ONTHELINE NEWSROOMS
DEFENDING PRESS FREEDOM

Protocole à l'attention des rédactions pour aider les journalistes victimes de cyber-harcèlement

International Press Institute (IPI)

PROTOCOL TO ADDRESS ONLINE HARASSMENT

Introduction

Le cyber-harcèlement et les attaques visant les journalistes (menaces, insultes et campagnes de diffamation) sont de plus en plus utilisés comme un moyen de faire taire les journalistes et de remettre en cause leur crédibilité dans l'espace public. Si la gestion du cyber-harcèlement et son impact négatif sur la libre circulation d'informations exigent une approche multi-acteurs, les rédactions jouent un rôle clé dans la protection de leurs journalistes des dangers professionnels et personnels engendrés par le harcèlement. Le présent protocole définit des étapes et des mesures que les rédactions peuvent adopter.

Les mesures présentées dans le présent protocole reposent sur des données recueillies par l'IPI au cours de visites dans 45 rédactions de cinq pays européens (Finlande, Allemagne, Pologne, Espagne et Royaume-Uni) entre avril et décembre 2018, ainsi qu'au cours de rencontres avec des experts de différents pays. Au total, IPI a interviewé plus de 110 rédacteurs, journalistes et community managers ainsi que des experts juridiques, des représentants de la société civile et de l'éducation. Lors des visites sur place, huit groupes de réflexion avec des femmes journalistes et des freelances ont été établis pour discuter de l'impact du cyber-harcèlement sur ces groupes en particulier.

Le présent protocole, partie intégrante de l'initiative Newsrooms Ontheline de l'IPI, n'a pas vocation à être une solution universelle. Il a pour objectif de poser les bases afin que les rédacteurs/trices en chef mettent au point un système adapté à leur propre situation et pouvant fonctionner à long terme.

Table des matières

Étape 1 : Signalement

a. Instaurer une culture de sécurité dans la rédaction concernant le cyber-harcèlement
a. Établir des hiérarchies et des canaux de signalement clairs
a. Documenter les cas d'attaques en ligne et de harcèlement

Étape 2 : Évaluation des risques

a. Risque de préjudice physique
a. Risque de préjudice psychologique
a. Risque d'atteinte à la réputation

Étape 3 : Mécanismes de soutien

a. Aide sécurité numérique
a. Aide juridique
a. Aide émotionnelle et psychologique
a. Congé temporaire, mutation et/ou réaffectation
a. Communiqué public de soutien
a. Modérer le cyber-harcèlement

Étape 4 : Suivi et réévaluation

Rôles et missions

- Coordinateur/coordinatrice cyber-sécurité
- Direction
- Rédacteurs/rédactrices
- Modérateurs/modératrices
- Journalistes

Étape 1 : Signalement

a Instaurer une culture de sécurité dans la rédaction concernant le cyber-harcèlement

La direction doit prendre toutes les mesures nécessaires à la compréhension des types d'attaques auxquelles sont confrontés leurs équipes et leurs contributeurs/trices et à la normalisation du dialogue entourant ces attaques.

- **Mémo interne :** envoyer un e-mail à toute l'équipe établissant clairement que l'organe de presse prend les attaques en ligne au sérieux. Cette mesure est capitale pour accroître la confiance au sein de la rédaction. Elle envoie deux messages importants : d'une part, cela combat l'impression bien ancrée chez les journalistes que l'abus sur les réseaux sociaux est la nouvelle norme et leur donne d'autre part un sentiment de sécurité en les assurant que l'organe de presse les soutiendra.

- **Évoquer régulièrement le cyber-harcèlement lors des réunions de la rédaction :** pour aborder ce problème, les rédacteurs/rédactrices peuvent demander de manière informelle si des journalistes ont été visés récemment et sensibiliser aux dangers de ces attaques lorsqu'ils assignent des sujets susceptibles d'attirer des abus. Ces discussions doivent devenir plus fréquentes en cas de crise politique, de troubles sociaux ou avant des élections.

- **Distribuer une enquête anonyme** dans la rédaction pour examiner l'impact du cyber-harcèlement et l'efficacité des mesures en place pour y faire face.

> *Le site d'informations espagnol publico.es a mené une enquête auprès de son personnel pour mesurer l'impact des attaques sur l'équipe et l'efficacité des mesures mises en place.*

- **Prévoir des réunions régulières avec les équipes réseaux sociaux et les journalistes** pour réaliser un « **bilan de santé** » concernant le travail des journalistes sur les réseaux sociaux ou l'engagement dans les commentaires.

- **Créer une section facile d'accès** dans l'intranet du service de presse contenant des informations sur la politique de l'entreprise en matière de cyber-harcèlement, ainsi que les outils et protocoles créés par l'entreprise pour gérer ce problème.

> *L'intranet de la BBC propose des films à visée pédagogique dans lesquels des journalistes parlent de traumatismes vécus sur le terrain et de leur impact. Les films font office de guide pratique sur le sujet du traumatisme et aident à démystifier ce problème.*

b Établir des hiérarchies et des canaux de signalement clairs

Tous les membres de l'équipe et les contributeurs/trices doivent savoir à qui et comment signaler une attaque. Les rédactions doivent créer différents canaux permettant de signaler facilement ces attaques et donnant accès à des mécanismes de soutien aux journalistes.

Mécanismes de signalement informels :

- ***Encourager les discussions informelles entre collègues :*** les rédactions doivent encourager les journalistes à partager leurs expériences de harcèlement avec leurs pairs et rédacteurs/rédactrices. Il faut indiquer très clairement que parler ouvertement des attaques en ligne n'est pas un signe de faiblesse ou d'hyper-sensibilité.

- ***Créer un groupe de discussion*** sur WhatsApp, Messenger ou une plateforme similaire (Signal, Telegram, Threema, etc.) où les journalistes peuvent partager des incidents de harcèlement. Un espace de discussion commun peut sensibiliser à ce problème tout en renforçant le sentiment de solidarité et de communauté.

Mécanismes de signalement formels :

- ***Créer un formulaire en ligne*** où les journalistes visés peuvent facilement signaler une attaque. Ce formulaire doit être court et facile à remplir, tout en recueillant toutes les informations essentielles liées à l'attaque.

- ***Créer une adresse mail spéciale*** où les journalistes peuvent signaler un cas de cyber-harcèlement.

Les mécanismes de signalement formels entraînent l'attente d'une action. Il faut donc indiquer clairement aux journalistes, aux autres membres de l'équipe et aux contributeurs/trices qui est la personne recevant

ces signalements les mesures qu'elle peut prendre. Cette personne doit posséder des connaissances sur le sujet du harcèlement (dans l'idéal, elle y a été formée) et doit jouir d'une certaine position dans la rédaction qui lui permet de faire remonter les cas aux personnes en mesure de fournir une réponse au nom du service.

Que le cas nécessite d'être remonté ou non, les personnes ayant effectué le signalement doivent recevoir une réponse afin de certifier que leurs signalements sont entendus et de maintenir la crédibilité du mécanisme. Enfin, étant donné que les femmes et les minorités constituent une part disproportionnée des victimes de harcèlement, les rédactions doivent faire en sorte que les coordinateurs/trices des mécanismes de signalement comprennent des représentants de ces groupes ou aient été sensibilisés aux attaques spécifiques visant les femmes et les minorités.

c Documenter les cas d'attaques en ligne et de harcèlement

Cela signifie d'une part que les journalistes visés par des attaques doivent faire des captures d'écran de l'attaque et noter toute autre information pertinente. Une documentation suffisante est essentielle pour comprendre l'origine de l'attaque, pour procéder à l'analyse des risques et pour décider, le cas échéant, des mesures à mettre en œuvre. Compte tenu de la gravité de certaines attaques, il faut inciter les journalistes à déléguer une partie de la procédure de documentation à leurs collègues, rédacteurs/trices et modérateurs/trices.

D'autre part, les personnes responsables de la coordination des mécanismes de signalement doivent **créer une base de données afin de garder une trace des incidents de cyber-harcèlement** qu'on leur a rapportés et des informations concernant les réponses apportées. Cette base de données est importante pour garder une trace des mesures prises et de leur efficacité (cf. informations supplémentaires à l'étape 4).

Étape 2 : Évaluation des risques

Une évaluation des risques minutieuse est importante pour déterminer le type de soutien le plus adéquat en cas d'attaques en ligne. Il faut évaluer les types de risques suivants :

- La probabilité qu'une ***attaque en ligne devienne une attaque physique***.
- ***L'impact émotionnel potentiel*** sur les journalistes visés et l'impact sur leur travail.
- La probabilité qu'une campagne de diffamation en ligne ***nuise à la réputation et à la crédibilité*** du/de la journaliste et/ou du service de presse.

Les personnes impliquées dans l'évaluation des risques doivent recevoir une formation adéquate leur permettant de détecter la présence de critères particuliers et de comprendre quand faire remonter certains cas. Une sélection de facteurs pouvant servir à l'évaluation des risques se trouve ci-après. La procédure d'évaluation des risques devra également inclure les cibles des attaques.

a Risque de préjudice physique

Facteurs à examiner :

- Le cadre global de sécurité (fréquence des attaques physiques à l'encontre de la presse, impunité pour ce type d'attaques, climat d'animosité généralisée à l'encontre de la presse).
- En cas d'un agresseur unique, analyse des risques d'une attaque physique en fonction des informations que l'on possède sur cet individu.
- En cas de campagnes, probabilité que les individus se sentent encouragés ou légitimes pour exécuter une attaque physique.
- La nature publique du travail du/de la journaliste : est-il/elle reconnaissable dans des lieux publics ?

b Risque de préjudice psychologique

Facteurs à examiner :

Éléments externes

- Intensité du harcèlement, à la fois en termes de contenu et de fréquence (un harcèlement « de bas niveau » mais fréquent peut être nocif).
- La présence de contenu discriminatoire (relevant du genre, de l'origine ethnique, de l'orien-

tation sexuelle, etc.) peut avoir un impact particulièrement grave sur la personne visée.

- Présence d'images traumatisantes.
- Messages révélant un comportement de harcèlement pouvant générer un sentiment de peur et d'insécurité.
- Solidité du réseau de soutien global de la personne visée.

Éléments internes

- Santé mentale de la personne visée : signes de dépression ou de traumatisme.

c Risque d'atteinte à la réputation

Facteurs à examiner :

- Degré de clivage et d'hostilité envers les médias dans la société.
- Probabilité que la diffamation soit crédible aux yeux du public.
- Volume et portée des attaques et des campagnes de diffamation, y compris tout facteur pouvant accélérer la diffusion des attaques comme :
  - L'utilisation de *memes* ou de créations graphiques élaborées.
  - L'utilisation de botnets.
  - L'utilisation de termes et de calomnies pouvant être réutilisés à l'avenir.
  - Le relais de l'attaque par des sites de désinformation.
  - Tout indice portant à croire que les campagnes de diffamation ont été orchestrées pour le compte d'intérêts politiques, économiques ou autres.

Cette liste de facteurs n'est pas exhaustive. Il est fortement recommandé aux rédactions d'investir dans une formation professionnelle afin d'être en mesure d'identifier les risques physiques, les risques de traumatisme émotionnel et les risques d'atteinte à la réputation, y compris les signes révélant des campagnes de diffamation organisées.

Étape 3 : Mise en place de mécanismes de soutien

Cette partie fournit un aperçu des mécanismes de soutien possibles lorsque des journalistes sont visés par des attaques en ligne ou harcelés. Tous ces mécanismes ont pour but de garantir que les journalistes visés puissent travailler en toute sécurité.

a Aide sécurité numérique

Cela peut par exemple comprendre :

- ***Localiser les utilisateurs derrière les attaques*** même s'ils ont posté leurs menaces depuis des comptes anonymes sur les réseaux sociaux.
- ***Bloquer tous les comptes des cibles***, changer les mots de passe, etc. pour minimiser les risques.
- ***Les rédacteurs/trices et collègues devraient proposer*** aux personnes visées de prendre en charge leurs réseaux sociaux afin qu'elles ne soient pas exposées à davantage d'attaques.

Mesures préventives :

- ***Informer les journalistes de leurs détails personnels*** accessibles au public via les comptes de réseaux sociaux. Vérifier si des informations sensibles ont été exposées involontairement.
- ***Former les journalistes à analyser leurs appareils électroniques*** pour identifier d'éventuelles failles qui pourraient permettre à des hackers d'accéder à leurs données personnelles et de les divulguer.

b Aide juridique

La décision de saisir ou non la justice en réaction au cyber-harcèlement doit être fondée sur un certain nombre de facteurs. Ces derniers comprennent :

- La présence dans les posts de contenu jugé illégal dans votre juridiction.

- La probabilité que la saisie d'un tribunal dissuade les futurs agresseurs en ligne de façon générale.
- La probabilité que la saisie d'un tribunal dissuade l'agresseur en question dans ce cas précis.
- La possibilité, en fonction du contexte, qu'intenter une action en justice braque l'attention sur le/la journaliste concerné/e, amplifiera et encouragera d'autres attaques.
- La possibilité qu'une action en justice renforce les éventuels dires des agresseurs sur les médias « puissants » qui s'en prennent aux « plus faibles » et ajoute éventuellement au harcèlement.
- Le fait que l'attaque ait été commise par un individu agissant seul ou participant à une campagne en règle. Dans ce dernier cas, une action en justice pourrait s'avérer contre-productive et exacerber les attaques futures.
- L'impact éventuel sur le/la journaliste visé/e : une action en justice donnera-t-elle satisfaction au/à la journaliste visé/e ou causera-t-elle encore plus de souffrance psychologique ?
- Le cas échéant, le fait que les procureurs aient également engagé des poursuites pénales, auquel cas l'effort serait plus facile à soutenir.

RESSOURCES COMPLÉMENTAIRES : Le site Internet Newsrooms Ontheline de l'IPI présente une **série de vidéos** récapitulant les éléments à prendre en compte si vous envisagez **intenter une action en justice**

C Aide émotionnelle et psychologique

Aide psychologique professionnelle

Une aide psychologique professionnelle peut jouer un rôle important dans la gestion des conséquences d'attaques en ligne et du harcèlement des journalistes. Les organes de presse doivent faire en sorte que leurs journalistes aient accès à des soins de santé mentale, soit par le biais de la couverture santé de l'entreprise, soit par le biais d'arrangements ad hoc conclus entre l'entreprise et des professionnels de la santé mentale.

Soutien par les pairs

Avoir des collègues au vécu similaire peut être source de réconfort pour les journalistes visés par des abus ou du harcèlement en ligne, tout comme profiter de conseils sur la meilleure façon de faire face à ces attaques et leurs conséquences éventuelles.

- ***Réseaux structurés d'entraide par les pairs*** **:** développer un réseau formel de membres de la rédaction disposés à écouter leurs collègues visés par des attaques en ligne et à leur expliquer comment gérer les conséquences. Dans l'idéal, les membres du personnel participant à ces programmes doivent suivre une formation spécifique pour apprendre à reconnaître un traumatisme grâce à des conversations structurées et être capable de référer les journalistes aux personnes compétentes au sein de la rédaction qui pourront mettre en place un soutien psychologique ou d'autres types de soutien (conseil juridique, modération d'audience, sécurité numérique et autres mécanismes de sécurité).

  > *Consultez l'analyse poussée de Dart Center sur le réseau d'entraide par les pairs et sa mise en œuvre sur l'Australian Broadcasting Corporation.*
  >
  > *Découvrez le réseau d'entraide par les pairs de la BBC.*
  >
  > *Découvrez le réseau d'entraide par les pairs de Reuters.*

- ***Programmes de parrainage*** **:** chargez un/e journaliste senior de parrainer des collègues moins expérimentés. Les mentors devraient aider leurs protégés à reconnaître les attaques en ligne, les sujets qui les provoquent généralement et les formes qu'elles peuvent prendre.
- ***Un groupe de discussion*** sur WhatsApp, Messenger ou une application similaire peut servir à signaler des menaces et à offrir de l'aide en cas d'attaques.
- ***Conversations régulières*** **:** les rédacteurs/trices doivent créer des occasions pour évoquer le cyber-harcèlement en groupe. Exemples :
  - Une « pause café » permettant aux journalistes de la rédaction ou issus d'autres organes de presse de partager leurs expériences en matière de cyber-harcèlement autour d'un café. Ces « experts par expé-

rience » peuvent offrir un point de vue et des conseils précieux pour « briser la glace » lorsqu'il s'agit de discuter du cyber-harcèlement ouvertement.

- Saper le pouvoir du cyber-harcèlement avec humour. Par exemple, les cibles des attaques peuvent afficher les commentaires reçus sur un mur. Les lire à voix haute avec des collègues ou en rire peut avoir un effet cathartique. Des rédactions ont rapporté que ce genre de mesures peut aider à atténuer l'anxiété et la tension et, dans certains cas, à prendre du recul sur les attaques.

Mesures de préservation pour journalistes (« self-care »)

Outre les mesures proposées par les rédactions et autres organismes, il faut inciter les journalistes à mettre en place des mesures pour se préserver (« self-care ») afin de minimiser le risque d'un traumatisme à long terme causé par un cyber-harcèlement aggravé.

RESSOURCES COMPLÉMENTAIRES : Le site Internet Newsrooms Ontheline de l'IPI présente une **série de vidéos sur les stratégies de gestion du cyber-harcèlement**

d Congé temporaire, mutation et/ou réaffectation

Un congé temporaire s'appuyant sur un examen de la détresse psychologique du/de la journaliste visé/e peut minimiser le traumatisme potentiel. Accorder un congé dans de telles situations est une pratique courante dans les rédactions, notamment dans les services fréquemment exposés à des contenus violents ou extrêmement stressants comme ceux qui travaillent avec l'UGC (contenu généré par les utilisateurs).

> *Le journal finlandais Turun Sanomat a muté une de ses journalistes de Turku (environ 250 000 habitants) à la capitale Helsinki après qu'une série de menaces en ligne s'est ensuivie de menaces réelles dans la rue. Elle aurait effectivement beaucoup moins de chances d'être reconnue dans une grande ville.*

e Communiqué public de soutien

Pour le service de presse, afficher son soutien public à un/e journaliste attaqué/e est une façon de montrer que l'entreprise défend son équipe et considère toute attaque envers ses journalistes comme une attaque sur l'institution toute entière. Toutefois, selon les cas, il faudra peut-être faire profil bas pour éviter d'attirer l'attention sur le/la journaliste, ce qui pourrait encourager d'autres attaques. Les critères suivants permettront de décider s'il convient de publier un communiqué de soutien :

- Est-ce que cela amplifiera l'attaque ?
- Est-ce que cela accroîtra le harcèlement ?
- Est-ce que cela pourrait nuire à une éventuelle action en justice ?

f Modérer le cyber-harcèlement

Une stratégie approfondie et bien pensée de modération des commentaires est nécessaire pour garantir la suppression rapide d'attaques visant les journalistes et les organes de presse, ainsi que de tout commentaire inacceptable.

Empêcher le cyber-harcèlement

- ***Créer un règlement pour votre communauté ou une netiquette***, deux outils clés pour les utilisateurs et les modérateurs. Ces règles de participation établiront clairement que les critiques sont les bienvenues, mais que les insultes, attaques, discours haineux et menaces ne seront pas tolérés.

  > *Consultez le règlement et les consignes de participation du Guardian.*
  > *Consultez la netiquette de la Deutsche Welle.*

- ***Former une communauté :*** même si leur développement et maintenance prend du temps, les communautés en ligne sont cruciales dans la lutte contre le cyber-harcèlement. Les lecteurs bien intégrés à une communauté seront plus susceptibles de défendre l'organe de presse ou le/la journaliste ciblé/e en cas de diffamation ou de menaces sur les réseaux sociaux et dans les commentaires du média.

- ***Mettre en place un système d'inscription sur votre page :*** il est recommandé de demander aux utilisateurs de s'inscrire pour pouvoir commenter. C'est un critère important en matière

de responsabilité légale qui constitue également un premier obstacle pour dissuader les agresseurs et les comptes tenus par des robots.

- ***Autoriser les commentaires sur certains contenus :*** si les ressources disponibles pour la modération de commentaires sont limitées, il sera judicieux de n'autoriser les commentaires que sur certains contenus. Ce faisant, veillez à choisir différents thèmes pour garantir que votre communauté puisse exprimer son opinion sur un large spectre de sujets.

- ***Bloquer les commentaires à certains moments :*** si vous craignez de ne pas pouvoir modérer les discussions dans la nuit, pendant les week-ends ou à tout autre moment où les modérateurs ne peuvent pas accorder suffisamment de temps à cette tâche, vous pouvez bloquer l'option commentaires pour ce laps de temps. Dans ce cas, assurez-vous d'indiquer à votre lectorat à quel moment il pourra recommencer à poster des commentaires.

- ***Limiter la période ouverte aux commentaires :*** une autre stratégie consiste à accorder la possibilité aux utilisateurs de partager leurs opinions, mais pour un laps de temps limité afin de ne pas surcharger votre équipe.

- ***Régler des alertes pour surveiller l'activité des utilisateurs :*** parfois, des discussions restées longtemps silencieuses s'activent soudainement. Si vous ne souhaitez pas clore les commentaires, utilisez un système de notification pour avertir les modérateurs/trices de toute activité.

Modérer et réagir au cyber-harcèlement

Rappelez-vous que supprimer des attaques, menaces et insultes visant les journalistes n'élimine pas le risque de violence physique émanant de l'agresseur. Les modérateurs/trices qui repèrent des messages agressifs à l'encontre de journalistes (notamment ceux qui contiennent des menaces) doivent non seulement supprimer ces messages, mais aussi notifier les personnes compétentes au sein de l'organisation, y compris les cibles de ces attaques.

Commentaires sur un site :

- ***Supprimer les commentaires :*** les commentaires qui contiennent des menaces, des insultes ou d'autres attaques à l'encontre de journalistes doivent être étudiés minutieusement par les modérateurs/trices qui devront déterminer si le commentaire relève d'une critique légitime ou s'il enfreint le règlement de la communauté et doit par conséquent être supprimé. Toute décision de supprimer un commentaire attaquant un/e journaliste doit prendre en compte le contenu de l'attaque ainsi que la vulnérabilité du/de la journaliste. Il est conseillé d'indiquer aux utilisateurs les raisons ayant entraîné la suppression de leurs commentaires et les articles du règlement qu'ils ont enfreint.

- ***Avertir et bloquer les utilisateurs :***

  - ***Avertissez les utilisateurs qui enfreignent souvent le règlement de la communauté :*** une façon efficace d'avertir les utilisateurs qui enfreignent souvent le règlement de la communauté consiste à les empêcher de commenter pour un certain laps de temps. Si vous avez recours à cette mesure, veillez à ce que les utilisateurs reçoivent un message de votre part expliquant pourquoi vous avez pris cette décision.

  - ***Informer les utilisateurs de la suppression de leur compte :*** supprimer l'accès d'un utilisateur aux commentaires est une mesure sérieuse et une réponse appropriée aux agressions graves. Les utilisateurs dont les comptes ont été supprimés doivent recevoir un message expliquant cette décision.

- ***Participation des modérateurs/trices dans une conversation entre utilisateurs :*** les modérateurs/trices doivent procéder depuis le compte du service de presse et rappeler aux utilisateurs les consignes du règlement. La participation de journalistes aux discussions peut élever le niveau de la conversation mais ne doit pas leur être imposée — il faudra en outre étudier attentivement les risques qui en découlent.

Sur les plateformes de réseaux sociaux :

Les services de presse utilisent les réseaux sociaux pour élargir leur audience, générer des débats publics autour de certaines problématiques et, à terme, former une communauté. Les médias ont tendance à appliquer les mêmes règles sur les pages officielles de leurs réseaux sociaux que sur leurs propres forums de discussion, où les équipes de modération discutent avec le public et créent un écosystème pour un débat public sain avec et entre les utilisateurs.

Gérer le cyber-harcèlement sur Facebook :

- ***Effacer un commentaire*** au contenu agressif, menaçant, dénigrant ou insultant. Les critiques, même acerbes, doivent toutefois être autorisées.

- ***Masquer un commentaire*** au contenu abusif. Les modérateurs/trices estiment généralement que cette mesure est moins efficace que la suppression, car l'utilisateur et ses amis peuvent toujours voir le contenu en question, même s'il devient invisible pour les autres utilisateurs.

- ***Bannir un utilisateur de la page*** Facebook de l'organe de presse lorsque l'utilisateur a posté des commentaires haineux ou injurieux à plusieurs reprises, même près avoir reçu des avertissements. Cela sert à éliminer un utilisateur qui sape continuellement les valeurs d'une discussion ouverte.

- ***Supprimer un utilisateur de la page*** à titre d'avertissement pour dissuader d'autres commentaires injurieux. Porte moins à conséquence que le bannissement puisque l'utilisateur peut aimer ou suivre la page à nouveau.

- ***Désactiver/couper les commentaires*** bien que cette fonction ne soit disponible que sur les publications de vidéos. À appliquer lorsque l'équipe de modération ne possède pas les ressources nécessaires à la modération d'une vague de commentaires sur une vidéo ou une vidéo en direct.

- ***Bloquer certains*** mots et paramétrer le degré du filtre à injures.

- ***Signalez une publication ou une page*** qui enfreint à la fois le règlement de Facebook et celui de la communauté du média.

Gérer le cyber-harcèlement sur Twitter :

- ***Masquer (muter) :*** lorsque le cyber-harcèlement enfreint à la fois le règlement de Twitter et celui de l'organe de presse, les modérateurs/trices ont tendance à muter plutôt qu'à bloquer les comptes. Cette option atténue l'impact direct de l'attaque et prévient toute réaction hostile puisque l'utilisateur muté ne sait pas qu'il a été muté. Enfin, cette option permet aux modérateurs/trices de continuer à voir le contenu posté par les comptes mutés et de rester ainsi vigilants face à d'éventuelles menaces crédibles.

- ***Bloquer :*** les modérateurs/trices ont tendance à bloquer les comptes qui envoient continuellement des spams ou des arnaques ; les modérateurs/trices appliquent généralement cette mesure en dernier ressort pour éviter les réactions hostiles des comptes bloqués puisque ceux-ci sont informés du blocage. En outre, les modérateurs/trices n'auront plus accès au compte bloqué ce qui complique la surveillance d'éventuelles menaces imminentes.

- ***Signaler :*** les modérateurs/trices signalent généralement à Twitter les tweets et comptes qui diffusent des menaces crédibles et imminentes ou qui contiennent des images violentes.

- ***Masquer les réponses :*** les modérateurs/trices peuvent choisir de masquer les réponses à leurs tweets. Tous les utilisateurs peuvent cependant consulter les réponses masquées grâce à l'icône Réponse masquée présente, le cas échéant, sur le tweet initial. Twitter a créé cette option dans le but de minimiser l'impact des trolls ou des commentaires insultants, afin qu'ils ne monopolisent pas la conversation. Si un/e modérateur/trice masque une réponse, l'auteur de la réponse ne recevra pas de notification.

Étape 4 : Suivi et réévaluation

Les rédactions doivent garder un œil sur les cas signalés de cyber-harcèlement et réévaluer la sécurité et les mécanismes de soutien pour protéger les journalistes du cyber-harcèlement.

Les organes de presse doivent **créer une base de données** pour garder une trace des incidents de cyber-harcèlement et des mesures prises. Cette base de données ne doit pas contenir tous les cas de harcèlement, mais devrait au moins inclure les cas signalés par les membres de l'équipe via des mécanismes for-

mels ou ceux pour lesquels l'évaluation des risques a déclenché la mise en place de mesures de soutien.

Le but premier de cette base de données est de suivre les cas signalés de cyber-harcèlement et de permettre une (ré)évaluation régulière des mesures de soutien mises en place, notamment si des mesures nouvelles ou différentes sont nécessaires.

En dehors des mesures de soutien en tant que telles, les rédactions devraient également réévaluer régulièrement l'efficacité de leurs structures de réaction au harcèlement. Cela devrait inclure des enquêtes qualitatives pour évaluer dans quelle mesure le personnel et les contributeurs/trices estiment que le problème est pris au sérieux et des enquêtes quantitatives recensant le nombre de cas ayant entraîné une réponse quelconque.

Rôles et missions

Ci-dessous figure une description des rôles et missions à prendre en considération. Dans les petites rédactions, certains de ces rôles peuvent être assumés par une seule personne.

Coordinateur/coordinatrice cyber-sécurité

Ce profil regroupe un certain nombre de tâches pouvant être réparties entre les membres de l'équipe ou assignées à une seule personne :

- Servir d'interlocuteur/trice à qui les journalistes peuvent signaler des incidents de cyber-harcèlement.
- Examiner chaque cas de cyber-harcèlement en coordination avec les journalistes ciblés, le/la rédacteur/trice en chef et le/la représentant/e du public, et suggérer les mécanismes de soutien dont le/la journaliste visé/e aura besoin.
- Le cas échéant, convenir d'une réponse officielle avec la direction et les experts juridiques.
- Mettre à jour la base de données des cas de cyber-harcèlement pour suivre et évaluer l'efficacité des mesures mises en place.
- Au vu de la nature évolutive des attaques en ligne, examiner régulièrement les mesures en place dans la rédaction pour prévenir et réagir au cyber-harcèlement.
- Servir de point de coordination et d'information pour ces mesures. Le/la coordinateur/trice cyber-sécurité doit être parfaitement au fait des mesures concernant la rédaction, être capable de les expliquer aux journalistes visés par des attaques en ligne et servir de point de contact principal pour leur mise en œuvre.
- Assister régulièrement aux réunions de la rédaction pour être au courant de futurs contenus susceptibles d'engendrer des attaques en ligne.

Direction

- Reconnaître que le cyber-harcèlement est un problème sérieux et qu'une attaque envers un membre de l'équipe constitue une attaque envers l'organe de presse tout entier. Réaffirmer cette position régulièrement à la rédaction.
- Adopter des changements structurels dans la rédaction pour créer un environnement favorable où le signalement d'attaques en ligne n'est pas stigmatisé. Faire en sorte que des ressources suffisantes (temps et argent) soient affectées à la maintenance et à la mise à jour de ces nouvelles structures.

Désigner un/e ou plusieurs coordinateurs/trices cyber-sécurité, cf. ci-dessus.

- Inclure les cibles des attaques en ligne dans les processus décisionnels qui les affectent.

Rédacteurs/rédactrices

- Reconnaître que le cyber-harcèlement est un problème sérieux et inacceptable, et ne constitue en aucun cas une facette du journalisme moderne.
- Évoquer régulièrement le sujet du cyber-harcèlement dans les réunions de la rédaction. Parler ouvertement de ce sujet créera une atmosphère dans laquelle les journalistes se sentiront plus à l'aise pour signaler des attaques.

Modérateurs/modératrices

- Identifier les menaces individuelles et les campagnes organisées sur les réseaux sociaux et

dans les commentaires visant des membres de l'équipe, les inscrire dans une base de données et les faire remonter aux journalistes, rédacteurs/trices et experts en sécurité numérique.

- Contribuer à l'analyse du degré de menace des attaques en ligne.

- Prendre en charge les comptes de réseaux sociaux du/de la journaliste visé/e pour réduire son exposition aux contenus violents et minimiser le traumatisme potentiel.

Journalistes

- Comprendre que le cyber-harcèlement est un problème sérieux et inacceptable, et ne constitue en aucun cas une facette du journalisme moderne.

- Participer à toutes les offres de formation pertinentes de l'organe de presse, notamment en matière de sensibilisation, de sécurité numérique et de gestion des risques de traumatisme.

- Participer à des structures formelles et informelles de soutien par les pairs.

- Signaler les attaques en ligne dès qu'elles surviennent, même si vous ne pensez pas subir de conséquences négatives liées à l'attaque. Leur signalement aide la rédaction à comprendre la portée du problème et à développer les mesures nécessaires pour le combattre.

À propos de l'IPI

Fondé en 1950, l'International Press Institute (IPI) est un réseau mondial de rédacteurs, journalistes et responsables médias engagés en faveur d'un journalisme indépendant de qualité. Ensemble, nous promouvons les conditions permettant au journalisme de remplir son devoir public, la principale condition étant la capacité des médias à opérer librement, sans interférences et sans peur de représailles. Nous avons pour mission de défendre la liberté de la presse et la libre circulation de l'information là où elles sont en danger.

À propos de l'initiative Newsrooms Ontheline de l'IPI

L'initiative Newsrooms Ontheline de l'IPI a pour but de recueillir et de partager les ressources et les meilleures pratiques pour les médias et les journalistes afin de prévenir, de contrer et de gérer le harcèlement et les abus en ligne à leur encontre. En fournissant ces outils aux rédactions, elle vise à contrer l'impact personnel et professionnel du cyber-harcèlement à l'encontre de journalistes et à prévenir toute autocensure découlant d'attaques en ligne qui menaceraient l'accès du public à l'information.

L'Adessium Foundation et la Democracy & Media Foundation ont permis de financer la publication du présent protocole

ADESSIUM FOUNDATION

Democracy & Media Foundation **Stichting Democratie & Media**

Copyright : Ce protocole à l'attention des rédactions pour aider les journalistes victimes de cyber-harcèlement est sous licence internationale Creative Commons Attribution. Vous êtes libre de réutiliser ce protocole à condition d'en citer la source.

Protocole à l'attention des rédactions pour aider les journalistes victimes de cyber-harcèlement

Éditeur :
International Press Institute (IPI)
Février 2020.

International Press Institute

International Press Institute

Tél. : + 43 1 512 90 11

E-mail : info@ipi.media

Site Internet : ipi.media