

Évaluation des risques

Introduction à l'évaluation des risques et à sa mise en pratique dans un cadre personnel ou organisationnel.

- Objectifs et activités d'apprentissage
- Introduction à l’évaluation des risques [activité d'introduction]
- La rue la nuit [activité d'introduction]
- Le cycle de vie des données, ou comment comprendre les risques [activité d'approfondissement]
- Organisation de manifestations et évaluation des risques [activité tactique]
- Les bases de l’évaluation des risques [ressource essentielle]
- Évaluation des risques et mouvements sociaux [ressource essentielle]

Objectifs et activités d'apprentissage

ev-risques_FR.png
Image not found or type unknown

Objectifs d’apprentissage

À la fin de ce module, les participant·e·s seront capables de :

- Comprendre les concepts fondamentaux de l’évaluation des risques.
- Appliquer les cadres d’évaluation des risques pour leur sécurité personnelle et/ou celle de leur organisation.
- Imaginer des manières d’évaluer les risques adaptées à leurs besoins.

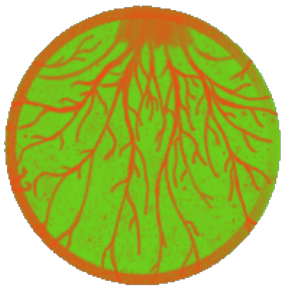
Activités d'apprentissage

Activités d'introduction



- Introduction à l’évaluation des risques (présentation & discussion)
- Assessing communication practices (en anglais)
- Daily pie chart and risk (en anglais)
- La rue la nuit

Activités d'approfondissement



- Re-thinking risk and the five layers of risk (en anglais)
- Le cycle de vie des données, ou comment comprendre les risques

Activités tactiques



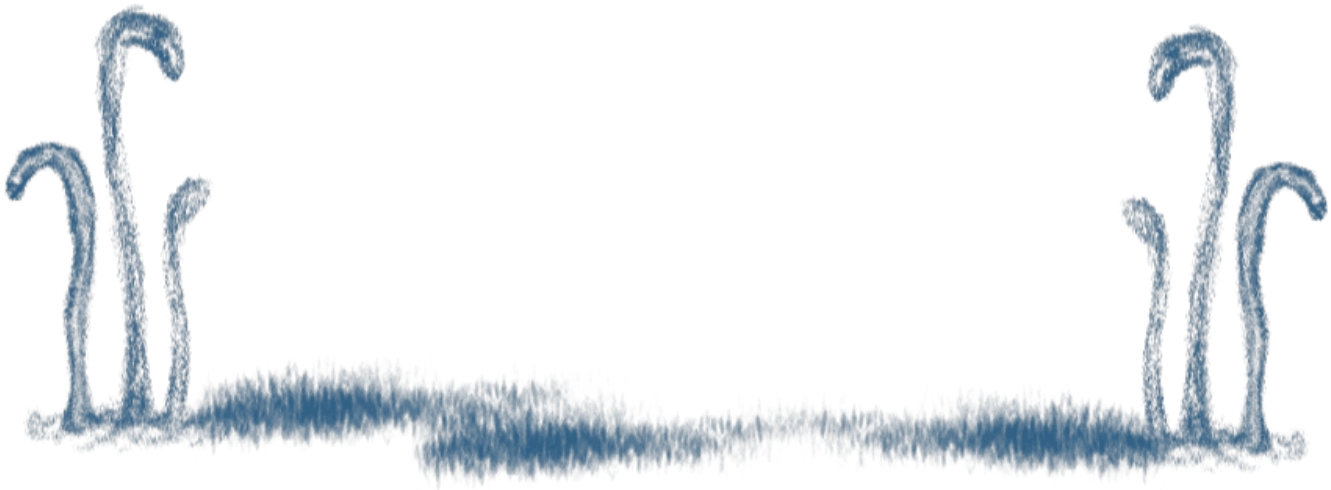
- Organisation de manifestations et évaluation des risques

Ressources essentielles



Consultez ces ressources pour approfondir vos connaissances en matière d'évaluation des risques et pour mieux préparer vos ateliers de formation.

- Les bases de l’évaluation des risques
- Évaluation des risques et mouvements sociaux



Introduction à l’évaluation des risques [activité d'introduction]

ativ_intro_FR.png
Image not found or type unknown

Cette activité vise à introduire un cadre d’évaluation des risques et à s’exercer avec.

Objectifs d'apprentissage

- Comprendre les concepts fondamentaux de l’évaluation des risques.
- Commencer à appliquer un cadre d’évaluation des risques pour sa sécurité personnelle et/ou organisationnelle.

À qui s’adresse cette activité ?

Cette activité est conçue pour toute personne sans expérience ou avec une expérience élémentaire dans l’évaluation des risques. Elle est également conçue pour un atelier ouvert à des personnes de différentes organisations.

Temps requis

Pour être réaliste, il faut compter une journée (huit heures au minimum) pour réaliser correctement cette activité.

Matériel

- Tableau à feuilles et marqueurs

- Projecteur
- Ordinateurs portables

Mécanique

Pour cette activité, créez un scénario mettant en scène une personne ou un groupe qui seront sujets et sujettes à l'évaluation des risques faite par les participant·e·s.

Selon les personnes qui participent, vous options peuvent être :

- Un groupe défendant les droits humains dans un pays qui vient d'adopter une loi autorisant à surveiller les ONG
- Une femme trans qui lance un site web en soutien aux autres femmes trans
- Un réseau d'activistes pour les droits des femmes qui travaille sur un sujet considéré comme tabou dans leurs pays
- Un groupe qui dispose d'une maison d'accueil sécurisée pour les jeunes trans
- Un petit groupe LGBTIQ victime d'attaques en ligne
- Une femme queer membre d'une minorité ethnique postant ses opinions en ligne.

Séparez les participant·e·s en groupes. Iels peuvent travailler sur le même type d'organisation/groupe ou sur des organisations différentes.

> **Conseil pour l'animation :** Il est important de proposer un scénario intéressant et proche de l'expérience des participant·e·s.

Une fois que les groupes sont formés, présentez le diaporama **Introduction à l'évaluation des risques**

Travail de groupe 1 : Précisez le contexte et le scénario

Avant de commencer à compléter le Modèle d'évaluation des risques (fichier .odt), les groupes devraient préciser les contours du scénario choisi.

Pour un scénario groupal :

- Créez le profil de cette organisation : situation géographique, taille, mission générale.
- Indiquez les activités ou les changements de contexte qui posent des risques : il peut s'agir d'une nouvelle loi, ou de la planification d'une activité que ses détracteurs voudront interrompre. Il pourrait également s'agir d'une question interne susceptible de présenter des risques, p. ex. un récent conflit au sein de l'organisation, ou d'un événement externe qui provoque un stress important parmi les membres de l'organisation.
- Nommez les personnes hostiles à leurs actions, et celles qui en seront les alliées.

Pour un scénario individuel :

- Créez le profil de cette personne : âge, situation géographique, orientation sexuelle, activité sur les médias sociaux.
- Imaginez pour quelles opinions cette personne est attaquée. Ou décrivez le site web qui lui fait courir des risques. Ou la situation contextuelle qui la met en situation de vulnérabilité (p. ex. perdre son domicile, sortir d'une relation abusive avec une personne de la même organisation ou mouvement, etc.).
- Indiquez qui sera hostile à ses actions et qui lui apportera son soutien.

  Donnez à chaque groupe une heure pour réaliser cette activité.

Ensuite, demandez à chaque groupe de présenter rapidement leurs scénarios.

Présentez ensuite le **Modèle d'évaluation des risques (fichier .odt).**

Voici quelques remarques sur le tableau :

- Les menaces devraient être **spécifiques** : quelle est la menace (l'intention négative envers le groupe individuel) et qui est à l'origine de la menace ?
- Réfléchissez à la **probabilité** d'une menace sous trois angles :
  - Vulnérabilité : quels processus, activités et comportements de l'individu ou du groupe augmente la probabilité pour une menace de se concrétiser ?
  - Capacité de la ou des personnes à l'origine de la menace : qui menace et de quelle manière peuvent-ils mettre cette menace à exécution ?

    - Précédents : ce type de menaces a-t-il déjà été présent dans un scénario du même type ? Si la réponse est oui, alors la probabilité augmente.
- Concernant les **répercussions**, ne tenez pas uniquement compte des répercussions à titre individuel, mais aussi dans une communauté élargie.
- L'évaluation d'une probabilité et des répercussions comme faibles, moyennes ou élevées est toujours relative. Mais il est important de les évaluer pour établir quels sont les risques pour lesquels définir des mesures d'atténuation.
- Risques : une phrase indiquant la menace et la probabilité qu'elle soit mise à exécution.

Travail de groupe 2 : Évaluation des risques

À l'aide du **modèle d'évaluation des risques**, chaque groupe analyse les risques de son scénario. L'objectif est ici d'identifier les différents risques et de les analyser l'un après l'autre.

> **Conseil pour l'animation :** distribuez une copie par groupe du modèle d'évaluation des risques pour qu'iels puissent y consigner directement le résultat de leurs discussions.

Ce travail durera au moins deux heures, au long desquelles la personne formatrice-animatrice passera parmi les différents groupes pour les conseiller.

À la fin, au lieu de leur demander de lire leurs modèles, posez-leur des questions sur le processus :

- Quelles difficultés votre groupe a-t-il rencontré pour évaluer les risques ?
- Quelles principales menaces avez-vous identifié ?
- En quoi l'analyse de la probabilité vous a-t-elle posé problème ?

Idées et discussions sur les tactiques d'atténuation des risques

Sur la base du texte de présentation des tactiques d'atténuation des risques (voir la rubrique Présentation plus bas), présentez les points principaux et discutez avec les participant·e·s.

Travail de groupe 3 : Prévoir des mesures d’atténuation des risques

Demandez à chaque groupe d’identifier un risque dont la probabilité et les répercussions sont élevées. Demandez-leur ensuite de créer un plan d’atténuation pour ce risque.

Quelques questions pour guider la réflexion

Stratégies de prévention

- Quelles actions avez-vous déjà entreprises et de quelles capacités disposez-vous pour éviter cette menace ?
- Quelles actions allez-vous entreprendre pour empêcher la concrétisation de cette menace ? Comment allez-vous modifier les processus du réseau pour empêcher cette menace de se réaliser ?
- Devez-vous créer des politiques et des procédures en ce sens ?
- De quelles compétences aurez-vous besoin pour éviter cette menace ?

Réponse à l’incident

- Que ferez-vous quand la menace sera concrétisée ? Quelles mesures prendrez-vous à ce moment-là ?
- Comment comptez-vous atténuer la gravité des répercussions de cette menace ?
- De quelles compétences avez-vous besoin pour prendre les mesures nécessaires pour répondre à cette menace ?

Compter de 45 minutes à une heure pour ce travail de groupe.

À la fin, posez-leur des questions sur le processus et demandez-leur s’il y a des questions sur les activités réalisées.

Pour synthétiser cette activité d’apprentissage, réitérez certaines leçons apprises :

- L’évaluation des risques permet d’imaginer des stratégies réalistes (préventives et réactives).

- Se concentrer sur les menaces les plus à même d’être concrétisées et sur celles aux répercussions élevées.
- L’évaluation des risques demande de la pratique.

Présentation

Il y a trois choses à présenter dans cette activité :

- La présentation de l’initiation à l’évaluation des risques
- Le modèle d’évaluation des risques
- Les idées de tactiques d’atténuation des risques (voir le texte ci-dessous).

Texte de présentation des tactiques d’atténuation des risques

Il y a cinq grandes façons d’atténuer les risques :

Acceptez le risque et prévoyez des plans de secours

Créer des plans de secours consiste à imaginer le risque et que sa pire répercussion possible ait lieu, et à prendre des mesures pour gérer la situation.

Évitez le risque

Réduisez vos points faibles. De quelles compétences aurez-vous besoin ? Que devrez-vous modifier dans vos comportements pour éviter le risque ?

Contrôlez le risque

Réduisez la gravité des répercussions. Concentrez-vous sur les répercussions et non sur la menace, et réfléchissez à la manière de les atténuer. De quelles compétences avez-vous besoin pour faire face à ces répercussions ?

Transférez le risque

Faites en sorte qu’une ressource extérieure prenne à sa charge le risque et ses répercussions.

Surveillez le risque

En termes d’évolution de sa probabilité et de ses répercussions. Ceci concerne habituellement les risques à faible probabilité.

Il y a deux manières d’envisager la gestion des risques :

Stratégies de prévention

- Quelles actions avez-vous déjà entreprises et de quelles capacités disposez-vous pour éviter cette menace ?
- Quelles actions allez-vous entreprendre pour empêcher la concrétisation de cette menace ? Comment allez-vous modifier les processus du réseau pour empêcher cette menace de se réaliser ?
- Devez-vous créer des politiques et des procédures en ce sens ?
- Quelles compétences devrez-vous acquérir pour éviter que cette menace ne se concrétise ?

Réponse à l’incident

- Que ferez-vous quand la menace se sera concrétisée ? Quelles mesures prendrez-vous à ce moment-là ?
- Comment comptez-vous atténuer la gravité des répercussions de cette menace ?
- De quelles compétences avez-vous besoin pour prendre les mesures nécessaires pour répondre à cette menace ?

Ajustements pour les ateliers au sein d’une organisation

Cette activité peut être utilisée dans le cadre d’un atelier où c’est une organisation qui réalise l’évaluation des risques, et où la formation consiste à guider l’organisation dans le processus.

Dans ce cas, au lieu de détailler un scénario, discutez des menaces générales qui pèsent sur l’organisation. Il peut s’agir d’un changement dans les lois ou de gouvernement avec des implications sur la capacité de l’organisation à continuer son travail. Il peut également s’agir d’un incident particulier lors duquel les personnes travaillant dans l’organisation ont senti une menace (par exemple, si une organisation partenaire, ou l’organisation elle-même, découvre qu’elle est sous surveillance). Poursuivez avec une discussion sur les capacités dont l’organisation dispose déjà : ressources, connexions, soutiens, alliées et alliés, et compétences. Ancrer une activité

d’évaluation des risques en construisant un savoir commun sur les menaces pesant sur l’organisation et sur ses capacités à y faire face sera important pour le reste du processus.

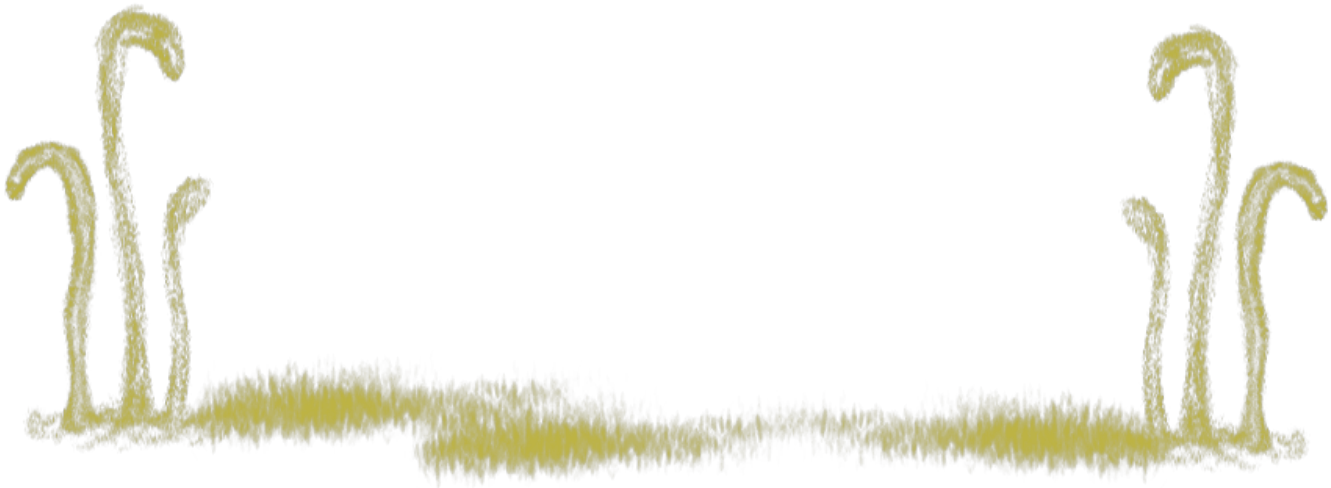
Séparez les participant·e·s en équipes/groupes pendant qu’iels parcourent le modèle d’évaluation des risques.
Dans ce contexte, le plan d’atténuation des risques est aussi important que le modèle d’évaluation des risques, si bien qu’il conviendra d’y dédier un temps équivalent.

> Il est possible de prévoir deux jours pour réaliser cette activité, en fonction de la taille de l’organisation et de ses opérations.

Pour plus d’informations (facultatif)

Consultez les ressources essentielles de ce module :

- Les bases de l'évaluation des risques
- Évaluation des risques et mouvements sociaux



La rue la nuit [activité d'introduction]

ativ_intro_FR.png
Image not found or type unknown

Cette activité vise à montrer comment nous évaluons les risques pour vivre et survivre. Au cours de cette activité, on montrera aux participant·e·s une rue sombre la nuit pour qu'iels répondent à la question suivante : « que feriez-vous pour circuler seul·e dans cette rue en toute sécurité ? ».

L'exercice vise à mettre en évidence les moyens utilisés pour évaluer automatiquement les menaces et les atténuer dans ce cas particulier.

Objectifs d'apprentissage

À la fin de l'activité, les participant·e·s :

- Commenceront à comprendre que l'évaluation des risques n'est pas une activité qui leur est étrangère.
- Feront part d'expériences sur leur façon d'aborder une situation dangereuse.

À qui s'adresse cette activité ?

Cette activité peut être réalisée avec des personnes sans expérience en matière d'évaluation des risques ainsi qu'avec celles et ceux ayant déjà effectué des évaluations des risques dans le passé.

> **Conseil pour l'animation :** Il est important que la personne formatrice/animatrice soit familiarisée avec le groupe, car cette activité pourrait faire ressurgir chez certaines et certains des traumatismes passés liés à la circulation nocturne dans les rues.

Temps requis

45 minutes

Matériel

- Un projecteur pour montrer une photo d'une rue la nuit,
- Un tableau blanc ou à feuilles pour écrire les réponses,
- Des marqueurs.

Mécanique

Présentez l'exercice en montrant une image d'une rue la nuit. Il convient également de rappeler aux participant·e·s qu'il n'y a pas de bonnes ou de mauvaises réponses.

Des exemples sont donnés ici mais vous pouvez aussi prendre votre propre image adaptée à votre contexte.

Rue1.jpg Image not found or type unknown *Photo : Yuma Yanagisawa, Small Station at night, sur Flickr.*

Rue2.png Image not found or type unknown *Photo : Andy Worthington, Deptford High Street at night, sur Flickr.*

Donnez aux participant·e·s un temps de réflexion pour répondre à la question « comment circuleriez-vous dans cette rue seul·e la nuit? »

> **Note intersectionnelle :** Ne supposez pas que tout le monde a les mêmes capacités et aptitudes physiques, c'est pourquoi nous utilisons circuler plutôt que marcher.

Demandez-leur d'écrire leur réponse pour elleux-mêmes.

Cela ne devrait pas prendre plus de cinq minutes. Vous ne voulez pas qu’iels réfléchissent trop à leur réponse.

Passez ensuite un peu de temps à les faire répondre à la question une personne après l’autre. À cette étape, en tant que personne formatrice/animatrice, vous vous contentez de reporter leurs réponses au tableau au fur et à mesure qu’iels les expriment.

Lorsque vous constatez des tendances dans les réponses, à savoir des réponses fréquentes autant que des réponses singulières – **commencez à leur demander pourquoi iels ont répondu de cette façon**.

À cette étape, nous passons à une sorte de rétroingénierie du processus. Nous avons commencé par les « comment », et nous en arrivons maintenant aux « pourquoi ». Nous recherchons les menaces, c'est-à-dire les causes du danger, dont iels ont supposé l'existence dans leurs réponses au « comment ».

Écrivez également les menaces.

Il est également bon de regarder de nouveau la photo pour voir des éléments pouvant poser une menace, ou pouvant permettre à une personne seule de circuler de façon plus sûre.

Par exemple, dans la première photo :

- Montrez les grilles et les buissons de faible hauteur. Est-ce que ce sont de bons endroits pour se cacher ?
- De quel côté de la rue marcheriez-vous et pourquoi ?
- Puisqu'il y a une petite gare, cela veut-il dire que la personne qui marche sur cette route pourra demander de l'aide à quelqu'un en cas de problème ? Si c'est le ce cas, cela rend-il la circulation dans cette rue plus sûre ?
- Est-on en sécurité sur cette route par rapport aux voitures qui passent ?

Dans la seconde photo :

- De quel côté de la rue marcheriez-vous et pourquoi ?
- Indiquez les deux personnes présentes dans la rue : leur présence rend-elle la rue plus sûre ou non ?
- La camionnette plus loin dans la rue : pourrait-elle être une possible vulnérabilité ou une source d'aide en cas de problème ?

Si vous pensez prendre votre propre photo d'une rue la nuit, envisagez d'y intégrer les éléments suivants :

- Vous pouvez avoir une image avec une source de lumière dans la rue dont la position est évidente et un côté de la rue visiblement plus sombre.

- Vous pouvez avoir une image contenant des éléments qui ajoutent des risques. Par exemple, des endroits où une autre personne pourrait se cacher de la personne qui circule, ou bien une rue à forte circulation automobile.

Après avoir passé un peu de temps sur les « pourquoi » des tactiques de sécurité et sur les menaces, posez la question suivante: « **qu'avez-vous besoin de savoir de plus sur cette rue pour prendre de meilleurs décisions afin d'y circuler en toute sécurité?** »

Laissez-leur le temps de réfléchir à leurs réponses.

Ensuite, recueillez les réponses et écrivez-les sur le tableau.

Synthèse de la session. Soulignez certains points importants :

- Les principales stratégies – les pourquoi et les comment – qui sont ressorties de la discussion.
- L'information clé nécessaire à une meilleure évaluation de la situation qui est ressortie de la session.
- Reliez l'activité à l'évaluation des risques en ce sens que pendant l'activité, les participant·e·s ont examiné une situation (la rue sombre) et ont pris quelques décisions concernant leur sûreté et leur sécurité par rapport à cette situation, en se basant sur le contexte, leur expérience et leurs connaissances. Et cela a été fait rapidement.
- Assurer votre sécurité lorsque vous circulez dans une rue sombre la nuit est une expérience courante. À ce moment-là, on peut évaluer le risque (Cette rue est-elle dangereuse ? À quelle vitesse puis-je courir ? Y a-t-il des endroits dans cette rue où je peux demander de l'aide, au cas où ? Suis-je seul·e? Y a-t-il des endroits où quelqu'un pourrait me surprendre dans cette rue ?) et appliquer des stratégies et des tactiques pour les atténuer. Nous atténuons les risques instinctivement, c'est un mécanisme de survie. Il est important de s'en souvenir lorsque l'on aborde l'évaluation des risques.
- La connaissance des risques éventuels dans ce cas précis a permis à chacune et chacun d'entre nous de trouver des stratégies et des tactiques pour réduire les risques.

Conseils pour l'animation

- Il est vraiment important, dans la première partie de l'activité que les participant·e·s ne suranalysent pas. C'est pourquoi cinq minutes suffisent. Ce que nous voulons souligner ici,

c'est l'importance de l'instinct et de l'expérience vécue pour évaluer les risques dans une situation donnée.

- Si vous sentez qu'une ou toutes les personnes participant sont en détresse du fait de devoir réagir à l'expérience de marcher dans une rue sombre, faites une pause. Donnez-leur le temps de respirer. Permettez-leur également de se retirer de l'activité.
- Le but de l'activité est de commencer à étudier l'évaluation des risques. Il n'est pas important de faire correspondre l'activité à la formule standard : risque = menace × probabilité × impact / capacité. L'important est que les participant·e·s puissent formuler les raisons pour lesquelles iels ont décidé de tactiques particulières pour circuler dans une rue sombre la nuit.
- Réitérez qu'il n'y a pas de bonnes ou de mauvaises réponses, seulement des réponses fondées sur l'expérience et le raisonnement.
- Si vous constatez, d'après votre connaissance des participant·e·s, qu'une activité sur le fait de circuler seul·e dans une rue la nuit peut faire ressurgir un traumatisme, vous pouvez utiliser à la place une rue bondée pendant la journée car cela serait sans doute moins traumatisant. Ou bien une rue bondée la nuit, pouvant présenter différents types d'éléments de réflexion sur le risque. Voici quelques exemples de photos que vous pouvez utiliser:

Rue3.jpg Image not found or type unknown *Photo Carl Campbell, El Chopo Saturday Market crowds, sur Flickr.*

Rue4.jpg Image not found or type unknown *Photo Waychen C, Shilin Night Market, sur Flickr.*

Le cycle de vie des données, ou comment comprendre les risques [activité d'approfondissement]

Pour approcher l’évaluation des risques sous l’angle du cycle de vie des données. Toutes et tous les activistes, organisations et mouvements ont affaire aux données, de la compilation/création/collecte à la publication d’informations basées sur des données.

À propos de cette activité d'apprentissage

ativ_aprof_FR.png
Image not found or type unknown

Cette activité d’apprentissage consiste à approcher l’évaluation des risques sous l’angle du cycle de vie des données. Toutes et tous les activistes, organisations et mouvements ont affaire aux données, de la compilation/création/collecte à la publication d’informations basées sur des données.

Cette activité peut être réalisée selon deux approches différentes :

- **L’atelier général** est conçu comme un atelier sur la sécurité numérique en général, destiné à des participant·e·s provenant de différentes organisations et/ou qui n’appartiennent à aucune organisation.

- **L’atelier organisationnel** est destiné à un groupe spécifique et à son personnel. Ce type d’atelier fonctionne avec un contexte général où différentes équipes d’une même organisation se rassemblent pour réaliser une évaluation des risques adaptée à la pratique et au traitement des données dans leur organisation.

Ces deux approches couvrent les mêmes objectifs d’apprentissage et thématiques générales, mais il faudra ajuster les méthodologies et les techniques d’animation à chacun de ces ateliers, à l’aide de scénarios différents.

Objectifs d’apprentissage

Suite à cette activité, les participant·e·s seront en mesure de :

- Comprendre les questions de risque et de sécurité à chaque étape du cycle de vie des données.
- Appliquer des cadres d’évaluation des risques pour leur sécurité personnelle et/ou organisationnelle.

À qui cette activité est-elle destinée ?

Cette activité est conçue pour les activistes individuel·le·s (pour un atelier général sur l’évaluation des risques ou la sécurité numérique), ou pour un groupe (une organisation, un réseau, un collectif) déjà engagé dans un processus d’évaluation des risques. Cette activité peut être proposée selon deux approches différentes, qu’il s’agisse d’un atelier général ou d’un atelier destiné à un groupe spécifique.

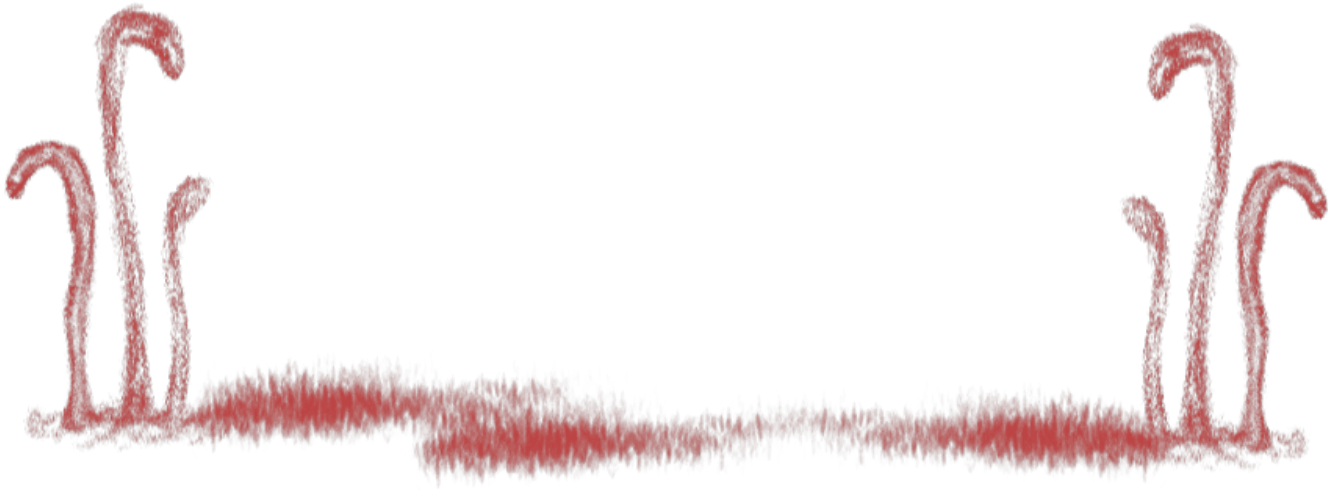
Elle peut également servir à faire un diagnostic permettant de définir des priorités sur les pratiques ou les outils les plus intéressants à traiter lors d’un atelier sur la sécurité numérique.

Temps requis

Cela dépend du nombre de participantes et de participants et de la taille du groupe. En général, cette activité prend un minimum de quatre heures.

Matériel

- Tableau à feuilles mobiles
- Marqueurs
- Projecteur pour présenter le cycle de vie des données et les questions-guides, ainsi que pour les éventuels retours partagés par les participant·e·s suite à l'activité.



Mécanique

Ceci est valable pour un atelier général sur l'évaluation des risques ou sur la sécurité numérique où des activistes issu·e·s de différents contextes se rassemblent le temps de la formation. Les objectifs d'apprentissage restent les mêmes, mais certaines tactiques de formation et d'animation diffèrent de celles d'un atelier destiné à un groupe de personnes plus établi.

Étape 1 : Que publiez-vous ?

Pour cette étape, on demande aux participant·e·s : **que publiez-vous dans le cadre de votre travail d'activiste ?**

L'idée est ici de commencer avec la partie la plus évidente du cycle de vie des données : de la donnée déjà traitée qui est partagée en tant qu'information. Il peut s'agir de rapports de recherche, d'articles, de publications de blogues, de guides, d'ouvrages, de sites web, de

publications sur les médias sociaux, etc.

On peut réaliser cette partie en séance plénière, en mode « popcorn » : la personne animatrice pose une question et demande des réponses brèves aux participant·e·s, comme le maïs dans une poêle !

Étape 2 : Présentation du cycle de vie des données et de questions de sécurité

La présentation a pour but de rappeler aux participant·e·s le cycle de gestion des données. Vous trouverez les points principaux de la présentation :

- dans le diaporama Cycle de vie des données
- et dans la section **Présentation.**

Étape 3 : Temps de réflexion sur les cycles de vie des données personnelles

Regroupez les participant·e·s en fonction de ce qu'iels publient. Demandez-leur de choisir un exemple parmi leurs publications (un article, un rapport de recherche, un livre, etc.) et demandez aux personnes travaillant sur le même type de publication de se regrouper.

Donnez un temps à chaque personne pour retrouver le cycle de vie des données de sa publication, puis demandez-leur de partager leurs réflexions avec les autres membres de leur groupe.

Le temps de réflexion devrait prendre environ 15 minutes, les discussions de groupes environ 45 minutes.

Les questions de la présentation (voir Diaporama et section **Présentation**) permettront de guider le temps de réflexion individuelle.

Pour le travail de groupe, chaque membre du groupe devra aborder avec les autres le cycle de vie des données de sa publication.

Étape 4 : Mise en commun et questions de sécurité

Au lieu de demander à chaque groupe de faire un retour, la personne formatrice-animatrice pose des questions à chaque groupe pour faire ressortir ce dont le groupe a parlé.

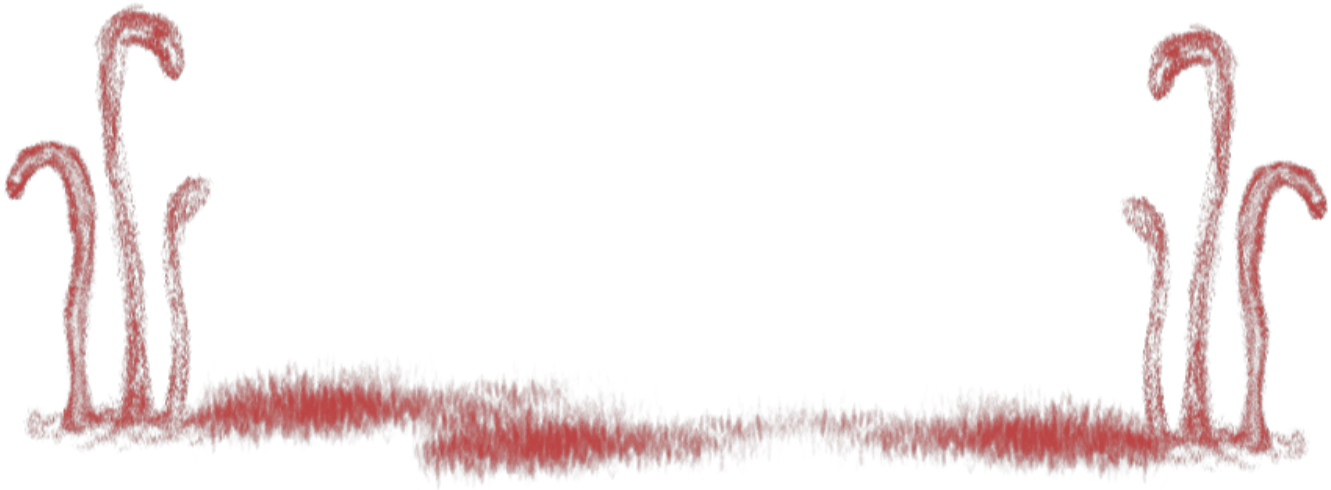
Voici des exemples de questions permettant de faire un bilan du temps de réflexion et des discussions de groupe :

- Quels sont les appareils de stockage de données les plus courants dans le groupe ? Quels sont ceux qui ont été utilisés exclusivement ?
- Quels différences et points communs sont ressortis concernant l'accès au stockage des données dans votre groupe ?
- Et pour le traitement des données ? Quels outils ont été utilisés dans votre groupe ?
- Des personnes dans le groupe ont-elles publié quelque chose qui les ont mises en danger, elles ou une personne de leur connaissance ? Qu'était-ce ?
- Certaines personnes du groupe avaient-elles déjà réfléchi à la question de l'archivage et de l'élimination des données avant aujourd'hui ? Si oui, quelles sont leurs pratiques dans ce domaine ?
- La sécurité et la sûreté ont-elles été sujets de préoccupations au cours du cycle de vie de vos données ? Quelles ont été ces préoccupations ?

Synthèse de l'activité

À la fin des présentations de groupe et de la mise en commun, la personne formatrice-animatrice peut synthétiser l'activité en :

- Pointant les principales observations réalisées.
- Demandant aux participant·e·s de donner les idées clés tirées de l'activité.
- Questionnant les participant·e·s sur de possibles évolutions de leurs pratiques en matière de gestion des données qu'iels ont appris pendant l'activité.



Déroulement d'un atelier organisationnel

Ceci concerne un atelier destiné à une organisation et à son personnel.

Étape 1 : Quelles sont les informations partagées par chaque service/programme/équipe de l’organisation ?

En fonction de la configuration et de la structure de l’organisation, demandez à chaque service ou équipe un exemple d’information qu’iels partagent, que ce soit au sein de l’organisation ou en externe.

Voici quelques exemples pour encourager les réponses :

- Pour des services de communication : en quoi consistent les rapports que vous publiez ?
- Pour des équipes de recherche : en quoi consistent les recherches sur lesquelles vous publiez des rapports ?

- Pour des équipes administratives et/ou financières : qui a accès aux fiches de paye de votre organisation ? Et aux rapports financiers ?
- Pour les services des ressources humaines : que se passe-t-il avec les évaluations de personnel ?

> **Conseil pour l'animation :** Il est bien plus simple de répondre à cette question pour les équipes tournées vers l'extérieur, comme un service de communication ou un programme qui publie des rapports et documents de recherche. Pour les services plus tournés vers l'intérieur, comme la finance et l'administration ou les ressources humaines, la personne formatrice-animatrice peut avoir besoin de passer du temps sur des exemples d'informations que ces services partagent.

Cette étape vise à ce que les différentes équipes reconnaissent qu'elles partagent toutes des informations, en interne comme vers l'extérieur. C'est important puisque chaque équipe devrait pouvoir identifier un ou deux types d'informations qu'elles partagent lorsqu'elles évaluent les risques dans leur pratique de gestion des données.

Étape 2 : Présentation du cycle de vie des données et des questions de sécurité

La présentation a pour but de rappeler aux participant·e·s le cycle de gestion des données. Vous trouverez les points principaux de la présentation :

- dans le diaporama Cycle de vie des données
- et dans la section **Présentation**.

Étape 3 : Travail en groupes

Au sein des équipes, demandez à chaque groupe d'identifier un ou deux types d'informations qu'ils partagent/publient.

Pour établir des priorités, encouragez les équipes à déterminer quelles informations elles souhaitent sécuriser le plus, ou quelles sont les informations les plus sensibles qu'elles partagent.

Ensuite, pour chaque type d'informations partagées ou publiées, demandez aux équipes de remonter le processus afin d'examiner le cycle de vie de ses données. Servez-vous de la présentation ci-dessous pour leur poser des questions clés sur leurs pratiques en matière de gestion des données pour chacune des données publiées ou partagées.

À la fin de ce processus, chaque équipe devrait pouvoir partager avec les autres les résultats de leurs discussions.

En règle générale, il faut compter environ une heure pour ce travail de groupe.

Étape 4 : Présentations de groupes et réflexion sur la sécurité

Selon la taille de l'organisation et le travail réalisé par chaque service, donnez-leur du temps pour présenter les résultats de leurs discussions à leurs collègues. Encouragez chaque équipe à réfléchir à des façons créatives de présenter et de mettre en valeur les points principaux de leurs discussions. Iels n'ont pas besoin de partager la totalité de leurs discussions.

Encouragez les autres participant·e·s à prendre des notes sur ce que les groupes partagent, puisqu'il y aura du temps pour les commentaires et les réactions à la fin de chaque présentation.

Ceci devrait prendre environ 10 minutes par groupe.

Le rôle de la personne formatrice-animatrice consiste ici, outre chronométrer et gérer les réactions, aussi à réagir après chaque présentation. C'est le moment de mettre votre chapeau de personne pratiquant la sécurité.

Quelques sujets sur lesquels il est intéressant de questionner :

- Si le processus de collecte de données est supposé être privé, ne serait-il pas préférable d'utiliser des outils de communication plus sûrs ?
- Qui a accès aux appareils de stockage, en théorie et en réalité ? Si ceux-ci sont physiques, où se trouvent-ils dans les bureaux ?
- Qui peut voir les données brutes ?

En tant que personne formatrice-facilitatrice, vous pouvez aussi profiter de ce moment pour émettre quelques recommandations et suggestions pour rendre les pratiques de l'organisation en matière de gestion des données plus sûres.

> **Conseil pour l'animation :** Consultez l'activité intitulée Outils alternatifs : Réseaux et communications pour mieux guider cet atelier.

Étape 5 : Retour aux groupes : Améliorer la sécurité

Après la présentation de toutes les équipes, celles-ci se reforment pour continuer à discuter et réfléchir aux manières de mieux sécuriser leurs processus de gestion de données et de leurs données elles-mêmes.

L'objectif est ici que chaque groupe planifie des façons d'améliorer la sécurité à chaque étape du cycle de vie de leurs données.

À la fin, chaque équipe devrait avoir quelques plans pour améliorer la sécurité dans leurs pratiques en matière de données.

> **Remarque :** On suppose ici que le groupe a déjà été un peu formé aux bases de la sécurité dans le but de faire ceci. Si ce n'est pas le cas, la personne formatrice-animatrice peut, lors de l'étape 4, suggérer quelques outils, options et processus alternatifs offrant davantage de sécurité pour la pratique du groupe en matière de gestion des données.

Questions-guides pour les discussions de groupes

- Parmi les types de données que vous gérez, lesquelles sont publiques (tout le monde peut en savoir quelque chose), privées (seule l'organisation peut en savoir quelque chose), confidentielles (seule l'équipe et certains groupes de l'organisation peuvent en savoir quelque chose), et comment votre équipe s'assure-t-elle que ces différents types de données sont bien privés et confidentiels ?

- Comment votre équipe peut-elle s’assurer que vous êtes en mesure de gérer qui a accès à vos données ?
- Quelles sont les politiques de conservation et de suppression des données des plateformes dont vous vous servez pour stocker et traiter vos données en ligne ?
- Que peut faire l’équipe pour améliorer la sécurité de ses communications, en particulier les données et informations privées et confidentielles ?
- Quels pratiques et processus l’équipe devrait-elle mettre en place pour préserver le caractère privé et confidentiel de ses données ?
- En quoi devriez-vous changer votre manière de gérer les données pour en améliorer la sécurité ? Revenez sur les résultats du précédent travail de groupe et cherchez ce qui peut être amélioré.
- Quel rôle devrait jouer chaque membre de l’équipe pour réaliser ces changements ?

Étape 6 : Présentation finale des plans d’évolution

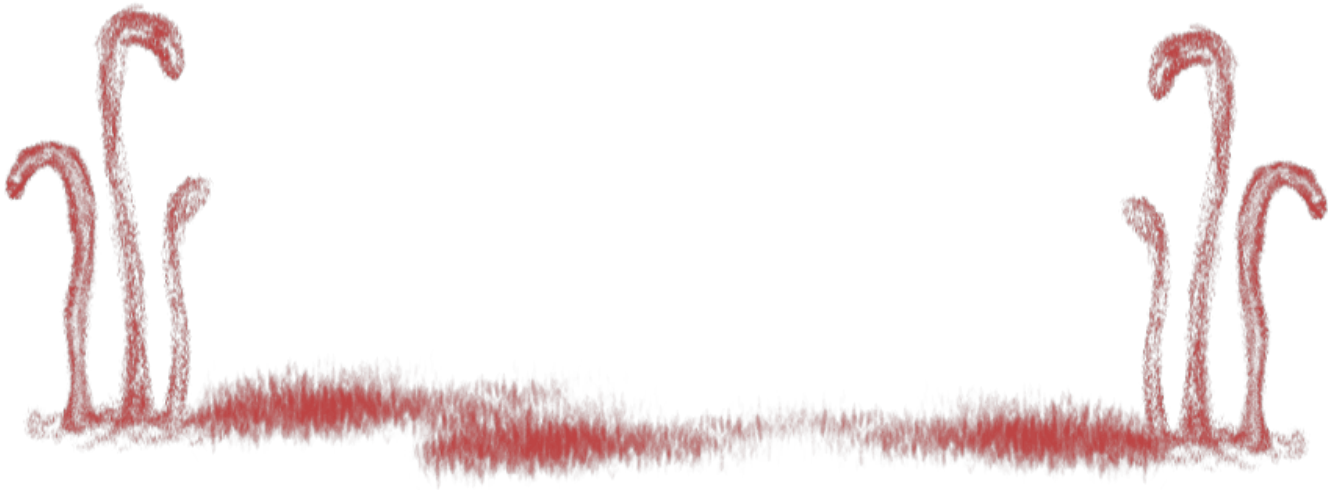
Ici, chaque équipe aura du temps pour présenter comment elle compte améliorer la sécurité de sa gestion des données.

C’est l’occasion pour l’ensemble de l’organisation de mettre en commun des stratégies et des tactiques, et d’apprendre les uns et les unes des autres.

Synthèse de l’activité

À la fin des présentations de groupes et de la mise en commun, la personne formatrice-animatrice peut synthétiser l’activité en :

- Pointant les principales observations réalisées.
- Demandant aux participant·e·s de donner les idées clés tirées de l’activité.
- Se mettant d’accord sur les prochaines étapes pour mettre les plans à exécution.



Présentation et ressources supplémentaires

Présentation

Diaporama : Présentation-Cycle de vie des données.odp

Une autre manière de comprendre les différents échelons des risques consiste à examiner les pratiques d'une organisation en matière de données. Toute organisation a affaire à des données, et chaque service d'une organisation aussi.

Voici quelques points à prendre en compte en matière de sécurité et de sûreté pour chaque phase du cycle de vie des données.

Création/compilation/collecte de données

- Quel type de données sont compilées ?
- Qui crée/compile/collecte les données ?
- Cela peut-il menacer des personnes ? Qui sera menacé pour la publication de ces données ?

- Dans quelle mesure le processus de collecte de données est-il public, privé ou confidentiel ?
- Quels outils utilisez-vous pour assurer la sûreté du processus de collecte de données ?

Stockage des données

- Où les données sont-elles stockées ?
- Qui a accès au stockage des données ?
- Quelles pratiques/processus/outils utilisez-vous pour veiller à la sécurité de l'appareil de stockage ?
- Stockage dématérialisé, stockage physique ou appareil de stockage ?

Traitement des données

- Qui traite les données?
- L'analyse des données menace-t-elle des individus ou des groupes ?
- Quels sont les outils utilisés pour analyser les données ?
- Qui a accès au processus/système d'analyse des données ?
- Lors du traitement des données, des copies secondaires des données sont-elles stockées ailleurs ?

Publication/partage des informations à partir des données traitées

- Où les informations et la connaissance sont-elles publiées ?
- La publication des informations peut-elle menacer des personnes ?
- Quel public visent les informations publiées ?
- Avez-vous le contrôle sur la façon dont les informations sont publiées ?

Archivage

- Où les données et les informations traitées sont-elles archivées ?

- Les données brutes sont-elles archivées, ou uniquement les informations traitées ?
- Qui a accès aux archives ?
- Quelles sont les conditions d’accès aux archives ?

Suppression

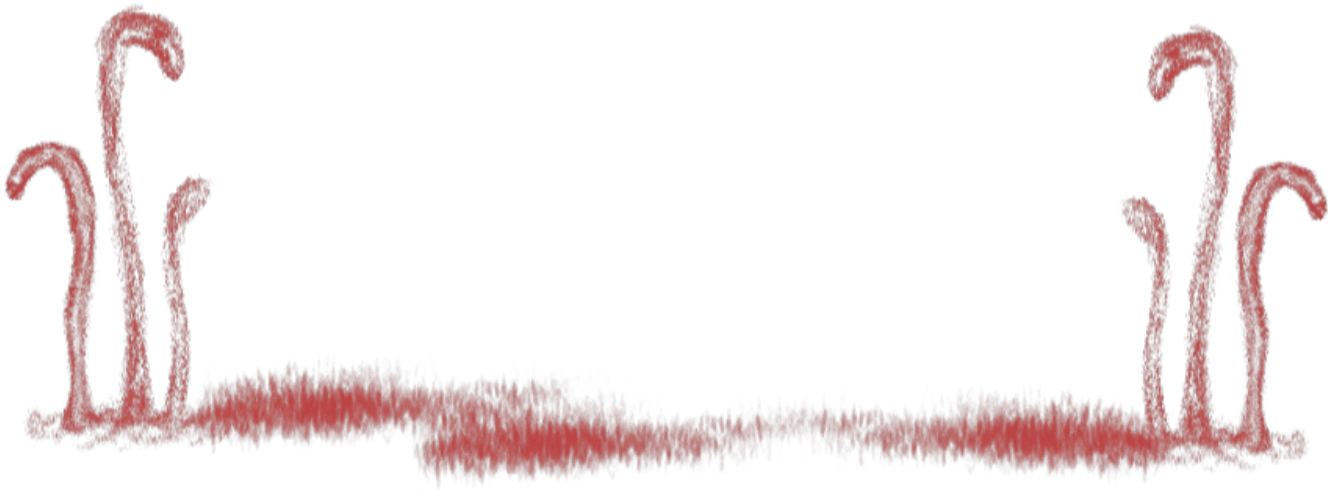
- Quand les données sont-elles écrasées ?
- Sous quelles conditions sont-elles supprimées ?
- Comment s’assurer que toutes les copies ont bien été supprimées ?

Conseils pour l’animation

- Cette activité est une bonne manière de connaître et d’évaluer les contextes, la pratique et les processus utilisés par les participant·e·s en matière de sécurité numérique. Mieux vaut se focaliser sur cet aspect que d’attendre de cette activité qu’elle débouche sur des stratégies et des tactiques pour améliorer la sécurité numérique.
- Pour un atelier auprès d’une organisation, il peut être bon de faire particulièrement attention aux équipes/services administratifs et de ressources humaines. D’une part, dans nombre d’organisations, ce sont les membres du personnel les moins susceptibles d’avoir déjà participé à un atelier sur la sécurité numérique, si bien que de nombreux thèmes et sujets peuvent être nouveaux pour elles et eux. D’autre part, une bonne partie de leur travail étant interne, il se peut qu’iels ne considèrent pas que leurs services « publient » quoi que ce soit. Pourtant, dans de nombreuses organisations, ces services détiennent et traitent un grand nombre de données sensibles (informations sur le personnel, salaires, notes de réunions du conseil, informations bancaires de l’organisation, etc.), il est donc important que le faire remarquer lors de l’atelier.
- Faites également attention aux matériels de stockage physique. S’il y a des tiroirs de classement où des copies imprimées de documents importants sont stockées, demandez où ils se trouvent et qui y a accès physiquement. On a parfois tendance à ne penser qu’aux pratiques de stockage en ligne, en oubliant d’améliorer la sécurité des tactiques de stockage physique.

Ressources supplémentaires (facultatif)

- Voir l'activité tactique Outils alternatifs : Réseaux et communications (du module Créer des espaces sûrs en ligne).
- Voir le module Sécurité mobile (FTX : Redémarrage de sécurité).
- Autodéfense contre la surveillance de l'Electronic Frontier Foundation : si ce guide est surtout destiné à un public basé aux États-Unis, il comporte des sections utiles qui expliquent les concepts utilisés par la surveillance et les outils utilisés pour les contourner.
- Guide de Front Line Defender pour sécuriser les conversations de groupe et les outils de vidéoconférence : un guide utile sur plusieurs services et outils sécurisés de clavardage et de conférence en ligne et qui obéissent aux critères de Front Line Defender en matière de sécurité d'une application ou un service.
- Le site web Confidentialité non incluse de la Fondation Mozilla : il examine les politiques et pratiques en termes de vie privée et de sécurité de différents services, plateformes et appareils pour évaluer leur conformité aux critères élémentaires de sécurité de Mozilla, portant sur le chiffrement, les mises à jour de sécurité et les politiques de confidentialité.



Organisation de manifestations et évaluation des risques [activité tactique]

Guider un groupe de personnes qui planifie une manifestation dans la réflexion et la prise en compte des risques et des menaces auxquels elles peuvent être confrontées. Peut s'appliquer aux manifestations hors ligne ou en ligne ainsi qu'aux manifestations ayant des composantes hors ligne et en ligne.

À propos

activ_tact_FR.png
Image not found or type unknown

Cette activité vise à guider un groupe de personnes qui planifie une manifestation dans la réflexion et la prise en compte des risques et des menaces auxquels elles peuvent être confrontées. Cette activité peut s'appliquer aux manifestations hors ligne ou en ligne ainsi qu'aux manifestations ayant des composantes hors ligne et en ligne.

Il ne s’agit pas d’une activité de planification de manifestation, mais plutôt d’une activité d’évaluation des risques en vue d'une manifestation. On suppose qu’avant la tenue de cette activité, le groupe aura déjà procédé à une planification initiale de l'objet de la manifestation et de ses principales stratégies, tactiques et activités.

Objectifs d’apprentissage

À travers cette activité, les participant·e·s apprendront à :

- Comprendre les différents risques associés aux activités de la manifestation.
- Élaborer un plan pour répondre aux risques identifiés afin de tenir une manifestation plus sûre.

À qui s’adresse cette activité ?

Cette activité est utile à un groupe de personnes (organisation, réseau, collectif) qui a convenu de planifier ensemble une manifestation.

Avant cette activité, le groupe devrait déjà avoir planifié sa manifestation. Les principales stratégies, tactiques et activités ont donc déjà fait l’objet de discussions ayant abouties à un accord.

Temps requis

L’activité durera au minimum quatre heures.

Matériel

- Un grand mur où l’on peut épingler des notes autocollantes (post-it) et des feuilles d’un tableau à feuilles mobiles. S’il n’y a pas de mur adapté à cet effet, il faut un espace dégagé au sol où les participant·e·s pourront faire ce travail ensemble.
- Des marqueurs.
- Des notes autocollantes (post-it).
- Des appareils permettant de documenter électroniquement les discussions. Il est important de désigner des personnes au sein du groupe pour documenter les discussions et de s’assurer que si la documentation est partagée, elle le soit par des canaux sécurisés.

Mécanique

Atelier destiné à un groupe qui planifie une manifestation commune

Cette activité comporte trois phases principales :

- La phase 1 consiste à **examiner le risque** du point de vue des personnes organisatrices et partisanes ainsi que des adversaires, en tant que sources de menaces (menaces directes et indirectes et se confronter aux façons dont la manifestation pourrait échouer). La phase 1 est divisée en trois exercices conçus pour que le groupe parvienne à une compréhension commune des risques éventuels qu'encourt leur manifestation.
- La phase 2 consiste à **élaborer des stratégies** visant à atténuer les vulnérabilités et les échecs éventuels de la manifestation et à déterminer le rôle qu'ont les personnes organisatrices dans ce plan d'atténuation.
- La phase 3 porte sur la mise en place de **communications internes sécurisées** entre les personnes participantes.

Phase 1 : Évaluer les sources de risques

Cette phase comporte quelques niveaux de participation et d'interaction afin d'évaluer les sources possibles de risques pour la manifestation. Pour rendre les mécaniques plus claires, les différents niveaux sont indiqués comme des « exercices ».

Préparer une feuille du tableau pour chacun des éléments suivants :

- **Personnes organisant la manifestation** : groupes et personnes participant à la planification de la manifestation. Ils comprennent également les allié·e·s.
- **Personnes partisanes** : groupes et personnes dont vous pensez qu'elles et ils participeront aux actions de la manifestation.
- **Adversaires de la manifestation** : groupes et personnes sur lesquels la manifestation aura des effets négatifs, ainsi que celles et ceux qui soutiennent ces personnes.

- **Activités de la manifestation** : les actions prévues lors de la manifestation et les endroits où elles se dérouleront. Ces activités peuvent se dérouler en ligne et hors ligne.

Exercice 1 : Définir les activités de la manifestation et les personnes y participant

Donnez aux participant·e·s le temps et l'espace nécessaires pour remplir chacune de ces feuilles du tableau avec des notes autocollantes contenant leurs réponses. Iels peuvent aussi simplement écrire directement sur les feuilles du tableau.

> **Conseil pour l'animation :** Pour procéder de manière plus organisée, surtout si le groupe est composé de plus de sept personnes, répartissez les gens en quatre groupes. Chaque groupe travaillera d'abord sur une feuille du tableau. Un groupe peut commencer par « Les personnes organisant la manifestation » et un autre groupe par « Les personnes partisanes » et ainsi de suite. Donnez-leur le temps de remplir leurs réponses pour leur feuille du tableau, puis demandez-leur de passer à la feuille suivante jusqu'à ce que tous les groupes aient eu le temps de toutes les remplir. C'est ce que l'on appelle la méthode World Café.

Exercice 2 : Étudier les personnes organisatrices, partisanes et adversaires

Une fois que les feuilles sont remplies avec les réponses, demandez-leur de se séparer en deux groupes :

- Le groupe 1 prendra les feuilles concernant les personnes organisatrices et partisanes
- Le groupe 2 prendra les feuilles concernant les adversaires

Les feuilles concernant les **Activités** resteront dans la partie commune pour que chaque personne puisse les consulter.

Chaque groupe aura sa propre série de questions-guides pour commencer à dévoiler où se situent les risques dans leur domaine.

Pour les personnes organisatrices et partisanes, les questions-guides sont les suivantes :

- Quelles personnes organisatrices font face à des menaces ? Quelles sont-elles ? Quels peuvent-être les effets sur la manifestation ?
- Existe-t-il des conflits internes parmi les personnes organisatrices ? Des tensions que l'on devrait connaître ? Quelles peuvent-être les conséquences sur l'organisation ?
- Parmi les personnes partisanes attendues, quelles sont celles qui risquent de subir beaucoup de réactions hostiles ?
- Quelles menaces de réactions hostiles peuvent être anticipées ? Y a-t-il eu des manifestations similaires ayant déjà suscité des réactions hostiles ? Quelles étaient ces réactions ?
- Où pourraient se produire les réactions hostiles ou les attaques ? Connaissez-vous des médias sociaux particulièrement ciblés par les adversaires ? Quel pourrait être les répercussions des réactions hostiles sur les réalités hors ligne, pendant et après la manifestation ?

Pour les adversaires, les questions-guides sont les suivantes :

- Quels seront les adversaires les plus actives et actifs contre la manifestation ?
- Où se rassemblent les adversaires ? Où est-ce qu’ils et elles se rassemblent hors ligne comme en ligne ?
- Qui sont les personnes meneuses et influentes parmi les adversaires ?
- Quelles capacités sont à leur disposition ?
- Que peuvent-elles et ils faire contre la manifestation et les personnes s’y impliquant ?
- Comment les adversaires peuvent influer sur la planification de la manifestation ?
- Comment peuvent-elles et ils perturber les activités prévues pendant la manifestation ?
- À quoi pourrait ressembler une réaction hostile après la manifestation ? Comment les adversaires pourraient-elles et ils tenter de perturber le message de la manifestation par cette réaction ? Qui serait ciblé ? Où cela se produirait-il et quel serait le rôle des médias sociaux ?

> **Conseil pour l'animation :** De nos jours, la plupart des manifestations ont des composantes en ligne et hors ligne. Les questions ci-dessus s'appliquent aux scénarios, manifestations et contextes en ligne comme hors ligne. Mais si vous constatez que les participant·e·s se concentrent trop sur les contextes hors ligne, vous pouvez leur poser des questions sur les contextes en ligne des personnes organisatrices et partisanes et des adversaires. Si iels ont tendance à se concentrer sur les facteurs en ligne, posez-leur des questions sur les contextes hors ligne. Demandez-leur comment les activités ou les événements en ligne peuvent avoir une répercussion sur les activités ou les événements hors ligne, et vice versa.

La discussion de groupe devrait prendre environ entre 45 minutes et une heure.

À la fin de la discussion de groupe, chaque groupe fera part des résultats de sa discussion. Pour cette mise en commun, chaque groupe doit se concentrer sur les questions suivantes :

Pour le groupe des personnes organisatrices et partisanes:

- Qui, parmi les personnes organisatrices et partisanes, fait face actuellement à des menaces ? Quelles sont ces menaces ?
- À quel genre de réactions hostiles vous attendez-vous à l'encontre des personnes organisatrices et partisanes pour leur participation à la manifestation ?
- Y avait-il des conflits ou des tensions internes susceptibles de poser un risque à la manifestation et quels sont-ils ?

Pour le groupe qui a travaillé sur les adversaires:

- Qui parmi les adversaires est susceptible de chercher à perturber la manifestation ?
- Quel genre de perturbation prévoyez-vous ?
- En quoi est-ce différent pour les différentes étapes de la manifestation : planification, pendant et après ?

Il est également bon de demander aux groupes d'être aussi précis que possible dans leur partage avec les autres.

Exercice 3 : Réfléchir à l’éventualité d’un échec

Cet exercice vise à mettre en lumière les différentes façons dont la manifestation peut échouer.

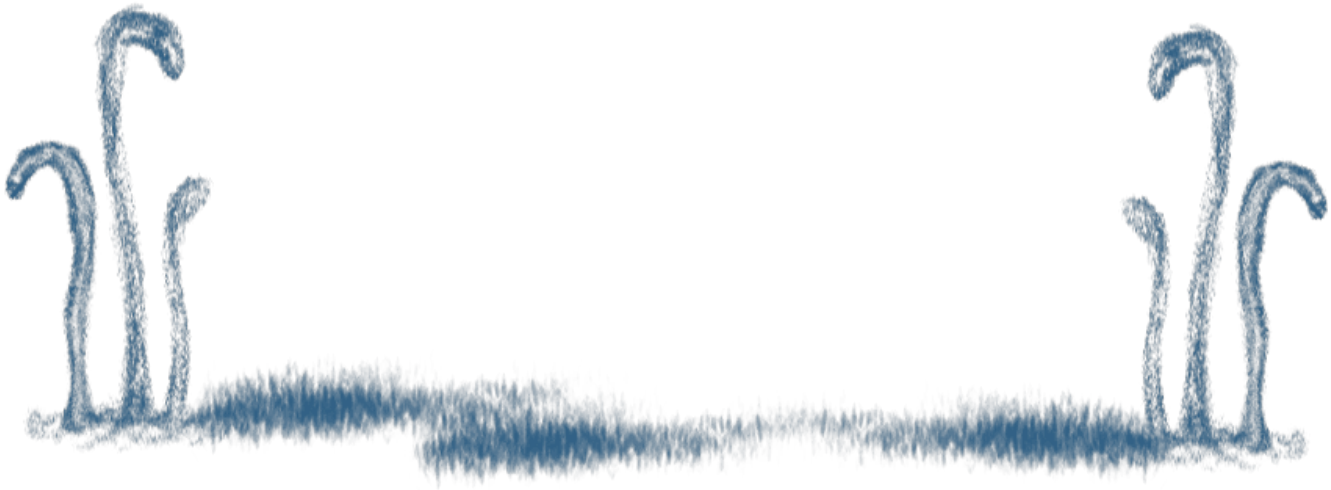
On donnera ensuite du temps aux participant·e·s pour réfléchir à cette question : **quelles sont les choses qui ne doivent PAS se passer dans cette manifestation ?**

Pour mieux décortiquer cette question importante, les questions suivantes pourraient aider le groupe :

- Pensez à vos personnes organisatrices et partisanes : quels effets négatifs pourrait avoir sur eux la manifestation ?
- Si la manifestation se déroule en ligne et hors ligne, comment les adversaires peuvent-elles et ils la perturber dans les deux espaces ?
- Pensez aux espaces où se déroulent les activités de la manifestation : qu’est-ce que vous voulez éviter ?
- Pensez aux activités de la manifestation : qu’est-ce qui pourrait les faire échouer ?

Demandez-leur de réfléchir aux discussions qu’iels ont eues et aux retours qu’iels ont entendus. Demandez-leur d’écrire leurs réponses sur des notes autocollantes séparées, puis de les afficher au mur après quelques minutes de réflexion.

Regroupez les réponses pour dégager des thèmes généraux à approfondir.



Phase 2 : Planifier des stratégies et des tactiques d’atténuation

Exercice 1 : Le groupe cherche à atténuer les éventuelles vulnérabilités et l’échec

En fonction des regroupements de l’exercice 3 de la phase 1, divisez les participant·e·s en groupes.

Chaque groupe discutera des questions suivantes :

- Que pouvez-vous faire pour empêcher cette issue défavorable ?
- Quelles stratégies, approches et protocoles de sécurité seront nécessaires pour l’éviter ?
- Les stratégies sont-elles différentes selon qu’il s’agit de la planification, de la manifestation elle-même et de la suite ?
- Que ferez-vous si cette éventuelle issue défavorable devient réalité ? Quelles mesures prendrez-vous ?
- Qui devrait prendre en charge ces stratégies ?

À la fin de la discussion, chaque groupe devrait disposer d’une liste d’approches et de stratégies ainsi que de protocoles de sécurité (règles) en rapport avec l’issue négative. Ils doivent être énumérés sur une feuille du tableau et/ou documentés électroniquement. Organisez-les en fonction

des différentes étapes de la manifestation : avant, pendant et après. Chaque groupe présentera sa liste aux autres en vue d'une discussion.

Le rôle de la personne formatrice-animatrice est ici de faire un retour sur les approches et les stratégies, de suggérer des améliorations (au besoin) et de trouver des stratégies communes dans les groupes.

Exercice 2 : Discussion sur les rôles

Dans le groupe au complet, discutez des rôles nécessaires pour atténuer les issues défavorables, adhérer aux protocoles de sécurité et gérer les communications sécurisées avant, pendant et après les activités de la manifestation. Il serait important que le groupe finalise ces rôles et détermine qui les remplira.

Phase 3 : Communication sécurisée

Ici, la personne formatrice-animatrice peut présenter des options pour des communications sécurisées pendant la tenue de la manifestation.

Le groupe peut ensuite passer du temps à l'installation et à s'assurer qu'iels peuvent communiquer par le canal choisi.

> Pour vous aider à planifier cet aspect, consultez l'activité Outils alternatifs : Réseaux et communications et le module sur la Sécurité mobile.

> **Note sur la sécurité :** Une façon de s'exercer avec ces outils est de s'assurer que les personnes qui documentent sont en mesure de partager des copies de leurs notes et de leurs documents au moyen de canaux de communication sécurisés.

Adaptation pour un atelier général

En général, les activités d’évaluation des risques sont plus efficaces lorsqu’elles sont menées avec des groupes qui ont des objectifs, des contextes et des scénarios de risques communs (c’est-à-dire lors d’interventions d’évaluation des risques d’une organisation ou d’évaluation des risques pour un réseau d’organisations). C’est pourquoi cette activité a été conçue pour un groupe de participant·e·s prévoyant déjà de mener une manifestation ensemble et ayant fait une planification initiale de leur manifestation commune. Mais l'activité peut être adaptée à un scénario de sécurité numérique plus général, dans lequel des personnes de différents contextes envisagent d’organiser leur propre manifestation avec leurs groupes.

Afin d’adapter cette activité à un usage plus général, avoir un exemple de manifestation sera une bonne façon d’amener les participant·e·s à pratiquer cette activité et à en tirer des leçons qu’iels pourront rapporter à leurs groupes/réseaux/collectifs de manière à évaluer les risques pour leurs manifestations réelles.

Quelques lignes directrices sur la création d’un exemple de manifestation :

- **Situer la manifestation dans la réalité :** il est important de situer la manifestation dans un contexte réel, car l'exemple aura alors le cadre et les paramètres d’une manifestation réelle, et les participant·e·s pourront être plus précises et précis dans leur analyse et leurs stratégies.
  Si les participant·e·s viennent toutes et tous d’un même pays, situez la manifestation dans ce pays. Si iels viennent de pays différents, utilisez une manifestation régionale.
- **Concevez un exemple de manifestation portant sur une question qui touche les participant·e·s** : la manifestation leur sera ainsi familière même si elle est imaginaire. Iels en auront peut-être déjà organisé une ou y auront participé.
- **Énoncez les exigences portées par la manifestation ou ses objectifs** : faites les clairement correspondre à la question étudiée pour faciliter l’exercice.
- **Concevez des activités en ligne et hors ligne** : assurez-vous que lorsque vous identifiez les activités de la manifestation, vous disposez de tactiques à la fois en ligne et hors ligne. Soyez précis·e : où auront lieu ces activités, quand auront-elles lieu, combien de temps dureront-elles ?

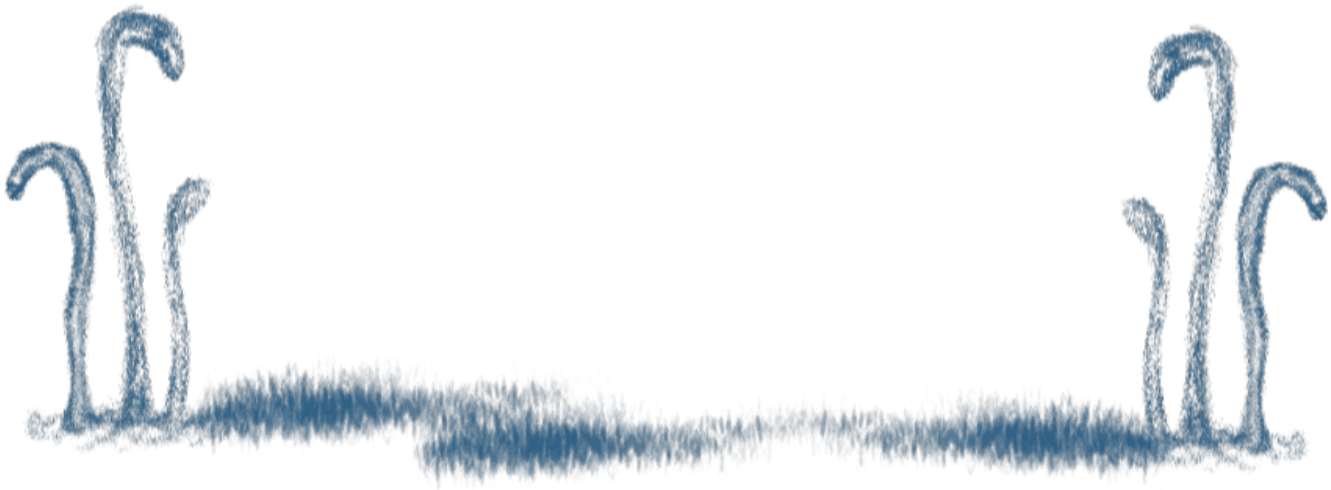
- **Inspirez-vous d’une manifestation réelle** : si vous connaissez une manifestation qui peut convenir aux participant·e·s, utilisez-la comme exemple.

La clé pour une manifestation d’exemple est d’essayer de simuler autant que possible un scénario de manifestation réelle. Une fois de plus, les activités d’évaluation des risques les plus efficaces sont appliquées à des cas précis.

Vous devrez également trouver les bons moyens et organiser votre temps pour que les participant·e·s puissent apprendre et assimiler l’exemple de manifestation. Vous pouvez donner les détails sur l’exemple de manifestation avant la formation, mais ne supposez pas que tout le monde a eu le temps de les lire avant l’atelier. Vous pouvez présenter le modèle au début de l’atelier et distribuer des documents pour que chaque groupe dispose des informations nécessaires pour les phases et les exercices de cette activité.

Ressources supplémentaires

- Évaluation des risques et mouvements sociaux (Ressource essentielle de ce module)



Les bases de l’évaluation des risques [ressource essentielle]

Cette section explore les bases de l'évaluation des risques (en ligne et hors ligne) dans une perspective féministe.

Introduction

Nous évaluons constamment nos risques. C’est comme cela que nous survivons. C’est un processus qui ne se limite pas à la sécurité numérique et/ou de l’information.

Quand on marche la nuit dans une rue tranquille, on prend des décisions – de quel côté de la rue marcher, comment se comporter, à quoi se préparer, comment marcher – basées sur la manière dont nous appréhendons la situation : *Cette rue est-elle connue pour être dangereuse ? Cette rue se trouve-t-elle dans un quartier dangereux ? Est-ce que je connais quelqu’un qui habite dans cette rue et pourrait me venir en aide ? Est-ce que je peux courir vite s’il se passe quelque chose ? Est-ce que je transporte quelque chose de valeur que je peux marchander en cas de problème ? Dans quelle partie de cette rue vaut-il mieux marcher pour éviter un éventuel danger ?*

Quand nos organisations montent un nouveau projet, on tient compte de ce qui pourrait le faire échouer. Lors de la conception, on prend des décisions basées sur nos connaissances du contexte et des facteurs qui pourraient empêcher notre projet d’aboutir.

Quand on organise des manifestations, on cherche à garantir la sécurité de celles et ceux qui y participent. On organise des systèmes de surveillance mutuelle. On s’assure d’avoir un soutien juridique immédiat en cas d’arrestations. On établit des stratégies pour mener une manifestation pacifique et ainsi amoindrir les risques pour les personnes qui participent. On prévoit des personnes chargées de la sécurité de la manifestation.

Si estimer nos risques personnels peut être une pratique instinctive, l'évaluation des risques est un processus spécifique, le plus souvent collectif, visant à examiner comment éviter les menaces et/ou réagir face à ces menaces.

Évaluation des risques : En ligne et hors ligne

En ligne, évaluer nos risques est loin d'être aussi instinctif, et ce pour plusieurs raisons. Nombre d'entre nous ne comprenons pas comment fonctionne l'internet et où sont ses menaces et risques, bien que ceux-ci continuent à évoluer et s'amplifier. Certaines personnes ne perçoivent pas la « réalité » des activités, des actions et du comportement en ligne et pensent que leurs effets sont moins sérieux que ce qui nous arrive physiquement. A contrario, certaines personnes ont vécu ou connaissent des personnes ayant vécu des incidents où leurs activités en ligne ont affecté leur vie « réelle » (arnaques sur des sites de rencontre, échanges tabous via internet dévoilés publiquement, arrestation d'activistes s'étant exprimé·e·s contre leur gouvernement) si bien qu'elles ont tendance à avoir une vision paranoïaque de l'internet.

En réalité, pour de nombreuses personnes activistes, cette opposition binaire entre en ligne et hors ligne est fausse. La plupart utilisent régulièrement des appareils numériques (téléphones et ordinateurs portables, tablettes, ordinateurs, etc.) et des services, des applications et des plateformes sur l'internet (Google, Facebook, Viber, Instagram, WhatsApp, etc.) dans leur travail, que ce soit pour s'organiser ou pour le plaidoyer. Notre manière de nous organiser et de faire notre travail d'activistes évolue continuellement avec les progrès et le développement technologique. L'internet et les technologies numériques font aujourd'hui partie intégrante de notre infrastructure organisationnelle. Nous nous en servons pour communiquer, organiser des activités, renforcer notre communauté, ou encore comme lieu d'activités. Les rencontres en présentiel et les activités de plaidoyer sont souvent accompagnées d'une participation en ligne, notamment sur les médias sociaux et avec des hashtags. Dans les mouvements de protestation récents, il y a souvent un flot ininterrompu entre mobilisations, organisation et rencontres à la fois en ligne et hors ligne.

Au lieu de percevoir ce qui se passe sur l'internet comme quelque chose de séparé de nos réalités physiques, pensez les réalités hors ligne <-> en ligne comme des entités interconnectées et poreuses. Nous existons dans les deux, la plupart du temps simultanément. Ce qui se passe dans l'une influe sur ce que nous sommes dans l'autre.

Cela signifie également que les risques et menaces passent du monde en ligne au monde hors ligne et vice versa. C'est ainsi que les stratégies avancées de surveillance d'État à l'encontre des activistes et de leurs mouvements exploitent l'utilisation non sécurisée des technologies (p. ex. quand on clique sur des liens non vérifiés, ou qu'on télécharge et qu'on ouvre des documents non vérifiés) pour rassembler des informations concernant ces activistes et leurs groupes ou mouvements, qui pourront au final amener à une surveillance physique. Toute personne ayant été victime de violence en ligne basée sur le genre connait les effets psychosociaux de ce type d'attaque et de harcèlement. **Dans certains cas, la cyberviolence basée sur le genre prend une telle ampleur qu'elle affecte la sécurité physique des personnes visées. Différentes formes de cyberviolences basées sur le genre (harcèlement, doxxing, intimidation) sont des tactiques utilisées à l'encontre des féministes et des activistes queer pour les menacer, les réduire au silence ou les obliger à obéir.**

Cette porosité des menaces et des risques entre le hors-ligne et le en-ligne peut sembler insurmontable lorsqu'on y réfléchit : *par où commencer pour évaluer et savoir en quoi consistent les menaces et d'où elles proviennent, et comment établir des stratégies pour y remédier ?*



Qu'est-ce que l'évaluation des risques ?

L'évaluation des risques est *le début d'un processus* permettant de mieux résister vis-à-vis des contextes et menaces en constante évolution. Son but est de mettre en capacité à concevoir des stratégies et tactiques d'atténuation des risques et à prendre des décisions plus éclairées.

En termes génériques, le risque est l'exposition à une possibilité de préjudice, de nuisance, ou de perte.

Dans le contexte de l'évaluation des risques, il s'agit de la capacité (ou de l'incapacité) d'un individu/organisation/collectif à remédier aux répercussions d'une menace qui a été mise à exécution, ou de la capacité d'un individu/organisation/collectif à éviter qu'une menace ne soit mise à exécution.

Il existe une formule connue d'évaluation des risques :

Risque = menace x probabilité x répercussions/capacité

Avec les définitions suivantes :

- Une **menace** est toute action négative à l'encontre d'une personne ou d'un groupe.
  - Les menaces directes sont l'intention déclarée de nuire.
  - Les menaces indirectes sont celles provoquées par un changement de situation.
  - Pour définir une menace, il convient d'en identifier l'origine. Ou mieux, de savoir de qui elle provient.

- La **probabilité** est le niveau de risque qu'une menace devienne réalité.
  - Lié au concept de probabilité est celui de vulnérabilité. Cette dernière peut concerner la situation géographique, les pratiques et le comportement de l'individu ou du groupe, qui augmentent les possibilités de mise à exécution d'une menace.
  - Elle concerne également la capacité des groupes/individus à l'origine de la menace, notamment par rapport à l'individu/groupe menacé.
  - Pour évaluer la probabilité, demandez si des personnes ou un groupe de votre connaissance ont des exemples concrets de menaces et comparez cette situation à la vôtre.

- La **répercussion** est ce qui arrive une fois que la menace a été mise à exécution : les conséquences de la menace.

- Une répercussion peut porter sur un individu, une organisation, un réseau ou un mouvement.
- Plus le niveau et le nombre de répercussions d’une menace est élevé, plus le risque est grand.

- Les **capacités** sont les compétences, les forces et les ressources auxquelles un groupe a accès pour réduire la probabilité de la menace ou remédier à ses répercussions.



Étude de cas (menaces et tactiques d'atténuation)

Étude de cas : Deya

En guise d’illustration, examinons l’expérience fictive mais relativement commune de Deya. Deya est une activiste féministe qui se sert de son compte sur Twitter pour interpeller les gens qui font la promotion de la culture du viol. Cela a amené Deya à recevoir des insultes et des menaces en ligne.

La menace qui la préoccupe le plus provient des personnes promettant de trouver l'adresse de son domicile et de diffuser cette information sur l'internet pour inviter les gens à lui nuire physiquement. Dans ce cas, la répercussion est claire : un dommage physique à l'encontre de Deya. Il y a d'autres menaces, comme harceler son employeur pour qu'elle soit renvoyée, et harceler ses ami·e·s en ligne.

Pour mettre en œuvre une évaluation des risques, Deya va devoir examiner chaque menace et l'analyser pour en évaluer la probabilité et les répercussions, afin de planifier comment atténuer les risques qui pèsent sur elle.

Menace nº1 : Trouver où elle habite et partager cette information en ligne

La plupart des menaces proviennent de comptes en ligne qu'elle ne connaît en majorité pas et dont elle ne peut vérifier s'ils sont réels ou falsifiés. Elle reconnaît que certaines de ces personnes proférant des menaces en ligne sont connues pour leurs attaques en ligne contre les femmes. Elle sait déjà, de leurs attaques précédentes, que certaines données personnelles ont parfois été publiées en ligne, ce qui suscite chez elle un véritable sentiment de peur pour sa sécurité personnelle.

Y a-t-il pour elle une manière d'empêcher que cela se produise ? Quelle est la probabilité pour ses harceleurs et ses agresseurs de découvrir où elle habite ? Elle doit chercher s'il est possible que son adresse soit déjà disponible sur l'internet ou que l'un de ses agresseur·e·s puisse la mettre à disposition.

Pour évaluer cela, Deya peut commencer par une recherche sur elle-même et les informations disponibles en ligne la concernant, pour vérifier s'il y a des espaces physiques associés avec elle et si ceux-ci peuvent permettre de déterminer sa localisation réelle. Si elle découvre que l'adresse de son domicile est en ligne, que peut-elle faire ? Si elle découvre qu'il est possible de rechercher son adresse sur l'internet, peut-elle éviter qu'elle reste publique ?

Deya peut également évaluer la vulnérabilité et/ou la sécurité de son domicile. *Vit-elle dans un immeuble gardé et avec des protocoles d'accès pour les non-locataires ? Vit-elle dans un appartement qu'elle doit sécuriser elle-même ? Vit-elle seule ? Quels sont les points faibles de son domicile ?*

Deya va également devoir évaluer ses propres capacités et ressources pour se protéger. *Si l'adresse de son domicile est rendue publique, peut-elle partir vivre autre part ? Qui pourrait lui offrir son soutien pendant ce temps ? Y a-t-il des autorités auprès de qui demander une protection ?*

Menace nº2 : Harceler son employeur pour qu'elle soit renvoyée de son travail

Deya travaille pour une ONG en faveur des droits humains et ne risque donc pas d'être renvoyée. Mais l'adresse des bureaux de l'organisation est bien connue dans sa ville et disponible sur leur site web.

Pour Deya, la menace d'un renvoi est faible. Mais les informations publiques sur son ONG peuvent être source de vulnérabilité pour sa sécurité physique et celle de tout le personnel.

Dans un tel scénario, c'est à l'organisation de réaliser sa propre évaluation des risques en raison des menaces qui pèsent sur une membre de son personnel.

Que faire avec les menaces ? Tactiques générales d'atténuation des risques

Au-delà d'identifier et analyser les menaces, la probabilité, les répercussions et les capacités, l'évaluation des risques consiste aussi à établir un plan pour atténuer tous les risques identifiés et analysés.

Il existe cinq méthodes générales pour atténuer les risques :

Accepter le risque et établir des plans de secours

Certains risques sont inévitables. Ou certains objectifs valent la peine de prendre un risque. Cela ne signifie pas pour autant qu'on peut les ignorer. Créer un plan de secours consiste à imaginer le risque et ses pires répercussions, et à prendre des mesures pour gérer la situation.

Éviter le risque

Cela signifie réduire la probabilité qu'une menace soit mise à exécution. Il peut s'agir de mettre en place des politiques de sécurité pour améliorer la sécurité du groupe. Il peut également s'agir de modifier certains comportements pour augmenter les chances d'éviter un risque en particulier.

Contrôler le risque

Un groupe peut décider de se focaliser sur les répercussions d'une menace plutôt que sur la menace elle-même. Contrôler les risques consiste à réduire la gravité des répercussions.

Transférer le risque

Faire en sorte qu'une ressource extérieure prenne à sa charge le risque et ses répercussions.

Surveiller l'évolution de la probabilité et des répercussions du risque

C'est la tactique habituelle pour atténuer les risques de faible niveau.

Dans le cas de Deya

Pour continuer avec l'exemple de Deya, différentes possibilités s'offrent à elle sur la base de son analyse de chaque menace, de la probabilité pour chacune d'entre elles d'être mise à exécution, des répercussions de chacune d'entre elles, et de ses propres capacités à gérer la menace et/ou ses répercussions.

Dans un scénario où l'adresse du domicile de Deya est déjà disponible sur l'internet, il lui faudra accepter le risque et concentrer ses efforts sur la mise en place de plans de secours. Ces plans peuvent aller de l'amélioration de la sécurité de son domicile au déménagement. Les possibilités dépendent des réalités et contextes existant pour Deya.

L'autre option pour Deya dans un tel scénario consiste à demander au site qui publie son adresse la retirer. Cette tactique n'est cependant pas infaillible. Elle lui permettra d'éviter le risque dans le cas où aucun de ses harceleuses et harceleurs n'aurait encore vu son adresse. Mais si son adresse a été vue et qu'une capture d'écran en a été faite, Deya n'aura plus grand-chose à faire pour en éviter la divulgation.

Dans un scénario où l'adresse de Deya n'est ni publique ni disponible sur l'internet, elle a un certain répit lui permettant d'éviter le risque. Que peut faire Deya pour éviter que les personnes la

harcelant ne découvrent l'adresse de son domicile ? Elle peut par exemple retirer ses publications géolocalisées près de chez elle et arrêter de géolocaliser en temps réel ses publications.

Dans les deux scénarios (selon que son adresse soit publique ou non), Deya peut également contrôler le risque en se concentrant sur la protection de son domicile.

De bonnes stratégies d'atténuation des risques impliquent de réfléchir à des stratégies préventives et aux mesures à prendre en cas d'incident. Autrement dit, évaluer ce qu'on peut faire pour éviter une menace et ce qu'on peut faire quand la menace est mise à exécution.

Stratégies de prévention

- De quelles capacités disposez-vous pour éviter la réalisation de cette menace ?
- Quelles actions allez-vous entreprendre pour empêcher la réalisation de cette menace ? Comment allez-vous modifier les processus dans le réseau pour empêcher cette menace de se réaliser ?
- Est-il nécessaire de créer des politiques et des procédures en ce sens ?
- De quelles compétences allez-vous avoir besoin pour éviter cette menace ?

Réponse aux incidents

- Que ferez-vous quand la menace se sera concrétisée ? Quelles mesures prendrez-vous à ce moment-là ?
- Comment atténuerez-vous la gravité des répercussions de cette menace ?
- De quelles compétences avez-vous besoin pour prendre les mesures nécessaires face à cette menace ?



Quelques rappels

N’oubliez pas…

Les évaluations de risques sont limitées dans le temps

On les réalise sur une période de temps spécifique, généralement lorsqu’une nouvelle menace se présente (p. ex. un changement de gouvernement, une modification législative, des modifications dans les politiques de sécurité d’une plateforme), lorsqu’une menace se précise (p. ex. le harcèlement en ligne d’activistes, des rapports faisant état du piratage de comptes d’activistes), ou lors de changements dans un collectif (p. ex. un nouveau projet, une nouvelle direction). Il est donc important de refaire ces évaluations régulièrement, étant donné l’évolution des risques en fonction de l’apparition et de la disparition des menaces, et de la capacité d’un groupe et d’individus dans ce groupe à réagir et à surmonter les répercussions d’une menace.

L’évaluation des risques n’est pas une science exacte

Dans un groupe sujet à une évaluation des risques, chaque personne a un point de vue et une posture qui influencent tant sa capacité à connaître la vraisemblance de la concrétisation d’une menace que ses capacités à éviter une menace ou à répondre à ses répercussions. L’objectif d’une évaluation des risques est de comprendre collectivement ces différentes perspectives présentes dans le groupe et d’avoir une vision commune des risques auxquels le groupe est confronté. Les évaluations de risques sont relatives. Il se peut que les mêmes risques et menaces pèsent sur différents groupes de personnes, mais ceux-ci n’auront pas les mêmes capacités pour les éviter ou réagiront différemment face aux conséquences.

L’évaluation des risques ne garantira pas une sécurité à 100%, mais elle peut préparer un groupe à faire face à des menaces

De la même manière que la sécurité à 100% n’existe pas, les évaluations de risques ne sont pas la promesse d’une sécurité garantie. Par contre, elles permettent à un individu ou un groupe d’évaluer les menaces et les risques qui peuvent les affecter.

L’évaluation des risques consiste à analyser des risques déjà connus ou émergents afin de comprendre les risques impossibles à prévoir

Il existe différents types de risques :

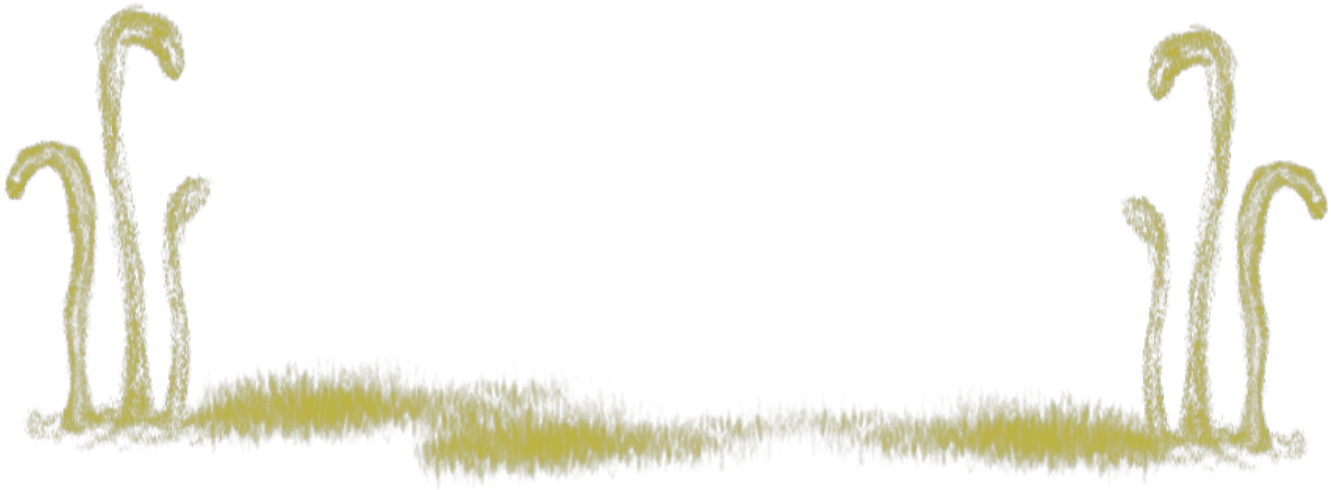
- Les risques connus : des menaces qui se sont déjà concrétisées dans la communauté. Quelles en sont les causes ? Quelles en sont les répercussions ?
- Les risques émergents : des menaces existent mais pas dans la communauté à laquelle la personne appartient. Il peut s’agir de menaces engendrées par le climat politique actuel, des nouveautés technologiques, et/ou des évolutions dans les communautés d’activistes au sens large.
- Les risques inconnus : ces menaces sont imprévisibles et il n’y a aucun moyen de savoir où et quand elles apparaîtront, ni si elles apparaîtront un jour.

Les évaluations de risques sont une partie importante de la planification

Celles-ci permettent à un individu ou un groupe d’examiner ce qui peut lui porter préjudice, les conséquences de ces préjudices, et leurs capacités à atténuer tant les préjudices que leurs conséquences. Le processus d’évaluation des risques permet aux groupes de prendre des décisions réalistes concernant les risques auxquels ils sont confrontés. Cela leur permet de se préparer aux menaces.

L’évaluation des risques est une manière de gérer l’angoisse et la peur

Il est bon de suivre ce processus pour faire ressortir les peurs de chacune des personnes dans un groupe et de trouver un équilibre entre la paranoïa et l’absence totale de peur ("pronoia"), afin d’anticiper les risques en prenant, collectivement, des décisions éclairées.



Évaluation des risques et mouvements sociaux [ressource essentielle]

Cette section approfondit les notions d'évaluation des risques liés à la mobilisation et aux mouvements sociaux.

Résumé

Évaluer les risques au niveau de la mobilisation et des mouvements sociaux signifie élargir le champ d’examen afin de prendre en compte également les espaces partagés, les processus, les ressources ou les activités menées collectivement, formellement comme informellement.

Les mouvements sociaux sont plus amples qu’une organisation, en cela qu’ils tissent des liens basés sur l’engagement politique et les actions partagées entre différent·e·s actrices et acteurs. Les actrices et les acteurs d’un mouvement, qu’il s’agisse d’individus, d’organisations, de collectifs, de groupes ou d’associations, apportent une diversité de connaissances, de compétences, de contextes et de priorités au mouvement. La manière dont les actrices et les acteurs d’un mouvement s’organisent, déterminent les rôles et domaines de responsabilités, et se mettent d’accord entre eux, sont des dimensions importantes de la structuration d’un mouvement, et l’évaluation des risques peut permettre de mettre à jour d’éventuels points de tension.

L’évaluation des risques appliquée à un mouvement social

Il est souvent plus simple d’identifier les mouvements rétrospectivement, en raison de leur croissance organique au cours du temps et qui dépend des préoccupations liées à des contextes ou moments spécifiques. On identifie parfois les mouvements à des manifestations, lieu de visibilité et de croissance de nombre d’entre eux. Mais tous les mouvements ne terminent pas (ou ne commencent pas) par des manifestations. Ainsi, beaucoup de mouvements LGBTIQ++ présents dans des lieux où être visible se paie au prix fort s’organisent et agissent moins visiblement, en créant notamment des espaces communautaires en ligne fermés, qui permettent de se rencontrer, de converser, d’offrir un soutien et d’établir des stratégies pour différents types d’interventions.

Un mouvement comporte de nombreuses étapes ou phases importantes telle que la diffusion dans la communauté, la collecte de preuves, l’approfondissement de la compréhension, la recherche de consensus, les actions, la tenue d’espaces collectifs de soin, la distribution de ressources, etc.

À chacune de ces étapes ou phases, les personnes responsables de l’espace ou du processus peuvent réaliser une évaluation collective des risques. Il pourrait être utile de penser la sécurité du mouvement comme le fait de réunir les conditions d’accomplissement et de prospérité des nombreuses étapes ou composantes du travail du mouvement.

Niveaux de risque

Une manière de commencer le processus d’évaluation des risques appliquée à des mouvements consiste à séparer les différents points à examiner. Il convient pour cela d’analyser trois volets différents, liés entre eux.

1. Les relations et les protocoles
2. Les espaces et l’infrastructure
3. Les données et l’information

Les sections suivantes décrivent ces différents volets et certains éléments qui les composent, notamment les questions à examiner pour mieux dégager, analyser et comprendre les risques dans le but d’établir un plan.



1. Relations/protocoles

Des relations solides fondées sur la confiance sont au cœur de la force d'un mouvement. Ceci est d'autant plus important que les mouvements reposent moins sur la forme que sur la force et la ténacité de leurs relations à différents niveaux.

L'évaluation des risques peut être réalisée au niveau individuel, organisationnel ou de groupes informels. Appliquée au renforcement d'un mouvement, elle consiste à s'intéresser aux relations *entre* ces différents niveaux.

Par exemple, si une personne est sujette à du stress parce qu'elle travaille d'arrache-pied pour son salaire, sa capacité à participer pleinement peut être affectée et avoir une incidence sur l'organisation du travail dans son ensemble. Si par ailleurs une organisation subit les attaques d'un gouvernement, d'autres organisations ou individus auxquels elle est affiliée dans le mouvement pourraient devenir sujets à des attaques similaires. Ou encore, si des cas de harcèlement se manifestent parmi les membres d'un collectif, le mouvement dans son ensemble pourrait s'en trouver affaibli en raison de tensions tant internes qu'externes.

Autrement dit, les risques en termes de mouvement doivent être examinés collectivement, et ils varient selon les pratiques et le bien-être des différents nœuds/actrices/acteurs de la structure du mouvement.

La gestion des risques au niveau des relations peut examiner les trois domaines suivants :

a) Prendre soin collectivement des individus

Le soin collectif est autant du ressort individuel que collectif. Il s'agit donc de tenir compte dans l'évaluation et la planification des risques des différents états de bien-être individuels, ainsi qu'entre les individus dès lors que des espaces, plateformes, ressources et processus sont partagés.

- Quels facteurs peuvent actuellement menacer le bien-être des actrices et acteurs du groupe ?
- Quelles pourraient être les répercussions ?
- En quoi la technologie peut-elle contribuer à cette question de bien-être ? Par exemple, existe-t-il des protocoles pour se déconnecter des médias sociaux, délimiter les réunions virtuelles, ou démontrer sa solidarité lorsqu'une ou un membre subit une attaque ?
- Comment mettre en place des pratiques collectives pour atténuer ou répondre à certains risques ou à leurs répercussions ? Peut-on regrouper ou partager des ressources ou des compétences en ce sens ? Par exemple, est-il possible pour différentes organisations ou individus de réunir des fonds pour souscrire à un canal de communication plus sûr ou une plateforme d'hébergement offrant un meilleur contrôle sur les données ?

b) Inclusion et représentativité

Ce point porte sur les processus et les critères visant à inclure des personnes à différents niveaux de l'organisation. Parfois, ceci n'est pris en compte que lors d'une brèche de sécurité, par exemple la fuite d'informations concernant un événement vers des individus ou groupes hostiles parce que tout circule sur un seul groupe WhatsApp ou Facebook. Réfléchir à des mécanismes d'inclusion peut contribuer à un développement plus ciblé de niveaux de sécurité de partage de l'information et de canaux de communication. Réfléchir à une diversité représentative dans les activités du mouvement peut également contribuer à révéler des risques particuliers pour des individus ou des groupes de personnes, et à trouver des solutions pour atténuer, distribuer ou se préparer face à ce risque.

- Quels sont les protocoles liés à l'arrivée de nouvelles personnes ou au départ des personnes ? Par exemple, les listes de diffusion ou autres espaces de discussion et de travail.
- Y a-t-il des risques spécifiques liés à la visibilité d'une ou plusieurs personnes à des moments donnés ? Comment planifier cela ? Par exemple, lors de la publication d'un

appel à participation, a-t-on prévu quels comptes en seraient à l'origine et pour combien de temps (il peut s'agir de comptes personnels, de comptes à utilisation unique ouverts spécifiquement pour une activité donnée, de comptes liés à l'organisation, etc.) afin d'empêcher toute possibilité de remonter à une unique source initiale ?
- Quels sont les risques liés aux actions en solidarité avec des allié·e·s lors d'un événement en particulier, et comment les prévoir ? Par exemple, souligner l'importance du consentement lorsqu'on documente et publie des photos sur un média social, particulièrement pour les identités ciblées, ou répartir le risque en amenant beaucoup de monde.
- Quelle est la situation des personnes appartenant au mouvement en termes de connectivité internet et de capacité technique, et comment cela affecte-t-il leur capacité à participer au mouvement en toute sécurité ?

c) Gérer les conflits

Ce domaine est souvent le moins analysé au sein des mouvements, puisqu'on présuppose des points de vue, des valeurs et des intérêts partagés. Il est cependant important qu'ils fassent surface, soient sujets à discussion et soient prévus, car ils peuvent servir la mission de justice du mouvement et aplanir les vulnérabilités internes ou les différences de pouvoir.

Une planification n'a pas à être complexe mais peut commencer par une discussion franche et tenue avec attention, qui fait ressortir les valeurs partagées et mène à des accords, puis qui construit là-dessus en désignant les personnes qui devraient être impliquées, les mesures à prendre, et les valeurs partagées que le collectif peut agir.

- Quels conflits potentiels pourraient représenter une menace pour le mouvement ? Quelles conséquences pourraient avoir des conflits entre membres ? Par exemple, une perte de confiance, des membres choisissant un camp, la perte du contrôle de ressources du mouvement comme les mots de passe, l'accès à des sites, etc.
- Comment élaborer un plan d'intervention selon différents types de conflit ? Par exemple, en cas de harcèlement sexuel au sein du mouvement, en cas de violence intime entre partenaires membres du mouvement, des relations amoureuses ou sexuelles entre membres du mouvement qui se terminent mal, la prise de décision concernant des ressources partagées ou un financement commun, des désaccords sur des valeurs essentielles ou des stratégies à suivre, etc. Certains conflits peuvent surgir autour de

mécanismes durables sur le long terme, tandis que d’autres sont plutôt liés à des activités ponctuelles.



2. Espaces/infrastructure

L’aspect numérique est aujourd’hui un facteur de plus en plus important dans la structuration et le renforcement d’un mouvement. Les mouvements n’étant pas fixés dans un espace institutionnel, l’infrastructure et les plateformes numériques deviennent des espaces partagés essentiels pour se rassembler, coordonner et planifier les activités, documenter les décisions et assurer la transparence, ou encore constituer des archives vivantes de l’histoire collective. C’est une partie indispensable de l’écosystème des mouvements actuels.

L’infrastructure numérique des mouvements consiste souvent en une combinaison de différentes plateformes, d’outils et de comptes utilisés ou apparaissant au gré de l’évolution du mouvement. Contrairement à une organisation, il peut y avoir plusieurs personnes chargées de différents types d’espaces servant des objectifs différents, qui peuvent en outre être utilisés par différentes communautés. Il peut s’agir de comptes personnels, de comptes temporaires ouverts pour une activité ou un événement spécifique, ou encore d’abonnements ou d’espaces créés uniquement pour rassembler des informations, des contenus et des flux communautaires. Prendre un moment pour comprendre ceci comme un écosystème – des composants interconnectés d’une

infrastructure collective partagée – et évaluer les risques potentiels peut aider à développer la responsabilité collective, le soin et la gestion de ces espaces, et à élaborer des mesures de sécurité pour pallier d'éventuelles compromissions.

Lors des discussions autour de l'évaluation des risques dans les espaces et l'infrastructure, on pourra prendre en compte les facteurs suivants :

a) Décisions portant sur la plateforme/l'outil/l'hébergement

Tout mouvement et travail d'organisation repose largement sur le partage des informations et l'efficacité des communications. Examiner les risques liés au choix de plateforme ou d'outil à utiliser pour s'organiser et à leur lieu de stockage peut donc avoir de grandes implications sur la sécurité et la sûreté des personnes, des groupes et du travail du mouvement. Lors d'une évaluation des risques en matière de vulnérabilité face aux fuites et aux attaques, il peut être utile de s'informer sur l'existence de solutions spécifiques, développées ou hébergées par des activistes ou des féministes, qui seront à priori plus attentives aux questions liées à la confidentialité et la sécurité.

Il est également important de tenir compte de l'accessibilité, de la facilité d'utilisation et de la probabilité qu'un large nombre de membres du mouvement l'adoptent de manière effective. Il n'est pas toujours utile de choisir la solution la plus sûre techniquement, si celle-ci exige un investissement important en temps et en énergie pour apprendre à l'utiliser, ce qui n'est pas toujours possible ni même préférable.

- Quelles plateformes, outils et espaces sont actuellement utilisés, dans quel but, et qui y a accès ?
- Quels sont les risques potentiels liés aux plateformes/outils/hébergements pour les besoins qui nous intéressent ? Quelles sont les répercussions de ces risques ?
- Quelles connaissances, compétences et capacités faut-il avoir pour les adopter ? Comment ces connaissances, compétences et capacités peuvent-elles être partagées et développées le plus largement possible avec les personnes du mouvement pour éviter de créer une hiérarchie de pouvoir interne basée sur la technologie ?
- Cette plateforme ou cet outil est-il accessible à la majorité de personnes qui en ont besoin ? Les obstacles à l'utilisabilité vont-ils au final engendrer des pratiques moins sûres ? Comment approcher ce problème ?

- Est-il possible de répartir les risques en répartissant aussi l'utilisation de cette plateforme ou de cet outil selon des besoins spécifiques ?

b) Propriété et gestion des ressources

Posséder et gérer une infrastructure numérique partagée est source de responsabilité, mais aussi de pouvoir et d'un contrôle potentiel de l'accès. Plus un mouvement sait voir ceci comme une conversation politique autour de valeurs partagées et de la compréhension de la gouvernance, de l'économie et du renforcement communautaire, plus les pratiques autour des technologies partagées seront durables.

- Comment l'utilisation d'infrastructures, de plateformes ou d'outils spécifiques sera-t-elle gérée et financée ? Qu'en est-il actuellement ? Comment fonctionne l'économie interne du mouvement pour répartir les coûts lors de l'utilisation et de l'investissement dans une ou plusieurs technologie(s) particulière(s) ?
- Quels risques court-on à utiliser des plateformes « gratuites » en termes de contrôle des données et des fonctionnalités, et quels sont les risques d'utiliser des services payants : peut-on s'engager à dépenser sur une période de temps prolongée ? Comment planifier ces coûts ?
- Comment prendre en compte cette question dans la politique que suit le mouvement ? Par exemple, à travers l'élaboration de protocoles sur la propriété commune, la gestion et le financement partagés. Est-il possible de s'organiser sur la base d'une économie de coopération ad hoc, informelle et souple ? Comment prendre des dispositions durables et transparentes ?

c) Administration et protocoles

En matière de structuration de mouvement, voir l'infrastructure comme un espace partagé signifie que savoir clairement comment et par qui ces espaces sont gérés peut non seulement contribuer à prendre soin du collectif, mais aussi dévoiler les risques potentiels liés à l'accès, la maintenance et l'éventuelle perte d'informations ou de l'espace communautaire.

- Qui contrôle l'accès aux différents espaces ? Cela dépend-il plutôt de la personne possédant l'espace (comptes personnels) ou le paramétrage, ou plutôt des prérequis à l'accès en termes de connaissances, d'appareils ou de la connectivité ?

- Quels sont les risques liés à la compromission de certains espaces ? D’où peut venir cette compromission (pensez aux menaces internes comme externes), et quelles pourraient en être les conséquences ? Comment prévoir cela ?
- Comment les espaces sont-ils gérés ? Et quels sont les protocoles, par exemple, combien de personnes peuvent administrer, où ces protocoles sont-ils gérés (individuel, organisation, réseau), à quelle fréquence cela change-t-il, quelles sont les conditions pour les modifier, pour modifier les mots de passe, etc. ?
- Y a-t-il des protocoles concernant la suppression d’espaces ou de données ? Qu’en est-il du stockage ? Suit-on déjà des pratiques que l’on puisse examiner et traduire en protocoles ?
- Comment, où et quand aborde-t-on la question de l’évaluation des risques pour l’infrastructure numérique partagée ?
- Qui réagira en cas d’incident (dans les espaces ou l’infrastructure) menaçant la sécurité et la sûreté du mouvement ?
- Quels changements dans les espaces utilisés par le mouvement (p. ex. de nouvelles politiques de sécurité sur les plateformes, la suppression de fonctionnalités de sécurité, etc.) et dans le contexte du mouvement (p. ex. des modifications dans la situation du pays, un changement de gouvernement, de nouvelles lois qui menacent la capacité du mouvement à continuer son travail, etc.) amèneront le mouvement à réanalyser les espaces ou l’infrastructure qu’il utilise ? Qui suivra ces changements ?



3. Données/information

Quand on organise un mouvement, on produit sans cesse des données et des informations. Celles-ci peuvent prendre une forme formelle ou informelle, avec des données produites délibérément ou sous formes de traces. Une autre manière de comprendre l'augmentation du risque consiste à examiner les pratiques en termes de données pour une activité ou une stratégie du mouvement en particulier. Pensez soit à un groupe de travail spécifique responsable de mettre en œuvre des tâches ou stratégies spécifiques, soit du point de vue d'une activité. On peut également analyser les risques au niveau des organisations, puisqu'elles doivent gérer des données, de même que chacune de leurs sections.

Voici quelques points à prendre en considération en matière de sécurité et de sûreté pour chacune des phases du cycle de vie des données. L'activité Le cycle de vie des données, ou comment comprendre les risques met ce point en application.

a) Création/rassemblement/collecte de données

- Quel type de données sont collectées ?
- Qui crée/rassemble/collecte les données ?
- Cela peut-il menacer des personnes ? Qui sera menacé si ces données sont publiées ?
- Dans quelle mesure le processus de collecte de données est-il public, privé ou confidentiel ?
- Quels outils utilisez-vous pour veiller à la sécurité du processus de collecte de données ?

b) Stockage des données

- Où les données sont-elles stockées ?
- Qui a accès au lieu de stockage des données ?
- Quelles pratiques/processus/outils utilisez-vous pour veiller à la sécurité des appareils de stockage ?
- Stockage dématérialisé, stockage physique ou stockage sur équipement dédié ?

c) Traitement des données

- Qui traite les données ?
- L'analyse des données menace-t-elle des individus ou des groupes ?
- Quels sont les outils utilisés pour analyser les données ?
- Qui a accès au processus/système d'analyse des données ?

- Lors du traitement des données, des copies secondaires des données sont-elles stockées dans un autre lieu ?

d) Publier/partager des informations à partir des données traitées

- Où les informations/connaissances sont-elles publiées ?
- La publication des informations peut-elle menacer des personnes ?
- Quel public visent les informations publiées ?
- Avez-vous le contrôle de la façon dont les informations sont publiées ?

e) Archivage

- Où les données et les informations traitées sont-elles archivées ?
- Les données brutes sont-elles archivées, ou uniquement les informations traitées ?
- Qui a accès aux archives ?
- Quelles sont les conditions nécessaires pour avoir accès aux archives ?

f) Suppression

- Quand les données sont-elles éliminées ?
- Sous quelles conditions sont-elles supprimées ?
- Comment s’assurer que toutes les copies ont bien été supprimées ?

Conclusion

Ce document entend contribuer à vous fournir un aperçu conceptuel de la manière d’approcher l’évaluation des risques dans le contexte de la structuration d’un mouvement. Souvent, l’évaluation des risques se fait à niveau individuel ou organisationnel. La penser à l’échelle du mouvement signifie de demander aux participant·e·s de se situer en tant que parties prenantes significatives, bien que partiales, d’une communauté élargie d’organisatrices et d’organisateurs.

Ceci peut être utile pour rassembler autour d’un sujet commun des groupes de personnes organisées différemment, et les amener à réfléchir à un projet commun lorsqu’un contexte, un objectif ou une activité partagés est identifié. Cela peut également contribuer à faciliter les

processus de réflexion collective en matière de durabilité et d'organisation, en anticipant et en planifiant les risques liés aux dynamiques groupales et relationnelles, dans lesquelles les technologies de l'information et de communication jouent un rôle essentiel en tant qu'infrastructure du mouvement.

> Vous pouvez partager ce document avec les participant·e·s en tant que ressource additionnelle de référence, ou choisir quels thèmes spécifiques approfondir lors d'un exercice de groupe ou d'un débat.

Autres documents généraux pour mieux comprendre la question du renforcement des mouvements et de l'organisation collective, ainsi que les réalités numériques

- TIC pour le renforcement du mouvement féministe : la boîte à outils de l'activiste (en anglais) : https://genderit.org/resources/icts-feminist-movement-building-activist-toolkit
- Créer un internet féministe : renforcer un mouvement à l'ère numérique (en anglais) : https://genderit.org/editorial/making-feminist-internet-movement-building-digital-age
- Donner une place prépondérante au féminisme transformatif : une boîte à outils pour les organisations et les mouvements (en anglais) https://www.sexualrightsinitiative.org/resources/achieving-transformative-feminist-leadership-toolkit-organisations-and-movements

