La cyberviolence au travail : un risque bien réel

Rachel Dupuis
rdupuis@asstsas.qc.ca

Daisy Gauthier
dgauthier@asstsas.qc.ca

La cyberviolence est un risque qui se rattache à celui de la violence. Harceler, menacer ou intimider en utilisant les technologies numériques ou le Web sont autant de formes qu'elle peut revêtir. La cyberviolence se déploie dans plusieurs espaces sociaux. Dans les milieux de travail, elle met en péril la santé et la sécurité du personnel.

La cyberviolence en milieu de travail renvoie à des gestes violents adressés à une ou à plusieurs personnes. Il s'agit de pratiques numériques qui portent atteinte à l'intégrité physique, psychique ou professionnelle. Cette violence peut être psychologique, verbale, écrite, sexuelle, économique ou physique. Elle s'inscrit sur un continuum allant de formes mineures à d'autres plus insidieuses et graves, comme le harcèlement en ligne, l'envoi de messages abusifs, la diffusion de rumeurs diffamatoires, le vol de données confidentielles, le partage non consensuel d'images ou de vidéos compromettantes.

Ces comportements violents peuvent entraîner des conséquences nombreuses, notamment sur les plans psychique, comportemental et physique, comme du stress, de l'anxiété, de la dépression, de l'absentéisme, de l'isolement et des troubles du sommeil. Ces effets détériorent le bien-être émotionnel et génèrent une baisse de la productivité, de l'engagement, de la satisfaction au travail.

Ignorer la cyberviolence ou ne pas réagir correctement face à elle peut créer un climat de travail toxique et augmenter les risques de conflits au sein d'une équipe.

Au programme de prévention

La cyberviolence équivaut à la violence, elle requiert donc les mêmes mécanismes de prévention. La promotion d'un environnement de travail sain, exempt de toutes formes de violence, passe par un mode de gestion engagé dans la prise en charge de la SST. Une politique et des procédures pour contrer la violence doivent être mises en place et communiquées au personnel. Elles doivent définir les notions de violence et les concepts qui lui sont relatifs. Elles devraient donc contenir une définition de la cyberviolence et des pratiques numériques violentes. De cette manière, il devient possible d'identifier les comportements nuisibles.

Au sujet des procédures, elles demeurent les mêmes : inspection préventive de l'environnement, intervention de crise, appel, déclaration d'événement accidentel, etc. En raison de la voie technologique empruntée par la cyberviolence, il importe d'ajouter une procédure de cybersécurité intégrée aux outils numériques utilisés à l'interne. Des mesures de sécurité doivent être mises en place pour protéger, entre autres, les informations sensibles du personnel. Cela peut inclure des protocoles de sauvegarde réguliers, des mots de passe robustes, des systèmes de pare-feu, ainsi que des formations sur la gestion sécurisée des données.

Il est essentiel de sensibiliser le personnel aux risques de la cyberviolence et de l'informer sur les mesures de prévention. Des sessions de formation complémentaire à celles traitant de prévention et d'intervention face à la violence traditionnelle doivent être offertes. Elles devraient viser le développement des compétences en matière de cybersécurité, promouvoir le respect et l'empathie en ligne et encourager des pratiques numériques responsables.

Photo : iStock

FORMES DE VIOLENCE

PSYCHOLOGIQUE → Vise à contrôler, à manipuler ou à nuire sur le plan émotionnel et mental. Ex. : critiquer constamment une personne, la faire douter d'elle-même, la manipuler sur le plan émotif, l'isoler socialement, etc.

VERBALE → Se manifeste par des paroles, par des mots ou des expressions destinés à nuire, à humilier, dévaloriser ou contrôler une autre personne. Ex. : recourir au sarcasme (complimenter avec l'intention d'exprimer le contraire), insulter, tenir des propos dégradants ou humiliants, etc.

ÉCRITE → Se produit à travers l'écriture de messages, de courriels, de textos ou de publications – souvent numériques – visant à nuire, à humilier, dévaloriser ou harceler. Ex. : écrire de manière privée ou publique des insultes et des menaces, envoyer des messages de façon répétée, publier des rumeurs ou des commentaires désobligeants en ligne, etc.

SEXUELLE → Implique l'utilisation de la force, de la coercition, de la manipulation ou de la menace pour contraindre une personne à participer à des activités sexuelles non consenties. Elle peut inclure des actes physiques ou non. Ex. : envoyer par messagerie des contenus à caractère sexuel sans consentement (nudité, pornographie), frotteurisme (frotter, toucher, frôler les parties génitales ou les seins d'une personne), exhibitionnisme, voyeurisme, etc.

ÉCONOMIQUE → Se caractérise par le contrôle, la manipulation ou l'exploitation des ressources financières d'une personne pour en abuser ou exercer un pouvoir et un contrôle sur elle. Ex. : extorquer de l'argent, obliger une personne à verser des montants ou à payer des dépenses qui ne lui appartiennent pas, voler des cartes de crédit ou de débit, emprunter des sommes au nom d'une personne sans son consentement, etc.

PHYSIQUE → Implique l'utilisation de la force physique pour causer des dommages, des blessures ou de la douleur à une personne, un groupe, des objets, des animaux ou des lieux. Bien qu'il s'agisse de l'une des formes les plus visibles et les plus directes de violence, il n'est pas rare que les personnes qui en sont la cible trouvent des stratégies pour camoufler leurs blessures. Ex. : donner un coup de poing sur la table, rouer de coups une personne, filmer l'agression et mettre la vidéo en ligne, etc.

N.B. Une situation peut présenter plus d'une forme de violence. Ex. : menacer une personne de partager ses photos intimes en échange d'argent. Il s'agit ici de violence sexuelle et économique.

Comme pour tous les risques, il faut favoriser une communication ouverte avec le personnel et contrer la sous-déclaration. Les personnes doivent se sentir à l'aise de déclarer un événement accidentel. Il est important de les encourager à signaler tout incident de cyberviolence à leur gestionnaire, sans crainte de représailles. Pour ce faire, il faut prendre au sérieux les préoccupations du personnel et appliquer rapidement des mesures pour corriger les risques.

Histoire de Johana

MISE EN SITUATION

Johana est une infirmière à l'urgence d'un centre hospitalier. Vers la fin de son quart de travail, le fils d'une patiente se présente au chevet de sa mère. Insatisfait des soins qu'elle a reçus, il se rend au poste. Il brandit son cellulaire, filme Johana, l'insulte en hurlant et la menace de mettre les images sur les médias sociaux.

ACTIONS À POSER

La priorité est d'assurer la sécurité de Johana et de toutes les personnes en présence. Comme le risque est immédiat, il devient crucial de recourir aux protocoles prévus en cas d'exposition à de la violence, comme les procédures de gestion de crise (code blanc) et d'appel. Johana ou toute autre personne formée à l'intervention en situation de violence (ex. : *Programme Oméga travailleurs*) devrait recourir à son savoir et ses compétences pour assurer sa sécurité, comme garder une distance sécuritaire et pacifier.

Photo : iStock

Les organisations peuvent réduire les risques d'exposition à la cyberviolence en bonifiant leur programme actuel de prévention de la violence.

Si le fils de la patiente se calme, la personne qui intervient pourrait lui demander calmement de fermer le cellulaire ou de cesser d'enregistrer. S'il refuse et recommence à s'agiter, elle doit prévoir un repli stratégique pour se mettre en sécurité.

Immédiatement après, Johana devra utiliser les mécanismes de déclaration d'événement accidentel. Pour documenter l'incident, elle le détaillera et recueillera des preuves, le cas échéant. Elle remplira le formulaire à cet effet et informera sa gestionnaire. Advenant qu'elle apprenne qu'une vidéo compromettante circule à la suite de cet événement, elle devra tenter d'archiver l'information (copie de la vidéo, capture d'écran, etc.) pour soutenir l'enquête et l'analyse.

Des mesures correctives immédiates doivent être mises en place. Il faut notamment s'assurer que le fils de la patiente n'est plus en mesure de nuire. Un service de raccompagnement pour quitter les lieux de travail peut être offert aux personnes ciblées. Si vous avez un service des communications dans votre organisation, il pourrait répondre de manière appropriée à la menace de diffusion de la vidéo. Si la situation le justifie, il peut être nécessaire d'impliquer les autorités compétentes.

En cas d'atteinte à l'intégrité, il est impératif d'apporter rapidement les premiers soins à Johana ou à tout autre membre du personnel affecté par la situation. Il est tout aussi important d'offrir un soutien psychologique et émotionnel. Par exemple, en les dirigeant vers des services de soutien psychologique (ex. : programme d'aide aux employés).

Par la suite, une enquête et une analyse de l'événement accidentel permettront de prendre des mesures préventives appropriées et d'en assurer la pérennité.

Cyber et bien réelle

L'exposition à la cyberviolence en milieu de travail est un problème qui doit être pris au sérieux. En raison de son caractère parfois insidieux et de la pluralité des pratiques numériques violentes, la cyberviolence paraît souvent peu tangible et difficile à prévenir. Toutefois, les organisations peuvent réduire les risques d'exposition à la cyberviolence en bonifiant leur programme actuel de prévention de la violence. Et n'oubliez pas : le préfixe « cyber » ne rend pas moins réelle cette violence ! ■

PRATIQUES NUMÉRIQUES VIOLENTES

PRATIQUE		DÉFINITION
Happy slapping (*Joyeuse baffe*)	→	Diffuser des images ou vidéos d'une agression
Lynchage	→	Détruire ou ternir l'image d'une personne
Flaming (*Embraser*)	→	Envoyer des messages grossiers à un individu ou à un groupe
Stalking (*Traquer*)	→	Suivre, surveiller
Mobbing (*Harcèlement psychologique*)	→	Intimider, dénigrer ou exclure socialement une personne en groupe
Trolling (*Provoquer*)	→	Générer des conflits en ligne par des messages provocateurs
Usurpation d'identité	→	Voler l'identité d'une personne et publier des messages, commentaires ou autres en son nom
Divulgation d'information privée	→	Publier des photos ou des extraits de correspondance, sans consentement
Photoshopping	→	Utiliser un logiciel (non exclusivement Photoshop) pour transformer les photos d'une personne de manière humiliante avant de les publier