# L’utilisation de l’IA pour plaider en faveur des personnes survivantes: Guide sur la réduction des méfaits à l’intention des maisons d’hébergement et du personnel antiviolence



# Table des matières

**Risques liés à l'utilisation de l'IA dans le travail contre la violence ..... 3**

**Éléments à prendre en compte lors de la réflexion sur l'utilisation de l'IA dans le travail antiviolence ..... 7**

**Utilisations à haut risque de l'IA dans la promotion des droits des survivantes ..... 9**

**Utilisations de l'IA présentant moins de risques ..... 13**

**Politiques et pratiques de l'organisation ..... 13**

**Résumé ..... 17**

L’intelligence artificielle (IA) fait de plus en plus partie de notre quotidien. Pour les programmes de lutte contre la violence disposant de peu de moyens, ces outils peuvent présenter des avantages concrets. Des outils tels que ChatGPT, Microsoft Copilot, les assistants de rédaction, les outils de transcription et de gestion de réunions, ainsi que les fonctionnalités d’IA intégrées aux messageries électroniques, aux traitements de texte et à d’autres logiciels peuvent permettre d’accélérer et de faciliter certaines tâches administratives.

Par ailleurs, le recours à l’IA dans le cadre des interventions auprès des survivantes peut entraîner des risques liés à la vie privée, la confidentialité, la sécurité, ainsi qu’aux aspects juridiques, éthiques et organisationnels. Les informations concernant les survivantes sont souvent extrêmement sensibles.

La divulgation d'informations permettant d'identifier une survivante, son lieu de résidence, ses enfants, sa situation ou les risques pesant sur sa sécurité peut avoir de graves conséquences. Une fois les informations partagées avec un outil d'IA tiers, l'organisation peut se retrouver avec moins de contrôle sur le lieu où elles sont stockées, les personnes qui y ont accès, la durée de leur conservation et leur éventuelle utilisation à d'autres fins.

Ce guide propose une approche axée sur la protection de la vie privée et la réduction des méfaits dans le cadre de l'utilisation de l'IA dans les maisons d'hébergement (MH) et les organisations antiviolence au Canada. Il vise à habiliter les organisations et le personnel à identifier les risques et à instaurer des politiques et des pratiques responsables en matière d'IA.

**Important: Ce document fournit des informations générales et ne constitue pas un avis juridique. Les organisations doivent déterminer quelles lois relatives à la protection de la vie privée et quelles autres obligations légales s'appliquent à elles, et solliciter l'avis de leur responsable de la protection des données, de leur conseillère juridique ou de l'autorité de contrôle compétente en matière de protection de la vie privée lorsque cela s'avère nécessaire.**

## Risques liés à l'utilisation de l'IA dans le travail antiviolence

L'IA soulève un large éventail de préoccupations, notamment relatives à l'éthique, l'impact environnemental, les répercussions sur le monde du travail, les préjugés, l'accessibilité et les effets sociaux plus larges de ces technologies. Ce sont là des questions importantes, mais elles sortent du cadre du présent document.

Ce guide traite des risques les plus directement liés à la sécurité des survivantes et aux pratiques antiviolence, notamment la vie privée, la confidentialité, la sécurité, les obligations légales et la responsabilité organisationnelle.

## 1. Les outils d'IA ne sont pas nécessairement privés ou confidentiels

Vous ne devez pas partir du principe que les informations saisies dans un outil d'IA restent privées et confidentielles. Celles-ci peuvent être transmises à un prestataire tiers et sont alors soumises aux conditions générales, pratiques en matière de confidentialité, politiques de conservation des données, pratiques de formation, mesures de sécurité et dispositions contractuelles de ce prestataire. En fonction de l'outil et de ses paramètres, les conversations peuvent être stockées, consultées, conservées pendant un certain temps, vendues, divulguées dans le cadre d'une assignation à comparaître ou utilisées d'autres manières décrites dans les politiques de confidentialité de l'entreprise. Cela signifie que d'autres personnes pourraient avoir à votre insu accès aux informations que vous saisissez.

Les obligations canadiennes en matière de protection de la vie privée ne disparaissent pas du simple fait que des informations sont saisies dans un système d'IA. La législation applicable à une organisation peut dépendre de facteurs tels que la province ou le territoire, son statut (organisme public ou privé) et la nature de ses activités. Par exemple, la loi sur la protection des renseignements personnels (PIPA) de la Colombie-Britannique s'applique aux organismes privés, y compris les associations à but non lucratif, tandis que d'autres textes législatifs peuvent s'appliquer aux organismes publics.

Les organisations ne doivent pas partir du principe que, sous prétexte qu'un outil est largement utilisé, gratuit ou fourni par Microsoft ou Google, il est pour autant adapté au traitement d'informations sensibles. Les autorités canadiennes chargées de la protection de la vie privée ont spécifiquement mis en évidence des préoccupations en matière de protection de la vie privée liées à l'IA générative, notamment la collecte excessive de données à caractère personnel, le consentement et la transparence, les informations inexactes, les difficultés d'accès, de rectification et de suppression, ainsi que la redevabilité.

## 2. Les informations que vous fournissez pourraient être conservées plus longtemps que vous ne le pensez, voire de manière définitive.

Le fait de supprimer une conversation de votre écran ne signifie pas nécessairement que toutes les copies de ces informations ont été immédiatement supprimées des systèmes de l'entreprise. Les pratiques en matière de conservation et de suppression varient d'un service d'IA à l'autre. Certaines entités peuvent conserver des informations pendant une certaine durée à des fins de sécurité, juridiques, techniques ou autres. Il peut également arriver qu'une entreprise soit légalement tenue de conserver ou de communiquer certaines informations.

Par exemple, les informations détenues par une entreprise pourraient faire l'objet d'une demande judiciaire, telles qu'une décision de justice ou une assignation à comparaître, selon les circonstances et la juridiction concernée.

## 3. L’IA peut fournir des informations inexactes

L’IA peut générer des renseignements qui sont:

- Incorrects
- Obsolètes
- Incomplets
- Fondés sur une juridiction erronée
- Présentés sans contexte pertinent
- Entièrement fabriqués

Cela revêt une importance particulière lorsque le personnel a recours à l’IA pour trouver des informations sur les procédures judiciaires, les programmes gouvernementaux, les services communautaires ou l’aide aux survivantes.

Par exemple, l’IA peut fournir avec certitude:

- Une procédure judiciaire incorrecte
- Une exigence légale obsolète
- Un dossier ou une ressource qui n’existe pas
- Des critères d’admissibilité erronés
- Des informations concernant un service qui n’existe plus

## 4. L’IA peut donner un faux sentiment de certitude ou de sécurité

L’IA peut générer des recommandations, des classifications, des résumés ou des classements qui semblent objectifs. Elles ne sont pas nécessairement objectives, exactes ou pertinentes.

L'IA ne devrait pas juger de manière autonome:

- Si une survivante est en danger
- Si une personne remplit les conditions pour bénéficier d'un service
- Qui devrait bénéficier d'une place dans une MH
- Qui doit être prioritaire sur une liste d'attente
- La crédibilité du témoignage d'une survivante
- L'efficacité d'un plan de sécurité
- Les interventions auprès des survivantes

Les décisions prises au service des survivantes nécessitent un jugement humain, la prise en compte du contexte, une expérience de terrain, une compréhension culturelle, une expertise professionnelle et le respect de l'autonomie des survivantes.

## Éléments à prendre en compte lors de la réflexion sur l'utilisation de l'IA dans le travail antiviolence

Avant d'utiliser un service d'IA ou de mettre en place un outil d'IA, les organisations doivent en comprendre les:

- Pratiques en matière de conservation des données
- Procédures de suppression
- Pratiques de sauvegarde
- Emplacements de stockage des données
- Contrôles d'accès
- Utilisations secondaires des informations
- Pratiques d'entraînement ou d'amélioration des modèles
- Sous-traitants et prestataires de services tiers

Lorsque vous examinez les politiques et les informations énumérées ci-dessus, veillez à prendre en compte les éléments suivants:

- Quelle législation en matière de protection de la vie privée s'applique à nous?
- Quelles données personnelles seraient saisies dans l'outil?
- L'utilisation de l'IA est-elle nécessaire à cette fin?
- Sur quelle base légale pouvons-nous collecter, utiliser ou divulguer des informations?
- Où ces informations sont-elles stockées ou traitées?
- Qui peut y accéder?
- Combien de temps ces données sont-elles conservées?
- Les données servent-elles à entraîner, améliorer ou développer de toute autre manière le système d'IA?
- Est-il possible de supprimer définitivement ces informations, et pas seulement de les effacer de notre système tout en les conservant sur un serveur?
- Qu'advient-il des sauvegardes?
- Que se passe-t-il si le prestataire est victime d'une violation de données?
- Quelles sont les garanties contractuelles prévues?
- Peut-on supprimer les informations que l'on a saisies?
- Avons-nous procédé à une évaluation adéquate de la confidentialité et de la sécurité?
- Cet outil répond-il à nos exigences en matière de confidentialité et de sécurité?

Les organisations devraient également se demander si les consignes ou les contenus générés par l'IA pourraient être intégrés aux archives de l'organisation et, par conséquent, soumis aux obligations applicables en matière d'accès, de conservation, de conformité juridique ou de divulgation.

**Demandez-vous: «L'utilisation de cet outil en particulier est-elle appropriée, nécessaire, autorisée et conforme aux obligations légales et de confidentialité de notre organisation?»**

N'oubliez pas: «anonyme» ne signifie pas toujours anonyme.

## Utilisations à haut risque de l'IA dans la promotion des droits des survivantes

En règle générale, ne saisissez pas d'informations concernant les survivantes, les clientes ou les dossiers dans des outils d'IA publics ou non approuvés. Cela comprend des informations concernant:

- Les survivantes
- Les enfants et les jeunes
- Les partenaires ou ex-partenaires
- Les membres de la famille
- Les amis ou d'autres personnes proches d'une survivante
- Les bénévoles ou le personnel, lorsque les informations sont confidentielles

Les données à caractère personnel peuvent aller bien au-delà du simple nom d'une personne.

Évitez d’entrer:

- Adresses ou lieux
- Lieux de travail ou établissements scolaires
- Numéros de téléphone ou adresses courriel
- Dates de naissance
- Numéros de dossier ou de procédure juridiques
- Études de cas
- Informations concernant les abus ou la violence
- Problèmes de sécurité
- Informations concernant les enfants
- Informations relatives à la santé ou à la santé mentale
- Informations financières
- Informations sur l’immigration ou juridiques
- Informations permettant d’identifier une personne même si son nom a été supprimé

Une description peut tout de même permettre d’identifier une personne lorsqu’elle est associée à d’autres éléments.

Par exemple: «Rédiger une note de consultation concernant mon rendez-vous d’aujourd’hui avec Jane. Elle est confrontée à des problèmes de santé mentale et la question du logement pour ses trois enfants» ne devrait pas être traité par un outil d’IA.

Mais le fait de supprimer «Jane» ne rend pas pour autant automatiquement la consigne sécuritaire. Par exemple: «Rédiger une note concernant une survivante de 37 ans vivant dans une petite communauté nordique, mère de

trois enfants, souffrant de dépression et hébergée actuellement à [nom de la MH]».

La combinaison de ces éléments pourrait tout de même permettre d'identifier la personne.

Les organisations devraient interdire ou contrôler rigoureusement l'utilisation de l'IA pour les activités impliquant des informations confidentielles sur les survivantes, notamment:

- **Documentation du cas**
    - Notes de dossier
    - Dossiers clientes
    - Rapports d'incident
    - Sommaires de cas
- **Communications des survivantes**
    - Courriels
    - SMS
    - Lettres contenant des informations personnelles
- **Sécurité et risques**
    - Plans de sécurité
    - Évaluations des risques
    - Évaluations des dangers
    - Évaluations des menaces
- **Décisions relatives aux services**
    - Décisions d'admissibilité
    - Priorité d'accès aux services
    - Détermination des niveaux de risque
    - Décider qui bénéficie de ressources limitées

- **Rencontres et discussions avec des survivantes ou à leur sujet**
    - Transcription ou prise de notes lors de réunions par l'IA
    - Résumés de réunions générés par l'IA
- **Informations d'ordre juridique ou relatives aux procédures judiciaires**
    - Histoire de cas de survivantes
    - Documents judiciaires contenant des informations à caractère personnel
    - Correspondance juridique
    - Résumés de la situation juridique d'une survivante

**Une règle simple: Si vous ne partageriez pas ces informations avec un tiers non lié à votre organisation ou si vous souhaitez que l'entreprise d'IA soit citée à comparaître pour les fournir, ne les saisissez pas dans un outil d'IA, sauf si votre organisation a expressément évalué et autorisé cette utilisation.**

Si l'IA venait à être utilisée dans un processus susceptible d'avoir un impact significatif sur une survivante, l'organisation devrait disposer de mesures de protection claires, d'un contrôle humain efficace et d'un moyen d'identifier et de corriger les erreurs. Les recommandations canadiennes en matière de protection de la vie privée mettent l'accent sur l'évaluation de la nécessité, la proportionnalité, la validité et la fiabilité des utilisations de l'IA générative, en particulier lorsqu'elles sont susceptibles d'avoir un impact significatif sur les personnes.

## Utilisations de l’IA présentant moins de risques

Une approche axée sur la réduction des méfaits n’implique pas nécessairement que les organisations interdisent toutes les fonctionnalités basées sur l’IA.

Les utilisations présentant un risque moindre peuvent inclure des tâches portant sur des informations non confidentielles, non personnelles et ne permettant pas d’identifier une survivante ni sa situation.

Par exemple:

- Modifier un document destiné au grand public, tel que votre site web ou une brochure
- Améliorer sa grammaire
- Résumer un document non confidentiel
- Réfléchir à des idées générales
- Traduire des informations non identifiables
- Rédiger des communications professionnelles générales
- Créer des communications professionnelles générales
- Créer des contenus de formation générale
- Réfléchir sur la formulation d’une demande de subvention ne contenant aucune information relative aux survivantes

## Politiques et pratiques de l’organisation

L’adoption de l’IA doit relever d’une décision organisationnelle. Toute organisation utilisant l’IA devrait établir des règles claires à l’intention de son personnel.

Les politiques devraient aborder les points suivants:

- **Le processus d'examen et d'approbation des outils d'IA**
    - Exiger la réalisation d'une évaluation appropriée de la protection de la vie privée et de la sécurité avant l'adoption de nouveaux outils d'IA et préciser qui, au sein de l'organisation, se chargera de mener cette évaluation.
    - Avant d'adopter un outil d'IA, examiner les conditions générales du fournisseur, les accords de confidentialité, les modalités de traitement des données, les pratiques de conservation et les mesures de sécurité à l'aide des questions énumérées dans les sections précédentes du présent document.
- **Utilisations et outils autorisés**
    - Déterminez quels outils d'IA, le cas échéant, sont autorisés au sein de l'organisation.
    - Déterminez à quels types de tâches ces outils peuvent servir et ce qu'il faut éviter.
- **Informations et tâches interdites**
    - Identifiez clairement les informations qui ne doivent en aucun cas être saisies dans les systèmes d'IA.
    - Interdire le recours à l'IA pour prendre des décisions concernant l'admissibilité des survivantes, les risques, l'ordre de priorité ou les services
- **Formation**
    - Veillez à ce que le personnel comprenne à la fois les avantages et les risques liés à l'IA et sache comment réagir en cas de doute.
- **Réponse aux incidents**

    - Mettez en place une procédure claire pour signaler et traiter les violations présumées de la vie privée, les divulgations accidentelles ou toute utilisation inappropriée de l'IA.
- **Révision périodique**
    - Les outils d'IA et leur terminologie peuvent évoluer. Examiner et approuver régulièrement les outils et les politiques de l'organisation.

## 1. Se méfier des fonctionnalités d'IA intégrées aux logiciels courants

L'IA ne se limite plus aux chatbots autonomes. Elle peut être intégrée à des outils que nous utilisons déjà dans notre travail, tels que:

- Courriel
- Logiciel de traitement de texte
- Stockage dans le nuage
- Plateformes de visioconférence
- Outils de transcription
- Logiciel de planification
- Systèmes de service à la clientèle
- Moteurs de recherche
- Téléphones et systèmes d'exploitation

De ce fait, on peut facilement passer à côté de l'utilisation de l'IA. «Cela fait déjà partie de notre logiciel» ne signifie pas pour autant que son utilisation pour des informations confidentielles soit automatiquement autorisée. Les organisations devraient identifier les cas où l'IA est intégrée aux technologies

qu'elles utilisent déjà et évaluer ces fonctionnalités dans le cadre de leurs pratiques en matière de confidentialité et de sécurité.

## 2. Que faire en cas de saisie accidentelle d'informations confidentielles

Ne partez pas du principe qu'il n'y a rien à faire. Si quelqu'un saisit par inadvertance des informations confidentielles ou personnelles dans un outil d'IA:

1. Cessez d'utiliser cet outil pour ces informations.
2. N'essayez pas de dissimuler cette erreur.
3. Informez la personne compétente au sein de votre organisation, par exemple votre responsable de la protection des données, votre directrice générale ou la personne désignée pour les enjeux de protection des données.
4. Respectez les procédures de votre organisation en matière de violation de la confidentialité et de gestion des incidents.
5. Consignez ce qui s'est passé, en précisant notamment quelles informations ont été saisies, quel outil a été utilisé, à quel moment cela s'est produit et quelles mesures ont été prises.
6. Si nécessaire, demandez conseil à une spécialiste de la protection de la vie privée.

Les autorités de contrôle de la protection des données fournissent des conseils et des ressources aux organisations confrontées à des violations de la vie privée. La réponse appropriée peut dépendre des informations concernées, de l'organisation, de la législation applicable et du service d'IA en question.

# Résumé

L'IA peut être utile au travail, mais la commodité ne constitue pas une raison suffisante pour exposer les informations relatives aux survivantes à un système technologique tiers.

Les organisations antiviolence doivent prendre en compte la vie privée, la confidentialité, les obligations légales, la sécurité des survivantes et la responsabilité organisationnelle lorsqu'elles décident s'il convient d'utiliser l'IA et, le cas échéant, comment l'utiliser.

Une approche axée sur la protection de la vie privée n'implique pas que le personnel doive craindre la technologie. Cela exige des organisations qu'elles comprennent la technologie utilisée, évaluent les risques, fixent des limites claires et placent les personnes, et non la technologie, au cœur de la promotion des droits des survivantes.

*La violence fondée sur le genre facilitée par la technologie (VFGFT) s'inscrit dans un continuum qui peut se manifester aussi bien en ligne qu'en personne. Si vous ou quelqu'un que vous connaissez êtes la cible de VFGFT, sachez qu'il existe de l'aide. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin d'explorer vos options et d'élaborer un plan de sécurité. Il n'est pas nécessaire de séjourner dans une maison d'hébergement pour bénéficier de services et d'un soutien gratuits et confidentiels.*