéder facilement à des politiques, outils et procédures adaptés aux spécificités du contexte de violence conjugale,
- que les pratiques commerciales des fournisseurs d'applications peuvent agir à l'encontre des efforts des utilisatrices ayant un besoin accru de protection de leur vie privée,
- que le fonctionnement des outils numériques (stratégies de développement ou de programmation, options mises à disposition, etc.) est régi par des décisions d'entreprises qui dépassent le niveau individuel des possibles incombant aux utilisatrices,
- que les enjeux de fractures numériques affectent une grande partie de la population, dont on ne peut pas séparer les femmes victimes de violence conjugale, et que ces fractures ont un impact sur l'accès aux outils et ressources pertinentes, l'aisance d'utilisation des outils, l'aisance de compréhension des contenus techniques souvent complexes et changeant rapidement,
- que des pratiques inadaptées, tant techniques (fonctionnalités) qu'humaines (service à la clientèle), peuvent s'avérer inefficaces en contexte de violence conjugale, voire contribuer à augmenter la mise en danger des résidentes et des travailleuses des MH2,

nous formulons les recommandations suivantes :

Mobilisation et action concertée

- Analyser les enjeux en lien avec la protection de la vie privée en ligne de manière structurelle et systémique, donc ne pas reporter ces enjeux uniquement sur la responsabilité des individus.
- Prendre en compte le contexte d'urgence et les particularités du contexte coercitif et de violence conjugale dans la mise en œuvre de mesures (notamment : acteur de menace connaissant sa victime, situation d'urgence et de détresse, besoin d'indications claires et faciles à suivre pour la mise en sécurité).
- Développer des liens étroits d'échange entre les milieux technologiques et les ressources d'aide afin de maintenir une sensibilisation et une formation actualisées sur les enjeux rencontrés et permettre une mise à jour efficiente des services et outils.

Adaptation des services et des outils

- Veiller à la sensibilisation et à la formation des équipes des fournisseurs de services numériques sur les besoins spécifiques en matière de confidentialité en contexte de violence conjugale afin, notamment, de faciliter l'identification des cas potentiels de violence conjugale et de fournir un support adapté aux victimes.
- Mettre en place des procédures et pratiques de protection des données personnelles spécifiques au contexte de violence conjugale.
- Présenter les fonctionnalités et procédures mises à disposition des utilisatrices en langage simple et accessible, et de manière facile d'accès et d'utilisation.

Diffusion de l'information

- Mettre en œuvre les mesures nécessaires et les plus sécuritaires possibles pour favoriser aux utilisatrices et aux ressources d'aide la prise de connaissance des procédures adaptées disponibles.
- Développer et rendre accessibles des canaux de communication par lesquels les femmes victimes de violence conjugale peuvent communiquer leurs besoins.
- Rendre accessibles en langage simple et clair les informations relatives aux pratiques de confidentialité des fournisseurs.

6. Conclusion

Dès le début de cette recherche, l'urgence d'agir était manifeste : les incidents de confidentialité numérique ont des impacts réels et tangibles sur les femmes victimes de violence conjugale et sur les travailleuses de maison d'hébergement de 2e étape. Surveillance en ligne et hors ligne, tentative de maintenir le contrôle et de poursuivre la violence, mise en danger physique de la femme ciblée, des autres résidentes et des travailleuses des MH2 – ces impacts ont pu être documentés en laissant la parole aux intervenantes et résidentes de MH2 grâce au sondage et au groupe focus.

L'enjeu est d'autant plus grand que, malgré la place de plus en plus centrale qu'occupent les outils et services numériques dans notre quotidien, la littérature présente une absence criante d'informations sur le degré de sensibilisation des fournisseurs de services et d'outils numériques au contexte de violence conjugale, et une absence toute aussi remarquable d'analyses des impacts des pratiques de protection de la vie privée mises en place, ou non, par ces fournisseurs sur la sécurité des utilisatrices aux prises avec la situation d'urgence que constitue la violence conjugale. Ce travail de recherche, à défaut de pouvoir s'appuyer sur un vaste curriculum, a donc dû s'atteler à créer la donnée manquante, pourtant essentielle.

Dans ce sens, recouper l'état des lieux des besoins et enjeux relatifs à la confidentialité numérique en MH2 avec une étude des politiques, fonctionnalités et procédures mises en place par les fournisseurs de services et d'outils, ou d'applications numériques a permis d'identifier plus concrètement les aspects de la pratique technologique qui ont un impact sur la possibilité ou non d'assurer la protection de la vie privée des utilisatrices pour qui un bris de confidentialité peut avoir des conséquences irrémédiables.

Forte de ces analyses croisées, la recherche a donc permis de dégager un ensemble de recommandations à l'attention des fournisseurs. Ces recommandations ont un double objectif : leur fournir des pistes d'action claires, mais aussi leur permettre, plus largement, de s'impliquer dans le

renforcement du tissu de sécurité des résidentes et intervenantes de MH2. En effet, face à des technologies dont le développement et le déploiement dépassent les volontés individuelles, des stratégies de protection de la vie privée des utilisatrices ne pourraient être complètes et efficientes sans une action concertée des différentes parties prenantes. Les intervenantes et les résidentes continuent de se former et de s'outiller autant que possible, mais cette recherche est une invitation aux fournisseurs qui ne le font pas encore à rejoindre l'effort collectif.

Cette conclusion elle-même ne pourrait se terminer sans étendre davantage l'invitation. La nécessité de mobilisation est encore plus vaste que les fournisseurs de services et d'outils numériques. Pour l'heure, au Canada, incluant le Québec, la mise en place de pratiques de protection de la vie privée en ligne spécifiques au contexte de violence conjugale est laissée à l'initiative des fournisseurs volontaires. Or, une action voulant avoir un impact structurant et à grande échelle ne pourrait se penser sans envisager l'instauration d'un cadre incitatif, de modalités de régulation qui, à l'instar des cas étudiés dans le présent rapport, comme le cas australien, permettraient de guider les fournisseurs dans l'adoption de meilleures pratiques adaptées et de faire de la protection de la vie privée en lien avec la violence conjugale une priorité incontournable, au fil du développement des technologies connectées.

7. Bibliographie

Afrouz, R. (2021). The Nature, Patterns and Consequences of Technology-Facilitated Domestic Abuse : A Scoping Review. *Trauma, Violence, & Abuse*, *24*(2), 913-927. https://doi.org/10.1177/15248380211046752

Aghtaie, N., Larkins, C., Barter, C., Stanley, N., Wood, M. J. E., & Överlien, C. (2018). Interpersonal violence and abuse in young people's relationships in five European countries : Online and offline normalisation of heteronormativity. *Journal of Gender-Based Violence*, *2*(2), 293-310. https://doi.org/10.1332/239868018X15263879270302

Aikenhead, M. (2021). Revenge Pornography and Rape Culture in Canada's Nonconsensual Distribution Case Law. In J. Bailey, A. Flynn, & N. Henry (Éds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (p. 533-553). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211039

Al-Alosi, H. (2017). Cyber-violence : Digital abuse in the context of domestic violence. *UNIVERSITY OF NEW SOUTH WALES LAW JOURNAL*, *40*(4), 1573-1603. https://doi.org/10.3316/agispt.20175338

Al-Nasrawi, S. (2021). Combating Cyber Violence Against Women and Girls : An Overview of the Legislative and Policy Reforms in the Arab Region*. In J. Bailey, A. Flynn, & N. Henry (Éds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (p. 493-512). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211037

Anderson, B., & Wood, M. A. (2021). Doxxing : A Scoping Review and Typology. In J. Bailey, A. Flynn, & N. Henry (Éds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (p. 205-226). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211015

Araújo, A. V. M. de, Bonfim, C. V. do, Bushatsky, M., & Furtado, B. M. A. (2022). Technology-facilitated sexual violence : A review of virtual

violence against women. *Research, Society and Development*, *11*(2), Art. 2. https://doi.org/10.33448/rsd-v11i2.25757

Baddam, B. (2018). TECHNOLOGY AND ITS DANGER TO DOMESTIC VIOLENCE VICTIMS : HOW DID HE FIND ME? *Albany Law Journal of Science & Technology*, *28*(1), 73-93.

Bailey, J., & Shayan, S. (2016). Missing and Murdered Indigenous Women Crisis : Technological Dimensions. *Canadian Journal of Women and the Law*, *28*(2), 321-341. https://doi.org/10.3138/cjwl.28.2.321

Barker, K., & Jurasz, O. (2021). Text-Based (Sexual) Abuse and Online Violence Against Women : Toward Law Reform? In J. Bailey, A. Flynn, & N. Henry (Éds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (p. 247-264). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211017

BC Society of Transition Houses. (2019). *The Technology Safety and Privacy Toolkit – BC Society of Transition Houses*. BC Society of Transition Houses. https://bcsth.ca/techsafetytoolkit/

Beagle, A. (2011). Modern Stalking Laws : A Survey of State Anti-Stalking Statutes Considering Modern Mediums and Constitutional Challenges. *Chapman Law Review*, *14*(2), 457-482.

Bernier, A. (s. d.). *L'utilisation des TIC à des fins de harcèlement criminel en situation de violence conjugale : La théorie des opportunités et des activités routinières de Cohen et Felson (1978) remaniée* [Travail dirigé, Université de Montréal]. Papyrus. https://papyrus.bib.umontreal.ca/xmlui/handle/1866/18553

Bowles, N. (2018, juin 23). Thermostats, Locks and Lights : Digital Tools of Domestic Abuse. *The New York Times*. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Cama, E. (2021). Understanding Experiences of Sexual Harms Facilitated through Dating and Hook Up Apps among Women and Girls. In J. Bailey, A. Flynn, & N. Henry (Éds.), *The Emerald International Handbook*

of Technology-Facilitated Violence and Abuse (p. 333-350). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211025

Centre Hubertine Auclert. (s. d.). *Je suis victime de cyberviolences conjugales | Guide de protection numérique*. Je protège ma vie privée en ligne. Consulté 24 août 2022, à l'adresse https://www.guide-protection-numerique.com/je-suis-victime-de-cyberviolences-conjugales

Cericola, R., & Wells, K. (2018, octobre 23). How to Keep Your Smart-Home Technology Secure From Domestic Abusers. *Wirecutter*. https://www.nytimes.com/wirecutter/blog/keep-your-smart-home-secure-from-domestic-abusers/

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., & Ristenpart, T. (2018). The Spyware Used in Intimate Partner Violence. *2018 IEEE Symposium on Security and Privacy (SP)*, 441-458. https://doi.org/10.1109/SP.2018.00061

Chayn. (s. d.). *Do it yourself online safety*. Chayn. Consulté 22 août 2022, à l'adresse https://www.chayn.co/safety

Cheung, A. (2021). Doxing and the Challenge to Legal Regulation : When Personal Data Become a Weapon. In J. Bailey, A. Flynn, & N. Henry (Éds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (p. 577-594). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211041

Citron, D. (2015). Spying Inc. *Washington and Lee Law Review*, *72*(3), 1243-1282.

Coalition Against Stalkerware. (s. d.). *Page d'accueil*. Coalition Against Stalkerware. Consulté 24 août 2022, à l'adresse https://stopstalkerware.org/fr/

Coombs, E. (2021). Human Rights, Privacy Rights, and Technology-Facilitated Violence. In J. Bailey, A. Flynn, & N. Henry (Éds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*

(p. 475-491). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211036

Dimond, J. P., Fiesler, C., & Bruckman, A. S. (2011). Domestic violence and information communication technologies. *Interacting with Computers*, *23*(5), 413-421. https://doi.org/10.1016/j.intcom.2011.04.006

Douglas, H., & Burdon, M. (2018). Legal Responses to Non-Consensual Smartphone Recordings in the Context of Domestic and Family Violence. *University of New South Wales Law Journal*, *41*(1), 157-184.

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated Domestic and Family Violence : Women's Experiences. *The British Journal of Criminology*, *59*(3), 551-570. https://doi.org/10.1093/bjc/azy068

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control : Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, *18*(4), 609-625. https://doi.org/10.1080/14680777.2018.1447341

Dumont, G. (2019, mars 24). Des femmes victimes de violence conjugale traquées par des moyens technologiques. *Radio-Canada.ca*. https://ici.radio-canada.ca/nouvelle/1159681/femmes-traquees-violence-conjugale-ottawa-outaouais-technologie

Dunn, S. (2021). Is it *Actually* Violence? Framing Technology-Facilitated Abuse as Violence. In J. Bailey, A. Flynn, & N. Henry (Éds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (p. 25-45). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211002

Dunn, S., & Aikenhead, M. (2022). On the Internet, Nobody Knows You are a Dog : Contested Authorship of Digital Evidence in Cases of Gender-Based Violence. *Canadian Journal of Law and Technology*, *19*(2), 371-409.

Fetters, A. (2018, juillet 11). Why It's Hard to Protect Domestic-Violence Survivors Online. *The Atlantic*. https://www.theatlantic.com/family/archive/2018/07/restraining-orders-social-media/564614/

Fraser, C., Olsen, E., Lee, K., Southworth, C., & Tucker, S. (2010). The New Age of Stalking : Technological Implications for Stalking. *Juvenile and Family Court Journal*, *61*(4), 39-55. https://doi.org/10.1111/j.1755-6988.2010.01051.x

Freed, D., Havron, S., Tseng, E., Gallardo, A., Chatterjee, R., Ristenpart, T., & Dell, N. (2019). « Is my phone hacked? » Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction*, *3*(202), 202:1-202:24. https://doi.org/10.1145/3359304

Freed, D., Palmer, J., Minchala, D. E., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital Technologies and Intimate Partner Violence : A Qualitative Analysis with Multiple Stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, *1*(46), 46:1-46:22. https://doi.org/10.1145/3134681

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A Stalker's Paradise" : How Intimate Partner Abusers Exploit Technology. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1-13. https://doi.org/10.1145/3173574.3174241

Fukuchi, A. (2011). A Balance of Convenience : Burden-Shifting Devices in Criminal Cyberharassment Law. *Boston College Law Review*, *52*(1), 289-338.

Grimani, A., Gavine, A., & Moncur, W. (2022). An Evidence Synthesis of Covert Online Strategies Regarding Intimate Partner Violence. *Trauma, Violence, & Abuse*, *23*(2), 581-593. https://doi.org/10.1177/1524838020957985

HACK*BLOSSOM*. *(s. d.)*. *DIY Cybersecurity for Domestic Violence*. *HACK*BLOSSOM. Consulté 22 août 2022, à l'adresse https://hackblossom.org/domestic-violence/

Hand, T., Chung, D., & Peters, M. (2009). The Use of Information and Communication Technologies to Coerce and Control in Domestic Violence and Following Separation. *Australian Domestic & Family Violence Clearinghouse*. *Newsletter*, *2009*, 1-16.

Harris, B., & Woodlock, D. (2021). Digital Coercive Control and Spatiality : Rural, Regional, and Remote Women's Experience. In J. Bailey, A. Flynn, & N. Henry (Éds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (p. 387-406). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211030

Havron, S., Freed, D., Dell, N., Chatterjee, R., McCoy, D., & Ristenpart, T. (2019). Clinical Computer Security for Victims of Intimate Partner Violence. *Usenix*, 105-122.

Henry, N., & Witt, A. (2021). Governing Image-Based Sexual Abuse : Digital Platform Policies, Tools, and Practices. In J. Bailey, A. Flynn, & N. Henry (Éds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (p. 749-768). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211054

Hosani, H. A., Yousef, M., Shouq, S. A., Iqbal, F., & Mouheb, D. (2019). A Comparative Analysis of Cyberbullying and Cyberstalking Laws in the UAE, US, UK and Canada. *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, 1-7. https://doi.org/10.1109/AICCSA47632.2019.9035368

Kabassema, P. S. (2020). Les plateformes numériques : Des nouveaux outils d'agression et de contrôle dans le couple – numérique investigation. *numérique investigation : Enquêtes sociophotographiques Université Paris 8- ENS Louis-Lumière*. https://numerique-investigation.org/cyber-surveillance-conjugale/4623/

Laguë Maltais, F. (2021). *Les technologies de l'information et de la communication utilisées en contexte de violence conjugale : Une*

analyse des liens entre les cyberviolences vécues, les stratégies d'adaptation et la détresse psychologique [Mémoire de maîtrise, Université de Montréal]. Papyrus. https://papyrus.bib.umontreal.ca/xmlui/handle/1866/26030

Lee, K., & Anderson, J. (2016). The Internet and Intimate Partner Violence : Technology Changes, Abuse Doesn't. *Criminal Justice*, *31*(2), 28-33.

Leitão, R. (2018). Digital Technologies and their Role in Intimate Partner Violence. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, 1-6.

Leitão, R. (2021). Technology-Facilitated Intimate Partner Abuse : A qualitative analysis of data from online domestic abuse forums. *Human–Computer Interaction*, *36*(3), 203-242. https://doi.org/10.1080/07370024.2019.1685883

Lo, M. (2021). A Domestic Violence Dystopia : Abuse via the Internet of Things and Remedies under Current Law Note. *California Law Review*, *109*(1), 277-316.

Lopes Gomes Pinto Ferreira, G. (2021). Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence : Perspectives from Advocates in the Global-South. In J. Bailey, A. Flynn, & N. Henry (Éds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (p. 427-446). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211032

Louie, Y. M. (2021a). *For better or worse : When technology intersects with domestic violence and the lived experiences of Chinese immigrant women* [Thèse, RMIT University]. https://researchrepository.rmit.edu.au/esploro/outputs/9922068770201341

Annexe 1: Grille d'analyse - analyse de politiques de confidentialité

Grille 1 : Politique de sécurité de l'information

		Application
Utilisation du chiffrement	En transit	
	Au repos	
Utilisation de mots de passe robustes	Permet l'utilisation de mots de passe robustes (nombre élevé de caractères, chiffres et caractères spéciaux)	
	Présence d'une interface graphique permettant d'évaluer la robustesse de son mot de passe	
	Mise en place de critères de sécurité minimaux lors de la création d'un mot de passe	
Utilisation d'un second facteur d'authentification	Permet l'activation d'une authentification à multiples facteurs	
	Méthodes d'authentification à multiples facteurs disponibles	
Révision des activités de connexion	Présence d'une fonctionnalité permettant au titulaire d'un compte d'identifier les appareils connectés	
	Facilité d'accès au paramètre (nombre de clics depuis la page d'accueil)	

Grille 2 : Politique de confidentialité

	Application
Données personnelles (données de navigation + localisation)	
Données sociales	
Données partagées/vendues à des tiers	
Données utilisées à des fins publicitaires	
Données utilisées à des fins publicitaires	
Possibilité de supprimer les données	
Antécédents de fuite/violation	
Possible d'utiliser hors-ligne	
Politique simple à comprendre	

Grille 3 : Paramètres de confidentialité

		Application
Les paramètres de confidentialité sont accessibles (nombre de clics depuis la page d'accueil)		
Les paramètres de confidentialité sont simples à comprendre	Clarté sémantique	
	Utilisation d'icônes	
	Nombre de paramètres de confidentialité	
Les paramètres permettent de rapporter du contenu problématique, de bloquer, restreindre ou mettre en sourdine rapidement des utilisateurs	Variété des fonctionnalités disponibles	
	Efficacité	

Annexe 2: Grille d'entretien

Durée et structure de l'entretien : 30 minutes à 1h

1) **Reconnaissance des cas de violence conjugale et de harcèlement**
   a) Que connaissez-vous des besoins en confidentialité dans le contexte spécifique de la violence conjugale en relation avec les services que vous offrez?
      i) Avez-vous reçu de l'information et / ou de la formation sur les besoins en confidentialité spécifiques à la violence conjugale? (pour aller plus loin: formations/informations ponctuelles ou mécanismes de mises à jour)
      ii) Pouvez-vous donner des exemples d'enjeux pour lesquels vous avez obtenu de l'information ou de la formation? (techniques, psychoaffectifs, sociaux, matériels)
   b) Avez-vous identifié des données traitées par votre entreprise qui sont susceptibles d'être ciblées pour faciliter de la violence conjugale?

2) **Mesures en place dans l'organisation**
   a) Pouvez-vous nous parler des mesures, procédures et efforts de sensibilisation déjà en place au sein de votre entreprise en lien avec la violence conjugale?
      i) Existe-t-il une procédure de signalement? Que se passe-t-il en cas de signalement par un.e client.e?
      ii) Si un.e client.e vit de la violence conjugale, y a-t-il la possibilité d'une modification de service?
   b) Des fonctionnalités permettant de mieux protéger ses données personnelles dans un contexte de violence conjugale sont-elles disponibles pour les utilisateur.rice.s?
      i) Avez-vous des procédures à destination des client.e.s (par exemple: un guide "en cas de rupture")
      ii) Peut-on demander la suppression des coordonnées de livraison et historiques de commandes passées enregistrées au dossier? (si applicable - ex.: services de livraison d'épicerie, de repas)
      iii) Y a-t-il un moyen d'ajouter un autre critère de sécurité au compte si on suspecte une surveillance du compte (ex.: un mot de passe ou mot-code additionnel à utiliser en ligne ou par téléphone)
   c) Quelles sont les parties prenantes impliquées dans les actions de prévention de violence conjugale? (par exemple: services juridiques, service à la clientèle, etc.)
   d) Au sein de votre entreprise, disposez-vous de procédures internes en cas d'incident ou lorsqu'une personne rapporte être victime de violence conjugale?

e) Quels sont les engagements que votre entreprise a envers la clientèle en matière de divulgation de données à un tiers.

3) **Perception organisationnelle de la menace**
   a) D'après vous, quel est le rôle qu'une entreprise devrait jouer afin de prévenir la violence physique envers ses clients? (physique, matérielle, économique, etc.)
   b) Quels sont les défis ou difficultés pour adopter des mesures de prévention?
   c) Est-ce que la violence conjugale est un enjeu reconnu au sein de votre entreprise. Est-ce que cette réalité occupe une place plus importante dans vos activités? Si oui, depuis quand?

4) **Conseils, recommandations et réflexions**
   a) Avez-vous des conseils à partager à votre clientèle afin de faciliter l'appropriation de vos mesures de confidentialité?
   b) Y a-t-il des thèmes et enjeux sur lesquels vous aimeriez être mieux informés?
   c) Souhaitez-vous ajouter autre chose?

Annexe 3: Sondage

Le sentiment de sécurité numérique en MH2

Dans le cadre du projet mené par le CDÉACF, l'Alliance des maisons de 2e étape et le Lab 2028, ce formulaire vise à réaliser un état des lieux actuel du sentiment de sécurité ou d'insécurité vécu dans les maisons d'hébergement de 2e étape par rapport aux enjeux de protection des données personnelles.

Dans le formulaire, il est demandé de décrire votre expérience avec les « fournisseurs de services numériques ». Notez que cette expression regroupe :

- les entreprises qui offrent des services à distance (livraison de repas ou d'épicerie, taxis, etc.),
- les entreprises qui fournissent des logiciels et des plateformes en ligne (logiciels et suites informatiques, comptes connectés, appareils connectés, etc.)
- les sociétés qui font du soutien technique ou informatique.

Merci pour vos réponses qui nous aideront à mieux comprendre la situation et produire des outils adaptés!

Présentez-vous

1) **Quel est votre nom?**

[Champ de commentaire]

2) **Dans quelle maison travaillez-vous?**

[Champ de commentaire]

3) **Dans quelle région administrative êtes-vous?**

[Champ de commentaire]

4) **Quel est votre courriel?**

[Champ de commentaire]

Les pratiques numériques

Questions aux intervenantes

5) **Quels types d'appareils numériques utilisez-vous pour le travail? (Cochez toutes les cases qui s'appliquent.)**

ordinateur

tablette

téléphone portable

autre

- Si autre : quels autres appareils utilisez-vous pour le travail?

[Champ de commentaire]

6) **Intervenante : Quels services numériques utilisez-vous? (Cochez toutes les cases qui s'appliquent.)**

1| stockage de documents (ex : Google Drive, etc.)

2| suite de logiciels (ex : Office 365, etc.)

3| outils de visioconférences (Zoom, Teams, etc.)

4| comptes personnels de réseaux sociaux

5| comptes ou pages de l'organisme sur les réseaux sociaux

6| commandes de repas chez des restaurateurs (ex : commande en ligne chez Saint Huber)

7| commandes de repas via des plateformes (Uber Eat, Skip the dishes, Doordash, etc.)

8| commande d'épicerie, de fournitures, etc.

9| comptes de loisirs (Disney +, Netflix, etc.)

10| fournisseur d'internet

11| Autre

- Intervenante : Si autre : quels autres services numériques utilisez-vous?

[Champ de commentaire]

7) **Est-ce que les pratiques de confidentialité des données des usagères font partie de vos critères de sélection d'une entreprise de services numériques?**

(Note : les pratiques de confidentialité comprennent, par exemple la création d'une politique de confidentialité, ou encore l'ensemble des actions qu'une entreprise met en place pour assurer la confidentialité des informations personnelles de ses clientes)

1| Oui, on fait toujours notre choix en fonction des pratiques de confidentialité de l'entreprise

2| Oui, on fait notre choix en fonction des pratiques de confidentialité de l'entreprise, quand on peut

3| On est sensibles aux pratiques de confidentialité, mais on n'a pas vraiment le choix dans les fournisseurs de service

4| Non, ce n'est pas un critère de sélection car c'est compliqué de savoir quelles sont les pratiques de confidentialité de toutes les entreprises

5| Non, on a décidé que ce n'est pas un critère de sélection

6| Je n'ai jamais pensé à la question

Questions aux résidentes

8) Quels types d'appareils numériques sont utilisés par vous ou par les membres de votre famille à la MH2? (Cochez toutes les cases qui s'appliquent.)

1| ordinateur

2| tablette

3| téléphone intelligent

4| assistant de maison (Alexa, Google home, etc.)

5| consoles de jeux connectées (PlayStation, Wii, Xbox, etc.)

6| montres connectées (iWatch, etc.)

7| jouets connectés (Hello Barbie, robot ou ourson connecté, etc.)

8| autre

- Si autre : quels autres types d'appareils sont utilisés par vous ou par les membres de votre famille à la MH2?

[Champ de commentaire]

9) **Est-ce qu'il y a des appareils qui circulent entre les parents? (Par exemple des appareils connectés des enfants ou tablettes autre qu'ils utilisent à la MH2 ou quand ils vont rendre visite à leur père s'il y a lieu.) Lesquels?**

[Champ de commentaire]

10) **Résidente : Quels services numériques utilisez-vous? (Cochez toutes les cases qui s'appliquent.)**

1| stockage de documents (ex : Google Drive, etc.)

2| suite de logiciels (ex : Office 365, etc.)

3| outils de visioconférences (Zoom, Teams, etc.)

4| comptes personnels de réseaux sociaux

5| comptes ou pages de l'organisme sur les réseaux sociaux

6| commandes de repas chez des restaurateurs (ex : commande en ligne chez Saint Huber)

7| commandes de repas via des plateformes (Uber Eat, Skip the dishes, Doordash, etc.)

8| commande d'épicerie, de fournitures, etc.

9| comptes de loisirs (Disney +, Netflix, etc.)

10| fournisseur d'internet

11| Je ne sais pas

12| Autre

- Résidente : Quels autres services numériques utilisez-vous?

[Champ de commentaire]

11) **Est-ce que vous avez des comptes communs avec votre ex-partenaire? (ex : Netflix, téléphone etc.).**

1| Oui

2| Non

3| Je ne suis pas certaine

- Si oui : Quels comptes avez-vous en commun?

[Champ de commentaire]

- Si pas certaine : quels comptes pensez-vous avoir peut-être en commun?

[Champ de commentaire]

Le rapport aux technologies connectées

Questions aux intervenantes

12) Quel énoncé décrit le mieux votre niveau de familiarité avec les technologies connectées?

1 | Je suis très à l'aise avec les technologies connectées en général

2 | Je me débrouille assez bien avec les technologies connectées

3 | Je suis à l'aise avec les outils que j'ai l'habitude d'utiliser, mais moins avec de nouveaux outils

4 | Je ne suis pas très à l'aise avec les technologies connectées

13) Qui fait la maintenance des appareils et / ou des plateformes numériques de votre maison d'hébergement? (Ex : mise à niveau du système d'exploitation de vos ordinateurs, création de compte pour un nouveau service en ligne, etc.)

1 | Chaque travailleuse maintient son matériel et ses plateformes

2 | Une ou plusieurs travailleuses sont désignées pour faire la maintenance

3 | Une ressource externe ponctuelle (spécialiste contacté.e pour un besoin spécifique)

4 | Une ressource externe habituelle (spécialiste qui fait le suivi continu des appareils et plateformes technologiques de l'organisme)

5 | Je ne sais pas

Question aux résidentes

14) Qui fait la maintenance des appareils et / ou des plateformes numériques des résidentes? (Ex : mise à niveau du système d'exploitation de leurs ordinateurs, création de compte pour un nouveau service en ligne, etc.)

1 | Chaque résidente fait sa maintenance seule

2 | Toute l'équipe est à l'aise d'accompagner la résidente qui en a besoin

3| Une travailleuse spécifique ou quelques travailleuses peuvent accompagner la résidente qui en a besoin

4| La résidente doit chercher de l'aide à l'externe

5| Ne sait pas

La gestion des risques numériques

Questions aux intervenantes

15) Diriez-vous qu'assurer la sécurité et la confidentialité de nos informations en ligne est :

1| très important

2| plutôt important

3| pas très important

4| pas du tout important

16) Pensez-vous que l'accès à des informations personnelles en ligne peut avoir un impact négatif sur la sécurité hors ligne des femmes résidentes?

1| Cela a un impact,

2| Il est possible que cela ait un impact

3| Il est peu probable que cela ait un impact

4| Cela n'a pas d'impact

5| Je ne sais pas

17) Quel degré de contrôle estimez-vous avoir sur la sécurité physique des résidentes et intervenantes?

1| contrôle total

2| beaucoup de contrôle

3| un peu de contrôle

4| Pas du tout de contrôle

18) Quel degré de contrôle estimez-vous avoir sur la sécurité des informations en ligne des résidentes et des intervenantes?

1| contrôle total

2| beaucoup de contrôle

3| un peu de contrôle

4| Pas du tout de contrôle

19) Selon vous, quelle importance faut-il accorder à la confidentialité et la sécurité des informations en ligne, par rapport à la confidentialité et la sécurité physiques des résidentes et des intervenantes?

1| C'est plus important que d'assurer la confidentialité et la sécurité physiques des résidentes et des intervenantes

2| C'est tout aussi important que d'assurer la confidentialité et la sécurité physiques des résidentes et des intervenantes

3| C'est moins important que d'assurer la confidentialité et la sécurité physiques des résidentes et des intervenantes

4| Ça n'a pas d'importance, il faut se concentrer seulement sur la sécurité physique des résidentes et des intervenantes

Partage d'expériences

Question aux intervenantes

20) Y a-t-il déjà eu un problème en lien avec la confidentialité des informations en ligne dans votre maison? (ex : votre adresse a été diffusée en ligne, les informations de localisation d'une résidente ont été partagées sans son consentement en ligne ou à une autre personne, etc.)

1| Oui

2| Non

3| Je ne sais pas

- Si oui : Pouvez-vous décrire ce qu'il s'est passé? (quel service était utilisé, quelles informations ont été partagées, etc.)

[Champ de commentaire]

21) Avez-vous, ou la personne concernée, tenté de signaler le problème à l'entreprise qui a fourni le service numérique?

1| Oui

2| Non

- Si oui : Avez-vous, ou la personne concernée, réussi à joindre l'entreprise facilement pour résoudre le problème? (Cochez toutes les cases qui s'appliquent.)

1| Oui, c'était facile de joindre quelqu'un

2| C'était compliqué d'arriver à parler à quelqu'un

3| On n'a pas réussi à parler à quelqu'un

4| L'entreprise a résolu rapidement le problème

5| L'entreprise a résolu le problème, mais ça a pris du temps

6| L'entreprise n'a pas résolu le problème et on a trouvé une solution nous-même

7| L'entreprise n'a pas résolu le problème et on n'a pas trouvé de solution nous-même non plus

22) Pouvez-vous expliquer comment s'est passée la prise de contact avec l'entreprise? Avez-vous obtenu l'aide dont vous aviez besoin? Quel est votre retour d'expérience?

[Champ de commentaire]

Le questionnaire touche à sa fin. N'hésitez pas à laisser un commentaire pour apporter une précision, compléter une de vos réponses ou nous partager votre point de vue sur les enjeux de confidentialité et de sécurité numérique. Merci!

[Champ de commentaire]

Annexe 4: Questionnaire de focus groupe

Déroulement

13h à 13h15 : Lise Chovino fait la présentation du projet en plénière

13h15 à 15h : Sous-groupes

15h-15h30 : En plénière : Restitution / échange

Questions pour sous-groupes

Les pratiques reliées à la confidentialité

Que veut dire pour vous « pratiques de confidentialité » des fournisseurs?
Notes :
Est-ce facile pour vous d'identifier les pratiques de confidentialité mises en place par les fournisseurs de services en ligne? Pourquoi?
Notes :
[question 7 du sondage] Est-ce que les pratiques de confidentialité des données sont un critère de sélection de vos outils numériques? Pourquoi?
Notes :
[question 10 du sondage] Est-ce que les résidentes gèrent chacune leur accès personnel à internet ou il y a une seule connexion commune pour toutes les résidentes de la maison?
Notes :
[question 11 du sondage] Comment sont gérés les comptes communs entre les résidentes et l'ex / conjoint-e?
Notes :
Est-ce que les résidentes nomment parfois des préoccupations en lien avec la confidentialité de leurs informations personnelles en ligne? (peur que leurs déplacements soient partagés, peur que leur adresse soit révélée, etc.)
Notes :
Avez-vous d'autres remarques à partager sur cette partie?
Notes :

Les expériences vécues

Est-ce que vous reportez / notez tous les incidents de confidentialité qui arrivent? Pourquoi?
Notes :
[question 15] La sécurité et la confidentialité de nos informations en ligne sont des préoccupations très importantes (14) ou plutôt importantes (1) pour toutes les maisons. Avez-vous mis des mesures en place pour prévenir les risques reliés à la confidentialité des informations en ligne dans votre MH2?
Notes :
[question 15] Quelles sont les conséquences en cas de fuite d'informations? (l'ex qui découvre la localisation, etc.) Y a-t-il des conséquences individuelles (ex : la résidente doit changer ses identifiants), des conséquences collectives (ex : il faut déplacer la résidente pour sécuriser les autres résidentes de la maison)?
Notes :
Dans le sondage, des intervenantes ont nommé des problèmes survenus avec différents fournisseurs [présenter les problèmes] Avez-vous eu des cas similaires? Cela peut concerner les fournisseurs pour l'équipe ou les comptes des résidentes.
Notes :
Qu'est-ce que les fournisseurs de services numériques pourraient mettre en place pour vous faciliter la gestion des données personnelles de l'équipe et des résidentes? (ex : que les restaurants acceptent de supprimer l'adresse de commande une fois la livraison finie? De la sensibilisation au personnel qui gère les dossiers scolaires informatisés, etc.)
Notes :
Avez-vous d'autres besoins et remarques par rapport à cette section?
Notes :

Centre de documentation sur l'éducation des adultes et la condition féminine (CDÉACF)

469, rue Jean-Talon O, Bureau 229
Montréal QC H3N 1R4

Téléphone : 514 876-1180
Sans frais : 1 866 972-1180

Courriel : info@cdeacf.ca

Site internet : www.cdeacf.ca

Ce projet a été financé par le Commissariat à la protection de la vie privée du Canada (CPVP).

CDEACF
Centre de documentation
sur l'éducation des adultes et la condition féminine

Lab 2038

Alliance MH2