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 ?*

wiggy-cactus-white-several.png
Image not found or type unknown

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.

wiggy-cactus-white-several.png
Image not found or type unknown

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 ?

wiggy-cactus-white-several.png
Image not found or type unknown

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.

wiggy-cactus-yellow-several.png
Image not found or type unknown

Revision #3
Created 26 April 2023 01:21:52 by Kira
Updated 28 June 2023 20:15:40 by Kira