CRISE DIGITALE

AGCS PLUS

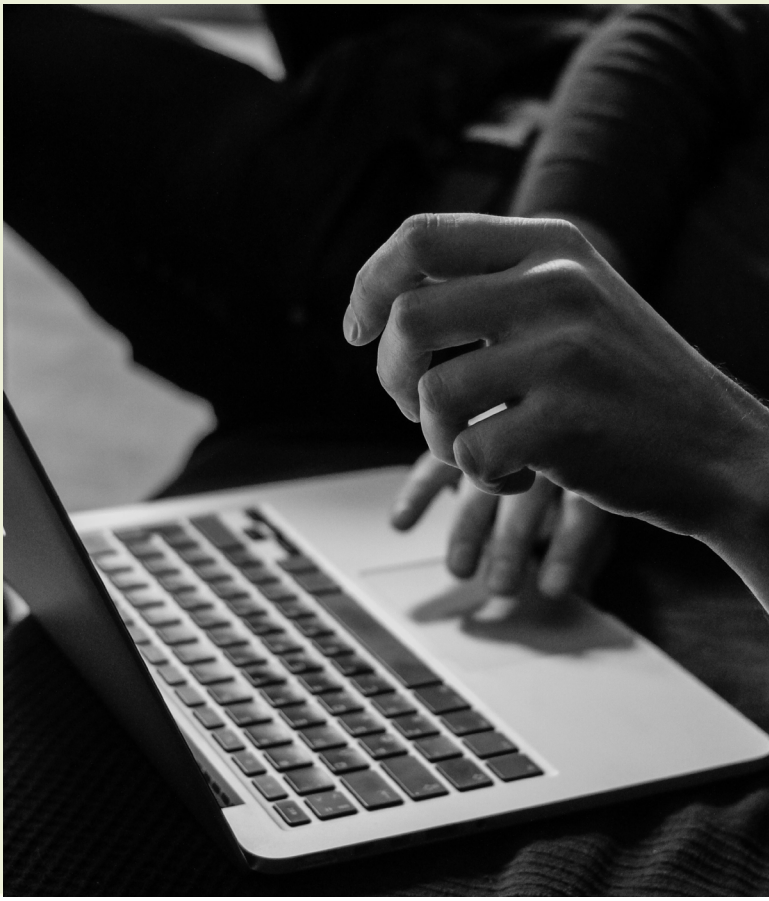
RÉSEAU DE COALITION PLUS

PROTOCOLE 2 : CRISE DIGITALE

Définition : une crise digitale fait généralement référence à une crise réputationnelle qui trouve son origine, ou dont le phénomène de propagation démarre et s'amplifie sur Internet.

Introduction

Internet est un outil indéniablement incontournable pour les minorités de genre et de sexe, les activistes et leurs organisations. Pour les communautés, la toile, et en particulier les applications de rencontre et les réseaux sociaux constituent de puissants outils de libération et d'épanouissement. Pour beaucoup d'associations, l'internet est un moyen de mobilisation efficace et permet le partage d'informations, l'apprentissage et le réseautage à travers le Monde. Pendant les crises qui affectent négativement la communauté, le réseautage sur Internet et les réseaux sociaux donnent accès à des ressources pour préserver notre santé mentale et physique. Plusieurs outils digitaux sont à notre disposition pour nous divertir, rencontrer des partenaires sexuels, affirmer son appartenance à la communauté, s'informer ou rester en contact avec les activistes et les influenceurs. Cependant, les Minorités Sexuelles et de Genre connaissent généralement bien les manifestations de la discrimination et de la stigmatisation sur les réseaux sociaux.



A qui est destiné ce protocole ?

Ce protocole est réalisé pour que les organisations dirigées par les Minorités Sexuelles et de Genre puissent jouir des réseaux sociaux et de l'internet de manière sécurisée et positive. Quel que soient les dispositions prises, les crises digitales peuvent toujours survenir. Il convient donc pour les organisations de Minorités Sexuelles et de Genre de se familiariser avec les directives et les conseils fournis dans ce protocole.

Contenu du protocole

Le protocole décrit les aspects les plus importants à connaître concernant la sécurité digitale, les types de risques encourus, dénoncer les auteurs de haine en ligne, les moyens de les prévenir ainsi que des ressources supplémentaires à consulter. Quelques astuces sont décrites pour sécuriser l'usage des réseaux sociaux au quotidien.

Pour bien intégrer la sécurité digitale dans leurs processus, les organisations sont encouragées à mettre en place un circuit avec les étapes suivantes :

- Identifier les menaces digitales
  - Établir des partenariats
    - S'informer
- Renforcer les moyens techniques et humains pour prévenir les crises
  - Gérer une crise
- Offrir des services en cas de crise
  - Documenter

Pourquoi ce protocole est-il important ?

On constate que l'usage d'internet présente des risques et la possibilité d'effectuer des actes risqués ou même dangereux pour la sécurité des individus, de l'organisation ou des communautés. Chaque année dans plusieurs pays, les crises digitales surviennent ; elles peuvent prendre des formes multiples, perdurer pendant quelques heures, des jours ou plusieurs semaines. Les crises digitales peuvent être liées à d'autres types de crise (réputationnelle ou intra-communautaire par exemple) et dans certains peuvent aller jusqu'à menacer les individus qui travaillent dans les organisations dirigées par les Minorités Sexuelles et de Genre.

Les outils digitaux créent des nouveaux défis et des dangers à prévoir et à gérer par les organisations de Minorités Sexuelles et de Genre. Les crises digitales sont des événements qui font aussi parfois référence aux crises réputationnelles.

L'origine provient souvent d'outils digitaux (téléphones par exemple) et se propage sur Internet. La plupart des réseaux sociaux les plus populaires, tels que Facebook, Instagram, WhatsApp ou Twitter (X) ont des méthodes pour censurer les contenus haineux.

On note cependant des variations ; par exemple plusieurs défenseurs de droits humains notent que les contenus haineux et campagnes contre les Minorités Sexuelles et de Genre ont pris de l'ampleur depuis l'arrivée de Elon Musk à la direction de 'Twitter,X'.

Ce protocole vise à aider les associations et les activistes pourront décider avec qui et comment iels peuvent s'engager en ligne de manière sécurisée

COMMENT PROTEGER VOTRE ESPACE FACEBOOK

Vous devez contrôler qui peut voir vos publications sur Facebook et Instagram, et vous pouvez choisir le niveau d'ouverture ou de privauté de votre espace. Pour cela, suivez les étapes suivantes :
Depuis votre page de profil Instagram, accédez à votre menu Paramètres, puis sélectionnez Confidentialité. Faites défiler jusqu'à Compte privé et déplacez le curseur vers la droite. Le curseur deviendra bleu une fois le compte privé
En passant à un compte privé sur Instagram, vous pouvez choisir qui vous suit et qui
voit les publications que vous partagez. C'est également rapide et facile à vérifier la confidentialité de votre compte Facebook et contrôlez qui voit vos publications.

'Privacy Checkup' vous guide à travers certains de vos paramètres de confidentialité et de sécurité, afin que vous puissiez revoir vos choix pour vous assurer que vous partagez avec qui vous voulez. Pour accéder à cette fonctionnalité, cliquez sur le bouton (***) de votre profil Facebook, sélectionnez et afficher le type de confidentialité qui vous convient.

FAITES ATTENTION LORSQUE VOUS PARTAGEZ UNE INFORMATION SUR FACEBOOK

Si vous avez hâte de partager quelque chose, mais que vous souhaitez uniquement qu'un groupe sélectionné d'amis ou de followers le voie, partagez-le via Direct ou Close Friends sur Instagram, ou utilisez les commandes de Facebook pour contrôler qui voit votre publication.

La haine sur les réseaux sociaux

Comment dénoncer les pages qui propagent la haine et la violence contre la communauté.

Les propos homophobes, transphobes ou haineux sont inacceptables dans les espaces et réseaux sociaux de nos organisations. Nous encourageons la communauté a rapporter les cas lorsqu'ils apparaissent sur nos platte-formes pour nous aider a le supprimer

Comment dénoncer les personnes qui diffusent la haine sur facebook ?

Tapez sur *** en haut de la publication, sélectionnez Rechercher de l'aide ou Signaler la publication et sélectionnez le motif du discours de haine pour le signalement. Une fois que vous avez signalé quelque chose, vous pouvez vérifier l'état de votre rapport depuis la boîte de réception du support.

Comment dénoncer les personnes qui diffusent la haine sur instagram ?

Appuyez sur... au-dessus de la publication, appuyez sur Signaler et sélectionnez C'est inapproprié. Sélectionnez Discours ou symboles haineux.

	ETAPES DU CIRCUIT	ACTIVITES / ACTIONS A ENTREPRENDRE
1	IDENTIFIER LES MENACES DIGITALES	**Identifier les divers types de menaces digitales** Campagnes médiatiques contre une organisation de Minorités Sexuelles et de Genre caractérisée comme faisant la 'promotion' de l'homosexualité ou de la prostitution. Divulgation intentionnelle (ou accidentelle) des données sensibles, des locaux ou d'un lieu social fréquenté par un grand nombre de Minorités Sexuelles et de Genre. **Divulgation de scandales ('mariages gay', concours 'Miss', etc.)** : ces événements créent des paniques morales qui à leur tour peuvent résulte sur une hausse de la violence contre les Minorités Sexuelles et de Genre. Harcèlements et 'espionnage' sur les sites de rencontre pour personnes LGBT. Dans certains pays les forces de l'ordre et des personnes mal intentionné infiltrent les sites de rencontre pour traquer les Minorités Sexuelles et de Genre. Ces situations entraînent des poursuites judiciaires, divulgations d'identités ('outing'), arnaques et divers types de harcèlements envers les victimes. **Piratage d'un site web ou d'un compte de réseau social** : en diffusant des messages sur la lutte contre les discriminations et la stigmatisation des Minorités Sexuelles et de Genre, les sites web et comptes des organisations peuvent être pirates. **Cyber-fichage :** ce sont des cas ou des images et vidéos de nus, ou personnes ayant des rapports sexuels sont diffuses pour nuire à la réputation d'une personne ou d'une communauté entière. Ce type de crises peut avoir de nombreuses conséquences notamment : • Dépression ou détresse psychologique • L'exclusion familiale • L'exclusion scolaire • Licenciements abusifs • Exclusion et perte du domicile ou des bureaux • Exil forcé
1	FORMEZ DES PARTENARIATS	**Avec les 'influenceurs' :** établir des contacts formels avec les influenceurs peut se révéler utile. Il faut cependant peser le pour et le contre d'un partenariat avec ces personnes, car ils.elles peuvent accroître les risques sécuritaires. Dans plusieurs pays certains activistes Minorités Sexuelles et de Genre ont une forte présence sur les réseaux sociaux et sont une source d'information régulière utile pour la communauté. Certains effectuent un travail d'alerte lors des crises qui affectent négativement les communautés. **Avec les juristes** : les pays possèdent généralement des lois sur la cybercriminalité qui sont censées protéger les citoyen.nes contre les attaques ou autres formes de crimes qui prennent leur source sur Internet. Il est important pour les organisations d'avoir à portée de main des numéros de téléphone de juristes qui peuvent interpréter ces lois.
2	Prévenir les crises digitales	Se doter de moyens budgétaires et techniques pour prévenir les crises digitales. Se familiariser avec les dispositifs de sécurité sur les réseaux sociaux, notamment INSTAGRAM et FACEBOOK. Pour cela, consultez quelques astuces dans la section suivante de ce protocole. Collaborer avec les autres organisations en vue de mettre sur pied au niveau du pays un mécanisme d'alerte et de soutien aux jeunes Minorités Sexuelles et de Genre sur la sécurité sur les réseaux sociaux (exemple Cameroun) Designer (et former) une personne focale dans l'organisation pour la gestion de la sécurité digitale Informer les membres de la communauté sur leurs droits fondamentaux selon les lois du pays. Vous pouvez faire cela de manière régulière lors des sessions en groupe sur la sécurité, ou à travers des publications écrites ou vocales diffusées sur les réseaux sociaux. • Animer des séances avec le personnel, les activistes et les bénévoles sur la cybersécurité. • Animer des causeries éducatives avec les bénéficiaires sur la cybersécurité et les conduites à tenir sur les réseaux sociaux • Diffuser sur les réseaux sociaux de l'association des messages éducatifs et factuels clés et pratiques sur la cybersécurité (voir exemples de capsules éducatives) **Accès à la justice :** partager les conduites à tenir et les recours judiciaires disponibles en cas de victimisation ou de harcèlement en ligne.

4	**GERER UNE CRISE**	Lorsqu'une crise digitale intervient, il est important pour les organisations de Minorités Sexuelles et de Genre et les activistes de prendre des mesures essentielles, notamment : • **Informer** la communauté à travers plusieurs canaux sur la nature du danger et sur les mesures individuelles de sécurité à prendre. • Mettre à la disposition des communautés **une ligne d'écoute et de conseils** • **Sécuriser l'organisation**, son personnel et bénévoles (quelques suggestions pour cela sont offertes dans le tableau.) • Accéder à un fonds d'urgence pour les acteurs associatifs et activistes comme ceux de Frontline defender ou Frontline aids oùles organisations financées par ISDAO.
6	**SERVICES**	• **Accès à la justice** : faciliter l'accès a des juristes ou parajuristes pour les personnes qui ont subi des dommages physiques ou moraux à la suite de la crise • **Soutien psychologique :** faciliter l'accès à des services psycho-sociaux pour les personnes qui ont souffert de la crise • **Assurer des médiations sociales et familiales** pour faciliter la réinsertion et le soutien aux personnes qui ont souffert de "outing" a la suite de la crise. • **Dans les cas de licenciement abusif :** faire des médiations avec les employeurs
7	**Documentation**	La documentation des expériences vécues lors d'une crise digitale est un élément important du circuit de prévention et de gestion. Les réseaux sociaux constituent un système d'information et d'alerte dans les cas de violation de droits humains des personnes. N'hésitez pas à documenter les cas que vous notez dans votre ville ou dans votre pays et de les transmettre aux organisations chargées de la documentation et de la veille sur les droits humains. Faites l'effort de noter toutes les leçons apprises dans les rapports annuels, les rapports des droits humains au niveau national et international

MESURES INDIVIDUELLES DE PREVENTION POUR PREVENIR ET GERER LES CRISES DIGITALES
Les conseils de @Bandykiki pour les activistes et personnes LGBT vivant dans des environnements hostiles qui veulent utiliser les réseaux sociaux de manière sécurisée et anonyme

ÉVITER DE POSTER LES PHOTOS PERSONNELLES
Pour votre profil, optez pour des photos qui ne montrent pas votre visage, ou toute autre aspect de votre personne susceptible d'être reconnu. Pour rester anonyme utilisez un symbole ou une image neutre.

EN CAS DE PERTE OU DE VOL DE VOTRE TELEPHONE (OU AUTRE OUTIL DIGITAL)
En cas de perte de votre ordinateur, téléphone ou objet digital que vous utilisez pour accéder à votre compte Facebook ou Instagram, utilisez un autre outil digital pour changer votre mot de passe.

Utilisez un nom diffèrent
Sur Twitter/X et Instagram par exemple vous pouvez utiliser un nom d'emprunt diffèrent du votre nom officiel. Évitez d'utiliser un nom identifiable qui peut être reconnu.

ÉVITEZ LA GEOLOCALISATION.
Fermez les options de géolocalisation lorsque vous publiez des photos ou des vidéos. La géolocalisation permet de connaître votre position géographique et compromet ainsi votre anonymat.

AUTHENTIFICATION A DEUX FACTEURS
Pour éviter les piratages et sécuriser vos outils digitaux opté pour une authentification à deux facteurs.

LIMITEZ VOS CONNECTIONS À PLUSIEURS PLATEFORMES.
Dans le cas où vous animeriez plusieurs plateformes sur les réseaux sociaux, évitez de vous connecter à ces diverses plateformes. Cela aide à renforcer votre anonymat.

LE PARTAGE D'OUTILS DIGITAUX
Minimiser les risques de piratage : lorsque vous utilisez un ordinateur public ou un téléphone qui n'est pas le vôtre, n'oubliez pas de vous déconnecter de votre compte Facebook ou Instagram après usage.

SOYEZ VIGILANTS SUR LE CONTENU DE VOS PUBLICATIONS.
Sachez que même les publications anonymes peuvent entraîner des conséquences fâcheuses pour la communauté. Soyez respectueux et attentif au contenu de vos publications.

Cas d'études :

Nigeria (2023) : le 29 août 2023, les autorités policières d'état du Delta au Sud Est du Nigeria publient une vidéo et des photos de douzaines de jeunes hommes et femmes rafles la veille dans un suppose 'mariage gay". Les images montrent des douzaines de personnes répondant à des questions humiliantes et présentées à l'opinion publique comme ayant contrevenu aux lois du pays bannissant les mariages de personnes du même sexe. Les vidéos des jeunes victimes de la rafle ont été vues par des millions de personnes à travers le pays et au-delà, malgré la nature illégale de cette forme de violation de la vie privée.

Cameroun (2021) : la visibilité liée au process de Patricia et Shakiro et les violences transphobes. Le 8 février 2021, des gendarmes ont arrêté Shakiro et Patricia à Douala parce qu'ils portaient des vêtements féminins. Ils ont été accusés de tentative de conduite homosexuelle, d'outrage public à la pudeur et de non-possession de carte d'identité nationale. Alors qu'ils étaient détenus dans la prison centrale surpeuplée de Douala, des gardiens et d'autres détenus les ont battus, insultés et menacés. Le 11 mai 2021, un tribunal a condamné Shakiro et Patricia à cinq ans de prison et à une amende de 200 000 francs CFA (370 dollars américains) en vertu d'une loi draconienne qui interdit les relations homosexuelles. Le 16 juillet, un juge a ordonné leur libération jusqu'à ce qu'un tribunal entende leur appel, prévu pour le 14 septembre. La persécution des personnes LGBT, sanctionnée par l'État, s'est intensifiée en 2021 au Cameroun. Entre février et avril de cette année, les forces de sécurité ont arrêté au moins 27 personnes, dont un enfant, pour des allégations de conduite homosexuelle consensuelle ou de non-conformité de genre, battant et soumettant certaines à des violences sexuelles.

Cameroun (2023) : les personnes lesbiennes, gays, bisexuelles, transgenres et intersexuées (LGBTI) au Cameroun ne sont que trop conscientes des discours homophobes et des attaques violentes à leur encontre. Cela a été une nouvelle fois souligné par l'effusion de vitriol avant la visite prévue de Jean-Marc Berthon, l'ambassadeur de France aux droits des personnes LGBT+. Larissa kojoue chercheuse à Human Rights Watch rapporte que l'annonce de cette visite a suscité une multitude d'appels à la haine en ligne ainsi que des déclarations haineuses de plusieurs responsables administratifs et politiques camerounais.

Afrique du Nord et Moyen-Orient (2023) : Des acteurs étatiques et des particuliers de la région Moyen-Orient et Afrique du Nord (MENA) ont piégé des personnes lesbiennes, gays, bisexuelles et transgenres (LGBT) sur les réseaux sociaux et les applications de rencontres, les ont soumises à l'extorsion, au harcèlement et aux sorties en ligne, et se sont appuyés sur des photos numériques, des discussions et des informations similaires obtenues illégalement dans le cadre de poursuites, en violation du droit à la vie privée, d'une procédure régulière et d'autres droits de l'homme. Ce rapport examine le ciblage numérique dans cinq pays : l'Egypte, l'Irak, la Jordanie, le Liban et la Tunisie. Les forces de sécurité ont ajouté ces tactiques de ciblage numérique aux méthodes traditionnelles de ciblage des personnes LGBT, telles que le harcèlement de rue, les arrestations et la répression, pour permettre l'arrestation arbitraire et les poursuites ultérieures contre les personnes LGBT.

Egypte (2021) : au cours des dernières années, les procureurs égyptiens ont commencé à s'appuyer de plus en plus sur la collecte de preuves numériques pour poursuivre les personnes LGBTQ via des applications de rencontres en ligne ou des preuves provenant des appareils des personnes. Cependant, depuis cette année, les procureurs transfèrent les affaires LGBTQ devant les tribunaux économiques égyptiens, connus pour poursuivre les crimes « moraux » en ligne. Le résultat est que les peines, les accusations et les amendes sont doublées. L'Egypte poursuit depuis longtemps la communauté LGBTQ. Bien que la loi égyptienne n'interdise pas directement « l'homosexualité », une infrastructure juridique complexe d'interprétations et de précédents a permis des poursuites continues et ciblées contre les personnes LGBTQ

Chili (2020) : Augmentation des chantages, meurtres et bastonnades d'hommes qui rencontrent d'autres hommes en ligne. https: www.movilh.cl-aumentan-los-asesinatos-y-golpizas-contra-hombres-que-acuerdan-citas-con-otros-hombres-por-aplicaciones. ,
Le Mouvement pour l'intégration et la libération des homosexuels (Movilh) lance l'alerte sur le risque grave pour la vie et la santé physique et psychologique des hommes homosexuels,bisexuels qui prennent rendez-vous via des applications ou sur Internet avec d'autres hommes, tout en soupçonnant « les personnes ou groupes organisés pour commettre ces crimes». La réaction de Movilh a eu lieu après l'arrestation aujourd'hui d'un sujet de 25 ans après avoir ôté la vie dimanche à Miguel Arenas Rodríguez, dont le corps a été retrouvé avec des signes évidents de torture à son domicile, situé à Villa San Andrés de Esmeralda, à Colina. À la suite des abus et aux assassinats contre les personnes qui organisent des rendez-vous pour les candidatures, le Movilh a développé une campagne d'information et de prévention. « Notre recommandation est que les gens commentent toujours ces nominations à un tiers en qui ils ont confiance, et que la première réunion ait toujours lieu dans un espace public et ouvert, où ils peuvent être vus par d'autres. Nous recommandons également de choisir des profils liés à un réseau social avec plus d'informations sur l'autre personne, de ne pas révéler la routine quotidienne et d'éviter la consommation de drogues. Tout cela a un effet dissuasif sur les victimes », selon Moviih.