

## Les



Premiers Gestes pour Affronter une Situation de Cyber Harcèlement









Les **Premiers** Gestes pour Affronter une Situation de Cyber Harcèlement

Guide

INTRODUCTION	6
Informées et soudées,	7
nous serons mieux armées	7
Boîte 1 : Comprendre et reconnaître le	
cyberharcelement	11
De quoi parle-t-on ?	11
Le harcèlement, c'est quoi ?	11
Différences entre cyberharcèlement et harcèlement	
physique	12
Les espaces numériques du cyberharcèlement	13
Les supports et médias, vecteurs du cyberharcèlement	13
Les formes que peuvent prendre les cyber violences/	
harcèlements: de la cyberintimidation au revenge porn	14
Les types de violences et discriminations véhiculées	
par le cyberharcèlement	17
5	21
Les premiers gestes:	22
Ne restez pas seul·e!	2
~ '	24
	25
Les preuves et traces numériques	30
Boîte 3: Porter plainte	33
·	33
	34
Après la plainte	36
Boîte 4 : Trouver de l'aide	39
	39
	40
	40
	41
	42
Trouver de l'arde à l'écore	12
Boîte 5: Prévention	45
Cybersécurité et digital care	45
Les 5 règles principales de Digital Self Care	46
Prévention à destination des mineur·es	48
Boîte 6 : Vous êtes mineur∙e ?	51
Vous êtes mineur∙e et vivez une	

situation d'urgence ?	51
Boîte 7: Comment être un∙e bon∙ne allié∙e	53
Boîte 8: Dispositifs juridiques  Le harcèlement en ligne est-il	55
passible de sanctions ?	56
Qu'en est-il des agissements sexistes ? Les freins au bon encadrement des	56
pratiques sur internet	59
Gestion du cyberharcèlement sur les plateformes	62
Boîte 9: Appel à témoignages	68
Boîte 10: Plaidoyers et synergies	71
Boîte 11 : Ressources	73

### INTRODUCTION

Commentaires à caractère sexiste, intimidation, humiliation, harcèlements, haine, violence, dans l'espace digital, public ou privé, ou sur des supports électroniques.

Vous sentez-vous inquiètes ou concernées ? Pensez-vous en être la cible ?

> Malheureusement, vous n'êtes pas seules! En 2015, à l'échelle mondiale, 76% des femmes avaient déjà été victimes de cyberviolences!. Le risque de harcèlement en ligne est 27 fois supérieur pour les femmes<sup>2</sup>.





## INFORMÉES ET SOUDÉES, NOUS SERONS MIEUX ARMÉES



Ce guide a pour objectif de rassembler les ressources, conseils et protocoles existants pour faire face au harcèlement et aux autres formes de violences en ligne. L'objectif étant de mieux comprendre ce phénomène et de fournir quelques pistes en «premier secours» pour réagir face au cyberharcèlement.

Toutes ces informations ont été récoltées auprès de personnes ayant traversé cette douloureuse expérience ainsi qu'auprès d'associations et d'organisations référentes en ce domaine.

Si ce guide entend s'adresser aux personnes susceptibles d'être victimes de violences fondées sur le genre<sup>3</sup>, et particulièrement aux femmes<sup>4</sup>, c'est qu'il en va de l'objectif premier de la collective Chayn, qui milite pour créer un meilleur accès à l'information via les technologies ouvertes.

Certaines personnes se trouvant simultanément à l'intersection de plusieurs oppressions se retrouvent plus exposées à une forme de violence en ligne. En effet, au sexisme ou violence à l'égard des personnes LGBTQIA+ se superposent des violences basées sur l'appartenance ethnique, philosophique ou religieuse, au handicap ou encore la situation économique.

Ce qui suit ne se donne pour autant pas pour vocation de se substituer au travail des organismes, services de médiation et autres services publics ou privés spécialisés dans l'accompagnement psychologique, social et juridique. Notre contribution entend simplement répondre à un besoin de prévention et d'information vous permettant de déceler les situations

de cyberviolence pour, par la suite, vous fournir des outils pour y faire face. Vous trouverez ici un certain nombre d'interlocuteur·rices et d'espaces de confiance vers qui vous tourner en toute sécurité.

Réagir face au cyberharcèlement et l'affronter demande de l'énergie et c'est pourquoi nous avons tenu à vous partager un maximum de ressources. Les structures en mesure de vous conseiller, de vous écouter et de vous soutenir dans vos démarches sont recensées dans ce quide. Cependant, nous sommes conscientes des mécanismes sociétaux qui permettent au cyberharcèlement de prendre forme et du fait que ces enjeux méritent une réflexion approfondie. Ce quide est un pansement, non une solution.

Mise en garde/Trigger Warning: Ces ressources peuvent être lourdes à lire si vous avez récemment dû vivre des cyberviolences. Nous vous conseillons de les lire boîte par boîte ou de les lire avec une personne de confiance. N'hésitez pas à faire une pause.



3 - La Convention d'Istanbul propose une conception inclusive des personnes susceptibles d'être victimes de violences « fondées sur le genre » : les femmes mais aussi toute personne discriminée pour des comportements liés au fait que le genre auquel elle s'identifie ne correspond pas au sexe qui lui a été attribué, ou toute personne violentée en raison de son orientation sexuelle.

4 - Par « femmes », il est entendu toute personne qui a fait, fait ou fera l'expérience sociale d'être femme ou d'être perçue comme femme au cours de sa vie. En effet, la cyberviolence est un phénomène largement répandu dans la forme de violence basée sur le genre et particulièrement de manière disproportionnée à l'égard des femmes .



## BOÎTE 1: COMPRENDRE ET RECONNAÎTRE LE CYBERHARCÈLEMENT

## DE QUOI PARLE-T-ON ?

Avec la digitalisation de nos sociétés, de nouvelles formes de violences sexistes et sexuelles apparaissent. Elles peuvent prendre différents visages, s'inscrire sur différents supports, et mener rapidement à du cyberharcèlement.

## LE HARCÈLEMENT, C'EST QUOI?

Le harcèlement ne trouve pas de définition claire dans le Code pénal. Néanmoins, le texte qui l'encadre stipule qu'il est composé de deux éléments: l'un matériel (les agissements doivent affecter la tranquillité d'une ou de plusieurs personnes) et l'autre, moral (l'intention de nuire). Il précise également les «Conditions à remplir pour qu'une situation soit acceptée juridiquement comme du harcèlement»:

- Le comportement doit être répétitif et abusif.
- Il doit y avoir atteinte à la tranquillité.
- Le harceleur doit être conscient du préjudice causé à sa victime.



## DIFFÉRENCES ENTRE CYBERHARCÈLEMENT ET HARCÈLEMENT PHYSIQUE

- La diffusion de cyberviolences (en «meute» par exemple) peut être massive et l'impact instantané et les contenus peuvent atteindre un public large difficilement identifiable. La rapidité de propagation du message rend la reprise de contrôle particulièrement complexe. Ceci ayant pour effet de générer un sentiment d'impuissance chez les victimes et de les plonger dans une détresse d'autant plus intense.
- De manière générale, le cyberharcèlement se combine à sa variante physique. Chaque espace de vie devient contrôlé et assujetti à la traque. Ainsi, dans bien des cas, les violences se poursuivent dans la vraie vie, ou l'inverse. Exemples: le domicile d'une personne est publié sur un forum, les violences scolaires, conjugales, au travail...
- La personne à l'origine du harcèlement peut agir sous le couvert de l'anonymat grâce à l'utilisation de pseudonymes, par exemple. Cela renforce le sentiment d'insécurité que peut ressentir la victime et peut parfois provoquer crises d'angoisses et épisodes paranoïaques. Sans compter que le ou les auteur(s) jouissent d'une impunité telle qu'il devient difficile, voire impossible, de leur appliquer toute sanction légale.
- Bien que les cyberviolences ne sont pas un phénomène nouveau, la nature de celles-ci et les évolutions numériques amplifient la problématique. Malgré un intérêt récent du politique pour la question, la législation n'est pas encore mature en ce qui concerne la régulation du web et de l'ensemble des outils numériques. De même, le web n'est pas organisé selon une structure stricte, ni par un fonctionnement, susceptible de faciliter l'intervention d'une autorité,

qu'elle soit juridique ou institutionnelle.

Avant d'envisager les différentes étapes que vous pourrez entreprendre pour réagir face à une telle situation, voici une liste des principaux espaces numériques où ces situations apparaissent, les différents supports numériques utilisés, les différentes formes que peuvent prendre les cyber violences/harcèlements ainsi que les types de violences discriminatoires véhiculées par celles-ci.

## LES ESPACES NUMÉRIQUES DU CYBERHARCÈLEMENT

- Emails
- Forums et salles de chat
- Conversations privées et en groupe: sur des applications comme Whatsapp, Facebook, Messenger, Signal, Telegram, Viber, Twitter, Instagram, Youtube, etc.
- Réseaux sociaux: Publications, tags, commentaires et messages.
- Plateformes de jeux: en streaming ou en réseau, chat privés ou publics.
- Commentaires: sur les sites web des différents médias, sur YouTube, etc.
- Plateformes collaboratives en milieu professionnel: visioconférence, canaux de discussions de groupe, commentaire de documents, etc.
- Sites de rencontre

## LES SUPPORTS ET MÉDIAS, VECTEURS DU CYBERHARCÈLEMENT

- Supports écrits: messages, commentaires.
- Supports d'images: photomontages, infographies, caricatures, dessins, photographies, gifs, etc.
- Supports vidéo: Reels, Stories, live chat et autres contenus vidéo.



- Supports audios: messages et commentaires vocaux, podcast, appels en ligne, etc.
- Création de profils virtuels ou de pages, piratages de compte, vol d'identité, etc.

## LES FORMES QUE PEUVENT PRENDRE LES CYBER VIOLENCES/HARCÈLEMENTS: DE LA CYBERINTIMIDATION AU REVENGE PORN

### - Cyberstalking:

Création d'un sentiment d'oppression chez une personne cible en la mettant dans une position de proie traquée. Technique qui vise à se saisir de l'ensemble de l'identité virtuelle d'une personne afin d'augmenter son sentiment d'insécurité et ainsi affecter sa vie personnelle.

### - Affichage:

Création d'un sujet de discussion, d'une salle de chat, d'un groupe ou d'une page sur un réseau social à l'encontre d'une personne dans le but d'attirer l'attention sur elle et de la dénigrer auprès d'autres utilisateurs.

#### - Insultes et discours haineux:

Formulation ou reprise de discours haineux, de menaces, de provocations ou d'insultes dans le but de blesser ou d'attenter à la réputation de quelqu'un, ou d'un groupe. De là est né le terme de trolling en anglais.

### - Diffamation et propagation de rumeurs:

Diffusion large et récurrente de faits, avérés ou non, impliquant une personne afin de promouvoir une image négative de celle-ci par dénigrement.

### - Attaques coordonnées ou raids furtifs:



Lorsque plusieurs personnes/comptes coordonnés accablent collectivement une personne ciblée en se servant d'attaques personnelles, de menaces ou d'insultes. Cette technique est souvent utilisée lors de débats d'opinion sur internet. Ces raids peuvent également se dérouler par messages privés ou par visioconférence, via les messageries par exemple.

#### - Exclusion:

Technique de discrimination volontaire et ciblée visant à évincer une personne d'un groupe, d'une conversation ou encore d'un jeux.

## - Harcèlement sexuel par le biais de supports numériques:

Sollicitations à connotations sexuelles ou sexistes exercées de manière répétée sur une personne constituant une atteinte à la dignité d'une personne en raison de leur caractère dégradant. Phénomène incluant notamment le sexting et l'envoi de contenus sexuellement explicites non désirés.

- Revenge porn (Diffusion non consentie, sextorsion, chantage à la cam, compte fisha, ...):

Très proche du «harcèlement sexuel par le biais de supports numériques». Diffusions de photos ou de vidéos à caractère sexuel, mettant en scène la victime, sans son consentement et dans la volonté de lui nuire, le plus souvent dans un contexte de vengeance (jalousie, rupture, violence, etc.).

### - Cyberviolences conjugales:

Lorsque le harcèlement s'inscrit dans les relations dysfonctionnelles et/ou abusives au sein d'un couple donné. Ces abus peuvent revêtir plusieurs formes: contrôle des activités du conjoint «en ligne» (lecture des sms, pression téléphonique constante, viol de l'intimité, etc.), d'injures et de campagnes de dénigrement sur les réseaux. Cela peut même mener à des menaces de mort dans certains cas. Les technologies numériques permettent également une surveillance accrue du conjoint (avec un contrôle des déplacements via

des logiciels de traçage, par exemple). Il faut savoir que dans le cadre des violences conjugales, on observe depuis quelque temps un glissement vers l'espace numérique des violences sexuelles (comme c'est le cas du revenge porn mentionné plus haut) Une violence économique peut également découler de ce glissement (piratage des comptes bancaires, restriction des accès, etc.)

- Exposition et abus de la vie privée (Doxing):
Utilisation et divulgation publique d'informations
personnelles. Cette technique, communément appelée
doxing, est utilisée par les harceleurs afin d'affaiblir
la victime ou encore d'accentuer le processus
d'intimidation.

### - Usurpation d'identité:

Création d'un compte, page ou profil sur un réseau social dans le but d'usurper l'identité digitale d'une personne.

### - Phishing:

Fraude à l'identité reposant sur la confiance et le crédit accordé à un organisme public ou privé pour en imiter les usages. Cette arnaque sert très souvent des fins lucratives en permettant l'accès à des informations personnelles ou bancaires. Le harcèlement découle du caractère répétitif et récurrent de cette technique.

### - Astroturfing:

Technique de harcèlement visant à coordonner des actions (création de faux comptes, achats de followers actifs, etc.) pour gonfler les volumes de propagation d'un message afin de faire croire à un engouement authentique. Cette méthode de pression est très souvent utilisée à des fins politiques ou polémiques. La pression exercée sur la personne ciblée est ainsi considérablement accrue par le soin apporté au réalisme et à la crédibilité du message véhiculé.

## LES TYPES DE VIOLENCES ET DISCRIMINATIONS VÉHICULÉES PAR LE CYBERHARCÈLEMENT

Les violences spécifiques entraînant une violation des droits humains et une forme de discrimination à l'égard de certains publics sont majoritaires dans les types de violences en ligne menant aux harcèlement. Violences sexistes et sexuelles, mais également violences basées sur l'appartenance ethnique, philosophique ou religieuse, au handicap ou encore la situation économique, certaines personnes se trouvant à l'intersection de ces oppressions. Dans certains cas, la nature de ces violences tombent sous le coup de la loi et peuvent intervenir dans la définition du harcèlement.

#### - Sexisme:

Lorsque le harcèlement consiste en des gestes, propos ou des attitudes sexistes. C'est-à-dire des remarques méprisantes et stéréotypées basées sur le genre.

- Chantage, message de haine, menaces et insultes, humiliation, envers des personnes LGBTQIA+: Lorsque le harcèlement consiste en des gestes, propos

ou attitudes portant sur l'orientation sexuelle d'une personne, son identité de genre et/ou son expression de genre. Les violences à l'égard des publics LGBTQIA+ découlent des violences de genres et s'inscrivent clairement dans le continuum des violences lié aux stéréotypes de genre.

### - Racisme:

Lorsque le harcèlement consiste en des gestes, propos ou attitudes portant sur l'origine ethnique d'une personne, sa religion ou son appartenance philosophique.



### - Slut shaming:

Lorsque la démarche a pour but de générer de la honte chez une femme\* en portant le discrédit sur sa sexualité, sa tenue vestimentaire, ou sur toute autre attitude ou posture jugée déshonorante.

### - Grossophobie:

Lorsque le harcèlement consiste en des gestes, propos ou attitudes portant sur le poids d'une personne, considéré comme supérieure aux standards esthétiques valorisés par le groupe.

### - Body Shaming:

Lorsque la démarche a pour but de générer de la honte chez une personne qui ne correspond pas, par l'un ou l'autre aspect, aux standards esthétiques valorisés par le groupe.

### - Validisme:

Le validisme ou capacitisme est une discrimination basée sur le handicap. C'est un système d'oppression qui considère que les personnes valides sont supérieures aux personnes handicapées. Le handicap est alors perçu comme quelque chose «d'anormal» et de honteux.







## BOÎTE 2: AGIR FACE AU CYBERHARCÈLEMENT

Comment réagir face au harcèlement en ligne ? Que faire si l'on doit faire face à une déferlante d'injures? Que faire face à une attaque furtive ?

Bienvenue dans la BOÎTE 2, agir face au cyberharcèlement. Nous l'avons vu, les formes de harcèlement ou de violence rencontrées dans l'espace digital peuvent être nombreuses (BOÎTE 1). De même, les impacts sur votre vie peuvent être multiples.

Il est donc peu réaliste de fournir une liste exhaustive adaptée à chaque situation. Mais, des premiers soins peuvent être prodigués. C'est l'objet de cette BOÎTE 2.

### Gardez à l'esprit:

Lors de vos démarches, surtout: «Ne restez pas seul·e» (+ de ressources d'aide en BOÎTE 4)

La frontière entre le digital et le monde physique (beaucoup de femmes\* ont pu le vivre), est ténue.

Il faut donc, dès que possible, envisager de porter plainte. Nous avons compilé toutes les informations, démarches et éléments nécessaires pour vous accompagner dans ce sens. (BOÎTE 3). Sachez qu'une information essentielle sera requise par les services de police et que vous devez impérativement prendre en compte:

Conservez les messages et tout autre élément qui pourraient constituer une preuve devant les autorités avant de signaler, supprimer les contenus ou de bloquer les comptes. N'hésitez pas à demander à une personne de confiance de le faire pour vous.



### LES PREMIERS GESTES:

### - Évitez de répondre:

Vous risqueriez d'ouvrir la voie à un acharnement de la part de votre agresseur, impliquant une surenchère dans ses attaques. Ne perdez pas de vue que tout ce que vous direz pourrait être instrumentalisé contre vous. Une réponse de votre part ira également renforcer la visibilité des contenus qui vous atteignent car les algorithmes mettent en avant les contenus en fonction du volume d'interaction, et non de leur nature, et c'est dans votre intérêt de l'éviter.

### - Demandez de l'aide:

Parlez-en à une personne de confiance, amis, proches, collègues, parents,... Si vous êtes seul·e, que vous peinez à trouver une écoute bienveillante parmi vos proches, ou pour une aide spécifique, il existe des organismes et des intervenants prêts à vous épauler. Vous trouverez toutes les ressources nécessaires BOÎTE 4.

### - Gardez les preuves:

Faites toujours des copies ou des captures d'écran des contenus que vous estimez illicites et abusifs. Pensez à sauvegarder tous ces éléments dans un lieu sécurisé (disque dur externe, sauvegarde cryptée en ligne...) Vous pourrez vous en servir si vous êtes amenée à constituer un dossier. Récolter des preuves peut demander énormément d'énergie. N'hésitez pas à demander à une personne de confiance de le faire pour vous.

### - Signalez aux plateformes:

Signalez l'infraction aux plateformes sur lesquelles se déroulent les abus. Pour que le signalement fonctionne et soit effectivement pris en compte, n'hésitez pas à demander à un maximum de témoins de signaler également les contenus avec yous.

### - Ensuite...

En fonction de la situation, ripostez de manière spécifique, prenez soin de vous, organisez les preuves (traces numériques) et portez plainte (BOÎTE 3).

## NE RESTEZ PAS SEUL.E! IL EST IMPORTANT DE SORTIR DE L'ISOLEMENT, D'ÊTRE ENTOURÉ.E ET CONSEILLÉ.E.

### **VOUS ÊTES ADULTE?**

Parlez-en à une personne de confiance, amis, proches, collègues, parents,... Il existe aussi des organismes et des intervenants prêts à vous épauler.

Nous avons recensé pour vous, en BOÎTE 4, les organismes et associations à votre disposition pour faire face au cyberharcèlement.

### VOUS ÊTES MINEURIE OU SOUHAITEZ AIDER UN MINEURIE ?

Parlez-en directement à un·e adulte de confiance. Choisissez une personne qui vous sécurise: un·e de vos professeurs, parents, assistant·e social, centre PMS de votre école ou de votre commune, planning familial, etc.

#### Contactez Child Focus:

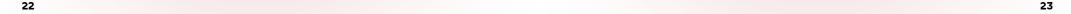
En Belgique, Child focus est joignable gratuitement au 116 000 pour les questions de sécurité en ligne destinées aux enfants, adolescents, parents et professionnels de l'éducation.

ChildFocus:

Email: 116000@childfocus.org 116 000 (24h/24) Clicksafe.be (sur la sécurité en ligne) facebook.com/ChilDfocus

### VOUS ÊTES TÉMOINS DE FAITS DE HARCÈLEMENT EN LIGNE ?

Vous pouvez porter secours à la victime en lui proposant votre soutien et votre écoute bienveillante et en vous référant aux conseils recensés en BOÎTE 7: Être un bon·ne allié·e.





### QUELQUES OUTILS

### - Récolter: les captures d'écrans:

Comme mentionné plus haut, faites toujours des captures d'écrans avant de bloquer ou de signaler les comptes et/ou les contenus indésirables car vous risquez de perdre définitivement de précieux éléments de preuve.

### En bref:

MAC: Maj (�) ,command (黑), et 4 PC: Maj (�), Touche Windows et S + Lien tuto

### - Signaler:

Pour signaler des messages, ou autres contenus indésirables, aux plateformes qui les hébergent, vous pouvez suivre les instructions disponibles via le lien suivant:

Ressource complète du «online harassment field manual».

Liens rapides de signalement:

Twitter / Facebook / Whatsapp / Tiktok / Instagram /
Twitch / Medium

### - Masquer et/ou supprimer des commentaires:

Sur Facebook, une fonctionnalité vous permet de masquer certains commentaires au bas de vos publications. L'auteur n'en sera pas alerté et sera, lui, toujours disposé à les voir. Ces contenus seront cependant bien conservés mais inaccessibles aux autres utilisateurs.

### - Démasquer:

Dans le cas d'attaques perpétrées par de très nombreux comptes, n'hésitez pas à questionner l'authenticité des comptes. En effet, lors de la création de faux comptes, il est fréquent qu'on laisse de nombreux indices qui peuvent permettre de remonter vers l'identité de la ou des personne, voire des organisations, dans certains cas, les ayant créés. Il existe de nombreuses techniques de repérage de faux comptes et d'identifications de leur(s) source(s).

Elles font partie de la discipline: <u>OSINT</u> (Open Source INTelligence). Certaines associations s'y spécialisent ainsi que les services de police en ligne.



### CAS PARTICULIERS

Et après avoir suivi les premiers gestes de base (aka: évitez de répondre, ne restez pas seul·e, gardez les preuves, signalez aux plateformes...)?

Nous l'avons vu, les formes de harcèlement ou de violences rencontrées dans l'espace digital peuvent être nombreuses, leur impact important et leur diffusion très large. Certains cas spécifiques nécessiteront des protocoles d'action bien précis, et parfois plus complexes. En effet, certaines victimes, en raison de leur situation, de leur statut ou de leur âge, devront faire l'objet d'un traitement plus particulier.

## PERSONNALITÉ PUBLIQUE : JOURNALISTE, FEMME POLITIQUE OU AUTRE FIGURE MÉDIATIQUE.

Les femmes participant au débat public, exprimant librement leur opinion, ou notoirement identifiées comme féministes forment un groupe à risque très important en matière de cyberharcèlement et de cyberviolence. 88 % des féministes sur Twitter et 66% sur Facebook ont été victimes de harcèlement en ligne.

Il s'agit ici d'un cas spécifique en raison de l'effet de la médiatisation sur la diffusion des contenus agressifs. Une rumeur, ou campagne de dénigrement, bénéficiera en effet d'un plus large écho en fonction de la notoriété de la personne visée.

Si vous subissez les répercussions négatives d'une couverture médiatique, relative ou importante, renforçant le sentiment de détresse ressenti face à du cyberharcèlement, voici quelques conseils susceptibles de vous aider:

- Évitez de répondre ponctuellement aux agressions afin d'éviter que vos propos soient isolés de leur contexte et instrumentalisés à vos dépens. Il est également important d'éviter une surexposition qui vous desservirait.
- Après les premiers gestes de bases (captures, signalements aux plateformes), vous pouvez mettre sur pied un dispositif de veille ou de monitoring (externe).

Demandez à une personne de confiance de prendre note des messages reçus ou qui circulent à votre sujet, de veiller à l'évolution des narratifs qui y sont accolés et d'en mesurer l'ampleur et l'impact mesuré (en utilisant votre propre compte ou non). Cela vous sera utile si vous décidez de porter plainte et/ou de riposter.

- Vous pouvez décider de récolter les traces numériques laissées par vos harceleurs et constituez un dossier de plainte. (BOÎTE 3: Porter plainte)

### Si vous bénéficiez d'une audience soutenante:

Essayer, à votre échelle, de fédérer une communauté de soutien disposée à porter votre parole et de témoigner en votre faveur.

Vous pouvez par exemple lancer une contre-offensive (ce qu'on appelle une «riposte») en demandant à des allié·e·s (des personnes que vous avez fédéré·e·s) de signaler des comptes problématiques, porter votre parole et de vous soutenir, en réponse.

### En cas de crise médiatique forte:

Vous pouvez publier un communiqué officiel, en utilisant de préférence le même canal que celui dont sont issues les attaques (par exemple, dans le cas d'une rumeur diffusée sur Instagram, utilisez cette même plateforme pour émettre votre message.)

Vous pouvez également envisager de contacter la presse, solliciter le concours de professionnels de l'information, si vous estimez que la situation vous échappe.

## CAS DE RAIDS COORDONNÉS VIA DES FAUX COMPTES (ASTROTURFING)



Technique de harcèlement visant à coordonner des actions (création de faux comptes, achats de followers actifs, etc.) pour gonfler les volumes de propagation d'un message afin de faire croire à un engouement authentique. Cette méthode de pression est très souvent utilisée à des fins politiques ou polémiques. La pression exercée sur la personne ciblée est ainsi considérablement accrue par le soin apporté au réalisme et à la crédibilité du message véhiculé.

### Pour identifier des contenus relevant d'astroturfing:

- sur Twitter, rendez-vous ici.
- sur Facebook, rendez-vous icl.

Souvent, il s'agit d'images glanées sur le web, comme des fausses photo de profil par exemple. Vous pouvez donc tenter une recherche d'image inversée sur Google. Ainsi vous verrez si cette même photographie a déjà été utilisée à d'autres fins.

Vous pouvez décider de récolter les traces numériques laissées par vos harceleurs et constituer un dossier de plainte. (BOÎTE 3: porter plainte)

### CAS DE DIFFUSION D'INFOS PRIVÉES (DOXING):

La diffusion publique d'informations personnelles ou sensibles, est une tactique utilisée par les harceleurs en ligne afin d'intimider et d'affaiblir leurs cibles.

### - En cas de situation de doxing:

Continuez à vous protéger au maximum via ces conseils:

Thttps://onlineharassmentfieldmanual.pen.org/fr/seproteger-du-doxing

**26** 5 - PAN 2021-2025 **27** 

### CAS DE REVENGE PORN:

Si vous êtes victime de la diffusion non consentie d'images et d'enregistrements à caractère sexuel.

### - Adulte:

En Belgique, l'IEFH, l'Institut pour l'égalité des femmes et des hommes peut vous aider en vous informant à propos de vos droits, de vos obligations et de vos possibilités d'actions, en vous apportant son soutien et parfois en entreprenant des démarches judiciaires avec vous.

L'Institut a élaboré un manuel qui explique, étape par étape, comment procéder pour signaler vous-même des images auprès des plateformes afin de les faire supprimer. Le manuel explique également comment déposer plainte à la police, ainsi que les conséquences d'une plainte.

Contacter l'IEFH:

0800/12 800

regalite.hommesfemmes@iefh.belgique.be
formulaire de contact
formulaire de signalement

#### - Mineur · e

Si la victime est mineure contactER Child Focus:
Le numéro d'urgence gratuit:
116 000 (24h/24)

7 116000@childfocus.org

### CAS DE PHISHING:

Fraude à l'identité reposant sur la confiance et le crédit accordé à un organisme public ou privé pour en imiter les usages. Cette arnaque sert très souvent des fins lucratives en permettant l'accès à des informations personnelles ou bancaires. Le harcèlement découle du caractère répétitif et récurrent de cette technique. Après les premiers gestes de bases (captures, signalements aux plateformes,...)

Signalez à Safeonweb = suspect@safeonweb.be.

### CAS DE CYBERVIOLENCES CONJUGALES:



Selon la Cour européenne des droits de l'Homme, des actes tels que surveiller, accéder à ou sauvegarder la correspondance du conjoint doivent être pris en compte par les autorités qui enquêtent sur des faits de violence domestique.

## On peut identifier 5 formes de cyberviolences conjugales:

- Le cybercontrôle (lecture des SMS, exigence que la partenaire soit joignable en permanence...).
- Le cyberharcèlement (appels incessants et envahissants, injures, menaces de mort).
- La cybersurveillance (contrôle continu des déplacements et agissements par exemple via un logiciel espion ou avec le GPS...).
- Les cyberviolences sexuelles (diffusion ou menace de diffusion d'images)
- Les cyberviolences économiques et administratives (comptes bancaires piratés)

## Il est possible de vous protéger au mieux dans l'espace numérique.

- Protégez-vous du doxing
- https://onlineharassmentfieldmanual.pen.org/fr/seproteger-du-doxing/
- Améliorez votre cybersécurité en renforçant, par exemple, vos mots de passe. Notre guide sur ce thème se trouve ici: \*\* <a href="https://chayn.gitbook.io/diy-online-safety/french">https://chayn.gitbook.io/diy-online-safety/french</a>
- Vous pouvez également suivre les conseils de notre guide Comment construire un dossier judiciaire de violences domestiques sans un avocat, et vous aider en prenant en compte ce qui constitue des preuves numériques.
- Suivez le chapitre suivant pour porter plainte qui vous aidera dans ces démarches.
- Ecoute violences conjugales: 0800/30.800

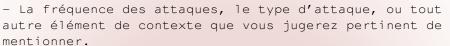
## LES PREUVES ET TRACES NUMÉRIQUES

Lorsque vous vous sentez prêt·e, compilez l'ensemble des éléments susceptibles de prouver qu'il y a bien fraude ou intention de nuire. Conservez également tout indice pouvant mener à l'identité du/des auteur·s. Cet ensemble d'informations constitue ce que l'on appelle «les traces numériques».

Dans un emplacement sécurisé, pensez à recenser et sauvegarder ce qui peut être considéré comme preuves numériques:

- Les dates et heures des messages ou échanges litiqueux,
- La plateforme le réseau social, l'application ou le site internet utilisé,
- Le type de document ou de support employé (Message privé, commentaire, contenu visuel, etc.),
- Les éventuels liens URL (vous pouvez utiliser Archive.is pour conserver une adresse URL)
- Le nombre de messages,
- La nature de l'incident en ligne (menace de nature sexuelle, attaque à caractère raciste, etc.)
- Le nom ou pseudonyme utilisé par l'auteur ainsi que ses potentielles autres identités digitales (accompagnées des différentes photos le représentant, ou désignées comme telles.) Si vous êtes en mesure d'y avoir accès, notez également son adresse email, son numéro de téléphone, son adresse IP ou encore des indices permettant sa localisation. Tout élément relatif à son identité peut s'avérer déterminant pour confronter la personne à l'origine du harcèlement,
- Les captures d'écran ou vidéos enregistrées, Votre matériel informatique, vos identifiants et votre nom d'utilisateur
- -Les autres agressions, verbales et/ou physiques, subies hors de l'espace numérique, liées aux faits relatés en ligne,
- Toute éventuelle preuve de préjudice: certificat médical, bilan psychologique, ordonnance psychiatrique,

ou tout autre témoignage de votre entourage, professionnel ou privé,







## BOÎTE 3: PORTER PLAINTE

En amont de ce qui va suivre, il est important que vous sachiez qu'un dépôt de plainte n'est jamais vain. Au-delà de la reconnaissance du préjudice subi, votre témoignage est essentiel à une meilleure compréhension du phénomène et à une meilleure prise en charge des victimes. Dans certains cas, la jurisprudence permet de faire évoluer le cadre législatif et peut considérablement améliorer la reconnaissance juridique de ces affaires.

Si vous décidez de porter plainte, voici ici rassemblées pour vous les différentes étapes que vous devrez aborder lors de la constitution d'un dossier:

### AVANT DE PORTER PLAINTE:

- Il est primordial de bien compiler toutes les preuves et traces numériques dont vous disposez pour attester des faits de harcèlement devant la loi.
- Sachez également que les preuves récoltées doivent s'inscrire dans le cadre légal pour être acceptées comme telles. Vous retrouverez les instances référentes à ce jour en BOÎTE 8.
- Listez bien les préjudices moraux, comme matériels, que vous estimez avoir subi. Cela pourra être utilisé à charge contre le ou les auteur(s). Exemple: si les préjudices ont un impact sur votre vie professionnelle, pensez à le mentionner.
- Mentionnez également tous les faits de harcèlement subis hors de l'espace numérique.
- Attention: Dans certains cas, un seul message outrancier ne suffira pas à caractériser des faits de harcèlement. Il vous sera demandé de prouver le caractère récurrent et insistant des sollicitations de la part de votre agresseur. Même s'il mène au

harcèlement. C'est à cet endroit que des lacunes dans la loi existent. En attendant, il pourrait tomber sur un autre coup de la loi, en fonction de la nature du harcèlement. Voir boîte 8.

Conservez toutes les preuves, en respectant bien les conseils émis en boîte 2, concernant la récolte des éléments de preuve.

### PORTER PLAINTE:

Toutes les démarches relatives à un dépôt de plainte sont recensées sur le Portail de la Fédération Wallonie-Bruxelles: 

http://www.victimes.cfwb.be/procedures-judiciaires/deposer-plainte/

### À QUEL MOMENT PORTER PLAINTE?

Le plus rapidement possible après les faits constatés, et après une récolte minutieuse de toutes les informations et éléments de preuve.

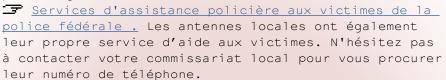
### OÙ PORTER PLAINTE ET QUI CONTACTER?

- N'hésitez pas à demander à une personne de confiance de vous accompagner. Vous n'êtes pas seul $\cdot$ e!
- Vous pouvez vous présenter dans n'importe quel commissariat de police.

Certains sont ouverts 24h/24h. Pour trouver votre commissariat le plus proche, rendez-vous sur le site de la police ( https://www.police.be/fr) et renseignez votre ville ou code postal.

- Le Service d'Assistance Policière aux Victimes (SAPV) de votre zone peut également être contacté. Ces services sont à votre écoute pour vous accompagner moralement, vous conseiller dans vos démarches administratives ou encore vous informer de vos droits. Ces services n'interviennent qu'à court terme et ne proposent pas de suivi psychologique. Ils peuvent néanmoins vous orienter vers des services de prise en

charge spécialisés pour vous assurer un suivi sur du plus long terme.



## - L'institut pour l'égalité des femmes et des hommes, IEFH.

Si vous pensez être victime de cyberharcèlement sexiste ou si vous constatez de tels comportements, indiquez-le à la police lors de la plainte. Vous pouvez aussi déposer un signalement auprès de l'Institut pour l'égalité des femmes et des hommes. Sur le site 

http://igvm-iefh.belgium.be.

Appeler le numéro gratuit 0800/12.800

### - L'institut interfédéral pour l'égalité des chances, UNIA.

Si vous pensez être victime de cyberharcèlement à caractère discriminatoire autre que fondé sur le genre ou si vous constatez de tels comportements, indiquez-le à la police lors de votre plainte. Vous pouvez aussi déposer un signalement auprès de UNIA.
Notez que: la discrimination fondée sur l'orientation

Notez que: la discrimination fondee sur l'orientation sexuelle est traitée par UNIA, la transphobie, par l'IEHFH. Sur le site:

Thttps://www.signalement.unia.be/fr/signale-le Appeler le numéro gratuit 0800/12.800

## COMMENT PROCÉDER CONCRÈTEMENT LORS D'UN DÉPÔT DE PLAINTE?

- Munissez-vous de vos documents d'identité et de tous les éléments préalablement compilés: certificats médicaux, preuves des faits, horodatage des faits, preuves ou éléments d'identité des personnes ou de la personne qui en est l'origine ou y contribuent.
- Sachez que la première personne que vous rencontrerez dans les locaux de la police se voit dans l'obligation de vous accueillir. Celle-ci sera, dans un premier temps, chargée de prendre note de votre identité ainsi que de la raison de votre venue. Vous serez très certainement amenée à patienter dans la salle d'attente

du commissariat jusqu'à ce que quelqu'un vous reçoive.

- Vous serez ensuite entendue par un·e inspecteur·trice. Cet entretien est strictement confidentiel. Cette personne établira un procès-verbal sur base des éléments que vous lui fournirez. Lors de cette audition, il est donc impératif que votre récit soit le plus précis et référencé possible.
- Vous avez le droit de demander une copie du procèsverbal établi lors de votre déposition. N'hésitez pas à demander à ce stade le numéro du Service d'Assistance Policière aux Victimes qui sera en mesure de vous soutenir, et de répondre à vos questions, à la suite de cette audition.
- Sachez que vous pouvez aussi demander à remplir une «déclaration de personne lésée» Cette démarche vous permettra notamment de bénéficier d'un meilleur suivi de votre dossier. En voici les avantages:
- http://www.victimes.cfwb.be/procedures-judiciaires/
  victime-vos-droits/#c7953
- À la suite de l'entretien, il vous sera remis un document, votre attestation de dépôt de plainte, que vous devrez conserver. Ce document pourra vous être demandé par la suite lors de vos démarches administratives et juridiques. Vous y trouverez également les coordonnées des services d'aide.

### APRÈS LA PLAINTE

Après la plainte, vous entrez dans la phase de «procédure judiciaire».

Le schéma établi par la Fédération Wallonie-Bruxelles vous permettra d'en comprendre chacune des étapes:

The http://www.victimes.cfwb.be/procedures-judiciaires/apres-la-plainte/

N'hésitez pas à vous faire conseiller par les services d'accueil des victimes proposés au sein des tribunaux. Ces personnes vous accompagnent et vous informent tout au long de la procédure, du dépôt de plainte jusqu'aux délibérations finales et même dans le cadre de la mise en application de la peine.

\*\*T http://www.victimes.cfwb.be/ou-trouver-aide/services-accueil-victimes/

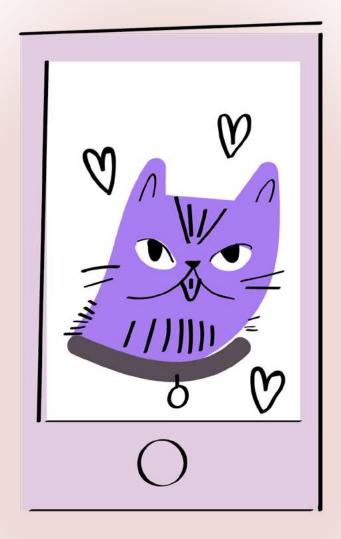
En tant que victime, vous bénéficiez d'un certain nombre de droits qui vous protègent tout au long de la procédure et également par la suite, dans le cadre de la mise en application de la peine.

http://www.victimes.cfwb.be/procedures-judiciaires/
victime-vos-droits/









## BOÎTE 4: TROUVER DE L'AIDE

Le cyberharcèlement n'est pas moins violent, ni moins impactant, qu'un harcèlement subi dans l'espace physique. Au contraire, les conséquences sont parfois d'autant plus pernicieuses: perte d'emploi, dépression, traumatisme, etc. Des cas de suicides sont d'ailleurs assez régulièrement relayés dans la presse. Les frontières entre l'espace digital et la vie réelle sont extrêmement poreuses, allant même jusqu'à se confondre dans l'esprit de certaines personnes.

Outre un accompagnement de la part des services de police ou des services d'aides aux victimes, il est primordial que vous puissiez bénéficier d'autres appuis. On ne vous conseillera jamais assez de faire appel à votre environnement familial, ou professionnel, pour faire face aux épreuves que vous traversez. Le cas échéant, il peut s'avérer nécessaire de solliciter l'aide de professionnels formés à l'écoute et au suivi thérapeutique de ce type de traumatisme.

Il existe différents services d'entraide et d'écoute vers lesquels vous pouvez vous diriger:

## **NUMÉROS IMPORTANTS**

- 112: Urgence médicale - 101: Urgence policière

# AIDE AUX VIOLENCES CONJUGALES

### - 0800/30.800: «ÉCOUTE VIOLENCE CONJUGALES»

Si le cyberharcèlement s'inscrit dans le cadre de violences conjugales, la ligne «Écoute Violences Conjugales» répond à des situations de détresse en proposant une écoute bienveillante, confidentielle et gratuite.

### - LE SITE ECOUTEVIOLENCESCONJUGALES.BE

Que vous soyez témoin, victime ou que vous ayez vousmême recours à la violence au sein de votre foyer, un chat a également été mis en place sur le site. Ce service dispose aussi d'un moteur de recherche permettant de trouver, près de chez vous:

- Des services juridiques spécialisés
- Des services d'aide à la jeunesse
- Des maisons d'accueil spécialisées
- Des services ambulatoires

Thttps://www.ecouteviolencesconjugales.be

# LES BUREAUX D'AIDE AUX VICTIMES

### SERVICES D'ASSISTANCE POLICIÈRE AUX VICTIMES DE LA POLICE FÉDÉRALE

Vous pouvez contacter le service d'assistance policière aux victimes de votre zone. Ces services sont à votre écoute pour vous accompagner moralement, vous conseiller dans vos démarches administratives ou encore vous informer de vos droits. Ces services n'interviennent qu'à court terme et ne proposent pas de suivi psychologique. Ils peuvent néanmoins vous orienter vers des <u>services de prise en charge</u> spécialisés pour vous assurer un suivi sur du plus long terme.



Vos antennes locales ont également leur propre service d'aide aux victimes. N'hésitez pas à contacter votre commissariat local pour vous procurer leur numéro de téléphone. Pour trouver votre commissariat le plus proche, rendez-vous sur le site de la police et renseignez votre ville ou code postal.

https://www.police.be/fr

# SOUTIEN PSYCHOLOGIQUE ET AUTRES LIGNES D'ÉCOUTE

### LES SERVICES DE SANTÉ MENTALE:

Il s'agit de services d'aide psycho-médico-sociale dans un cadre ambulatoire (prise en charge sans hospitalisation) à disposition de chaque personne qui en fait la demande. En Wallonie, il en existe 65, à Bruxelles<sup>5</sup>.

Wallonie: <u>F Les SSM de Wallonie</u>
Bruxelles: <u>F https://www.ccc-ggc.brussels/fr/</u>
institutions/services-de-sante-mentale

### LES CENTRES DE PLANNING FAMILIAL:

Vous pourrez trouver le centre le plus proche dans l'annuaire du site:

https://www.planningfamilial.net/liste-des-centres/

### CENTRE DE PRÉVENTION DU SUICIDE :

Ce service est joignable au 0800/32.123. Il est disponible 24h/24, il est gratuit et anonyme.

### SOS VIOL

Si le cyberharcèlement s'inscrit dans le cadre de violences sexuelles, vous pouvez contacter les équipes de « SOS Viol», ce service est également disponible 24h/24, gratuit et anonyme.

**3** 0800/98.100



## TROUVER DE L'AIDE À L'ÉCOLE



### LES CENTRES PSYCHO-MÉDICO-SOCIAUX (CPMS)

Tout au long de votre scolarité, et ce jusqu'à la dernière année des secondaires, ces centres vous permettent d'aborder toutes questions qui vous préoccupent. Y compris sur des aspects relatifs à la vie sociale et à la santé et non seulement pour vous accompagner dans votre orientation scolaire. Vous y serez accueilli par des personnes ressources: psychologues (conseillers et assistant·e·s psychopédagogiques), assistant·e·s sociaux·ales (auxiliaires sociaux) et infirmier·e·s (auxiliaires paramédicaux) qui travaillent en équipe. Les CPMS sont des lieux d'accueil, d'écoute et de dialogue. Ces centres accueillent aussi les familles.

### Comment contacter le Centre PMS ?

- Par téléphone, courrier ou par mail.
- En consultant la page:

http://enseignement.be/index.php?page=26028&navi=149

- Lorsque leurs services assistent aux réunions de parents d'élèves, à des rencontres informelles et lors de leurs éventuelles permanences au sein de votre école.
- En demandant l'information à votre direction ou à vos professeur  $\cdot$  e·s.

### LE SERVICE ÉCOUTE-ENFANTS

Le numéro 103 est le numéro d'écoute pour les enfants et adolescent·e·s. Il répond à l'ensemble des questions qu'elles ou ils peuvent se poser et abordent les difficultés qu'elles/ils peuvent affronter. Ce service est anonyme et il est accessible partout en Belgique.

## COMMENT CONTACTER LE SERVICE ÉCOUTE-ENFANTS ?

- Par téléphone, au numéro 103.
- Via le site = http://www.103ecoute.be.



## BOÎTE 5: PRÉVENTION

Vous trouverez ici quelques conseils de cybersécurité qui vous permettront, sinon d'empêcher tout risque de harcèlement en ligne, du moins d'en limiter l'occurrence sans qu'il ne vous soit pour autant nécessaire de quitter définitivement l'espace digital.

## CYBERSÉCURITÉ ET DIGITAL CARE

Le concept de digital care, développé par l'activiste britannique Seyi Akiwowo, également fondatrice de l'association Glitch<sup>6</sup> (association du Royaume-Unis qui lutte contre les abus ayant lieu en ligne), pourrait se traduire par «protection numérique». Cette locution désigne ainsi la mise en place de systèmes de protection en ligne afin d'éviter certaines violences, ou abus, par le biais d'internet.

6 - https://glitchcharity.co.uk/about/

## LES 5 RÈGLES PRINCIPALES DE DIGITAL SELF CARE:

### 1. UNE ÉVALUATION PERSONNELLE:

Demandez-vous dans un premier temps si vous assumez ce que vous partagez en ligne ainsi que la pertinence des informations personnelles que vous dévoilez. Certaines personnes partageront beaucoup, d'autres moins. C'est tout simplement un choix.

Nous vous conseillons de vous livrer à une petite expérience qui vous permettra d'évaluer votre «empreinte numérique», c'est-à-dire les informations vous concernant disponibles en libre accès sur internet. Si vous vous ne vous sentez pas à l'aise dans cette démarche, n'hésitez pas à demander à une personne de confiance de le faire pour vous.

Pour cela, il vous suffit de taper votre nom, adresse courriel ou numéro de téléphone dans votre moteur de recherche en n'oubliant pas de les encadrer de guillemets. Vous vous apercevrez peut-être que certaines données confidentielles ont filtré sans votre consentement.

### 2. UN RENOUVELLEMENT DE VOS MOTS DE PASSE

Il paraît assez évident que la faible sécurité d'un mot de passe, couplée à sa récurrence, accroît considérablement les risques de piratage. Il n'est pour autant pas nécessaire de modifier tous vos mots de passe en une fois, cela prend littéralement des heures. Commencez par ceux qui sont liés à vos informations les plus intimes et essentielles à garder secrètes: données bancaires, mails, messagerie, réseaux sociaux, etc.

À savoir: un bon mot de passe comporte au moins 8 caractères différents. Il est également conseillé d'y introduire chiffres, majuscules et caractères spéciaux. Nous vous recommandons d'utiliser un gestionnaire de mot de passe de type LastPass, qui vous permettra de générer des mots de passe en vous proposant une sauvegarde sécurisée par un coffre-fort digital.

### 3. L'AUTHENTIFICATION À DEUX FACTEURS



Il est possible de sécuriser l'accès à ses comptes importants en y apposant une double sécurité. Dans ce cas, il vous sera demandé 2 étapes d'authentification. La première, à l'aide de vos identifiants habituels, la seconde soit en vous envoyant un code par sms soit en vous envoyant un code par le biais d'un générateur de codes, via une application sur votre téléphone (

authentificator est l'application la plus sécurisée).

Étapes pour activer la double authentification pour Gmail:

Protéger votre compte avec la validation en deux étapes - Ordinateur - Aide Compte Google Étapes pour activer la double authentification pour Facebook:

What is two-factor authentication and how does it work on Facebook?

Étapes pour activer la double authentification pour Twitter:

<u>Tomment utiliser l'authentification à deux facteurs</u>
(2FA) sur Twitter

Étapes pour activer la double authentification pour Instagram:

<u>What's two-factor authentication and how does it</u> work on Instagram? | Instagram Help Center

Ce dispositif permet de rendre la tâche plus complexe aux éventuels hackeurs dans le cas d'un cyberharcèlement qui impliquerait une brèche de vos informations personnelles.

Il est également possible de recevoir une notification en cas de connexion suspecte sur un de vos comptes.

### 4. LA CRÉATION D'UNE MESSAGERIE « POUBELLE »

Comme vous pouvez sans doute le constater, de très nombreuses actions que vous effectuez en ligne requièrent votre adresse courriel. Que ce soit pour l'envoi de newsletter, de confirmations de commandes ou

encore dans le but de transmettre des tickets, places ou billets en tous genres, cette boîte se voit inlassablement sollicitée par les différents démarcheurs. C'est d'ailleurs très régulièrement le biais qu'utilisent certains faussaires pour accéder à vos informations confidentielles. Afin d'isoler ces contenus du reste de vos échanges, et donc d'éventuels éléments importants, il peut être pertinent de créer une messagerie entièrement dédiée à ces requêtes et activités plus secondaires.

### 5. VOS RÉSEAUX SOCIAUX, VOS RÈGLES!

Vos comptes sur les réseaux sociaux vous appartiennent. En cela, vous êtes seul·e maître·sse de ce qui s'y déroule et des éléments qui y figurent. Pour marquer clairement votre volonté de contrôle ou pour imposer toute autre règle de conduite que vous souhaitez y voir respectée, rien ne vous empêche de le signifier clairement sur les profils ou comptes concernés. Sur Facebook, par exemple, vous pouvez exprimer votre refus de toute agressivité ou de contenus déplacés, dans la section «à propos». Cela marquera ouvertement votre position et pourra peut-être dissuader certains comportements indésirables.

Un guide complet a été rédigé par Chayn HQ à ce sujet. Il est disponible via ce lien: Français - DIY Online Safety

## PRÉVENTION À DESTINATION DES MINEUR·ES

## Si vous êtes enseignant(e), le site web des autorités belges (Besafe<sup>7</sup>) vous conseille de :

- Créer une ambiance positive et de bien-être dans la classe, intéressez-vous à ce que vos élèves font sur l'ordinateur/leur téléphone portable, abordez la discussion de manière positive.
- Apprendre aux élèves à utiliser internet de manière sûre et responsable (cf. Dossier proposé par ChildFocus), par des jeux de rôles, des discussions

de groupe, des jeux d'opinion dans lesquels les élèves peuvent s'exprimer, etc.

- Élaborer des règles «anti-harcèlement» avec la participation des élèves en les exposant de manière visible dans la classe et/ou dans la classe informatique
- Parler des responsabilités de chacun et des conséquences du harcèlement pour favoriser une prise de conscience.
- Prévoir un point de contact par le biais duquel les élèves ainsi que les parents peuvent signaler un cas de harcèlement en toute confiance en mettant en place une boîte aux lettres anonyme, par exemple
- Informer les parents en cas de problème.
- Continuer à vous informer des pratiques et habitudes d'utilisation de l'outil internet par les élèves.

## Si vous êtes parent(s), le site web des autorités belges, (Besafe), vous conseille de:

- Vous intéresser aux activités en ligne de vos enfants, d'en parler de manière ouverte et positive tout en les sensibilisant aux risques qui y sont associés sans interdire leur accès aux nouveaux médias, même si vos enfants ont commis une erreur/négligence.
- Pour les enfants de moins de 12 ans, assurez-vous que l'ordinateur se trouve dans un lieu commun (pas dans la chambre à coucher par exemple), pour que vous puissiez de temps en temps jeter un coup d'œil à l'écran et que vous puissiez entendre si vos enfants s'effraient de certaines images, mails, etc.
- Continuer à vous informer pour rester à jour par rapport aux évolutions et à l'environnement des jeunes (tablettes, smartphones, applications, etc.)
- Si des problèmes se manifestent, signalez-les rapidement.







## BOÎTE 6: VOUS ÊTES MINEUR·E ?

Une étude de Forbes<sup>8</sup> nous apprend qu'aujourd'hui le phénomène touche principalement les jeunes, et plus particulièrement les jeunes filles. C'est pourquoi il était essentiel qu'un espace au sein de ce guide leur soit dédié.

## VOUS ÊTES MINEUR·E ET VIVEZ UNE SITUATION D'URGENCE ?

- Parlez-en à un.e adulte de confiance: votre prof, vos parents, votre assistant social, le Centre PMS de votre école ou de votre commune, votre planning familial,...
- Ne répondez pas aux messages, commentaires, cela le découragera et évitera un retour de flamme.
- Vous pouvez aussi contacter par téléphone le numéro «103», ou vous rendre sur les sites web:
- T Childfocus chat
- **→** 103ecoute.be

Child Focus en appelant le numéro d'urgence gratuit 116 000 (24h/24) ou en envoyant un e-mail à l'adresse suivante:

3 116000@childfocus.org.





Si vous êtes témoin de cyberharcèlement, que l'un e de vos proches, ou de vos élèves, en est victime et que vous souhaitez lui apporter votre soutien, voici quelques conseils.

### Ne lui dites pas:

- 1. «Tu exagères, c'est juste sur internet». Les cyberviolences sont des violences réelles, elles ont simplement lieu dans l'espace digital.
- 2. «Éteins ton téléphone, ça va se dissiper de soimême.» Ces violences peuvent avoir un impact décisif sur la santé mentale des victimes et sur leur parcours de vie.
- 3. «X a dit ça de toi, regarde». Il n'est pas nécessaire de relayer davantage les attaques et d'ainsi accentuer la portée des messages et contenus blessants.

### Il est préférable de :

- 1. Lui dire que vous la croyez et la soutenez.
- 2. Lui proposer de l'aider à rassembler des preuves afin de lui permettre de monter un dossier solide avant de porter plainte.
- 3. Proposez-lui de vous déléguer l'accès à ses comptes et ne lui faites seulement parvenir que les messages positifs et les manifestations de soutien.
- 4. Proposez également de témoigner en sa faveur auprès des instances judiciaires.
- 5. Une fois les preuves récoltées, n'hésitez pas à massivement signaler et reporter les contenus.





## BOÎTE 8: DISPOSITIFS JURIDIQUES

Nous avons vu plus haut les différentes formes que peuvent prendre le cyberharcèlement et comment il vous est conseillé de réagir. Malheureusement, dans certains cas, les démarches juridiques peinent à aboutir en raison du vide juridique entourant les pratiques en cours sur internet.

Pour rappel, il est important que vous sachiez qu'un dépôt de plainte n'est jamais vain. Au-delà de la reconnaissance du préjudice subi, votre témoignage est essentiel à une meilleure compréhension du phénomène et à une meilleure prise en charge des victimes. Dans certains cas, la jurisprudence permet de faire évoluer le cadre législatif et peut considérablement améliorer la reconnaissance juridique de ces affaires.

## LE HARCÈLEMENT EN LIGNE EST-IL PASSIBLE DE SANCTIONS ?

Au moment de la rédaction de ce guide, en 2021, il n'existe pas encore de texte spécifique encadrant le harcèlement dans l'espace numérique. Juridiquement, ce phénomène est considéré comme une forme de harcèlement moral définie par l'article 442bis du code pénal belge.

Ainsi, le texte précise les «Conditions à remplir pour qu'une situation soit acceptée juridiquement comme du harcèlement":

- Le comportement doit être répétitif et abusif.
- Il doit y avoir atteinte à la tranquillité.
- Le harceleur doit être conscient du préjudice causé à sa victime.

Or, dans le contexte de cyberviolences, il existe des situations dans lesquelles ces conditions ne peuvent être remplies, alors que le préjudice subi par la victime n'en n'est pas moins important.

C'est notamment le cas des attaques groupées, ou raids furtifs, que nous avons décrit plus haut. En effet, le phénomène de multiplication des agressions portées sur une seule et même victime viendra intensifier leur portée. Pourtant, chaque auteur, pris isolément et n'ayant émis qu'un seul message, ne saura remplir la condition de récurrence nécessaire à la qualification du harcèlement. Tous ces individus seront donc difficilement poursuivis.

## QU'EN EST-IL DES AGISSEMENTS SEXISTES?

Si les femmes sont davantage confrontées aux phénomènes de cyberharcèlement c'est que, très souvent, les faits impliquent des propos et intentions sexistes. Dans ce cadre, la Floi du 3 août 2014 destinée à lutter contre le sexisme dans l'espace public, peut également être saisie. Une qualification d'agissement sexiste pourra s'ajouter à celle de harcèlement et peser sur les délibérations et alourdir la peine.

## Pour être considéré comme sexiste, tout comportement doit correspondre aux 5 caractéristiques suivantes:

- Se définir par des agissements physiques comme verbaux (insultes, gestes obscènes, etc.) Ce qui comprend par conséquent les publications sur les réseaux sociaux, par exemple.
- Avoir lieu dans des circonstances publiques (dans un lieu public, en milieu professionnel en présence d'autres personnes, sur les réseaux sociaux, sur des forums, etc.)
- Êtres commis dans le but manifeste de nuire à la/aux victime(s). Cette volonté peut se traduire dans l'attitude de l'auteur mais aussi dans l'acte en lui-même.
- Viser une ou plusieurs cibles clairement définies en fonction de leur sexe et identifiables en tant que telles.
- Être commis dans l'intention d'humilier ou de mépriser la personne en raison de son sexe, avec pour conséquence une atteinte grave à la dignité. C'est le juge qui détermine si les faits sont de nature à constituer une atteinte grave à la dignité.
- Si vous pensez être victime de sexisme ou si vous constatez de tels comportements dans votre entourage, vous pouvez déposer plainte auprès de la police. Vous pouvez aussi faire un signalement auprès de l'Institut pour l'égalité des femmes et des hommes soit sur le site \*\* <a href="http://igvm-iefh.belgium.be">http://igvm-iefh.belgium.be</a>) ou en appelant gratuitement leur ligne de signalement au 0800/12.800.

### ET CONCERNANT D'AUTRES AGISSEMENTS HAINEUX... LA LOI ANTIRACISME ET DE LA LÉGISLATION **ANTIDISCRIMINATION**

Si les faits impliquent des propos et intentions incitant à la haine, à la violence et à la discrimination envers un individu ou un groupe dont un ou plusieurs critères sont dit «protégés" par la législation antidiscrimination (lois fédérales, décrets et ordonnances), ils sont interdits et punissables.

Si vous pensez être victime de cyberharcèlement à caractère discriminatoire autre que fondé sur le genre ou si vous constatez de tels comportements, indiquezle à la police lors de votre plainte. Vous pouvez aussi déposer un signalement auprès de UNIA -L'institut interfédéral pour l'égalité des chances Sur le site: Appeler le numéro gratuit 0800/12.800

Notez que: la discrimination fondée sur l'orientation sexuelle est traitée par UNIA, la transphobie, par l'IEHFH.



## LES FREINS AU BON ENCADREMENT DES PRATIQUES SUR INTERNET

### A) L'INTERPRÉTATION DES TEXTES DE LOI

Pour chaque affaire, la personne représentant la loi est censée appliquer des règles et recommandations définies par la législation sur une situation unique et singulière, avec tout ce que cela implique d'interprétation, de compréhension et donc parfois de subjectivité.

En ce qui concerne les infractions commises dans l'espace numérique, cette lecture peut s'avérer problématique pour plusieurs raisons, et notamment parce qu'agents de police, avocats et magistrats ne sont pas suffisamment sensibilisés à ces phénomènes. C'est ce qu'on appelle la problématique de «l'application des textes».

- Les juges, comme les avocats, sont peu sensibilisés à ces phénomènes et trop souvent les plaintes n'aboutissent pas ou bien sur des actions dérisoires pour les victimes. Le souci réside surtout dans l'interprétation que font les juges des lois.
- Certains agents de police qui réceptionnent la plainte ne sont pas non plus suffisamment sensibilisés. Des formations sont co-organisées avec l'Institut de l'égalité entre les femmes et les hommes.

### B) LA TEMPORALITÉ

La plupart des faits de harcèlement sur internet se développent et se propagent à une vitesse telle que cela peut parfois suffire à décourager la victime en impliquant un sentiment d'impuissance parfois paralysant.

Pour adopter les bons réflexes et réagir rapidement, rendez-vous BOÎTE 1.

D'autre part, il existe une sorte d'incompatibilité

de fond entre le temps du web, qui est celui de l'instantané, et celui de la démarche judiciaire, qui se traduit par un processus parfois long d'enquête et de délibérations.

La rapidité de propagation d'un message sur le web est élevée et dépourvue contrairement à l'espace physique d'intervention policière directe. Ces critères rendent difficiles les interventions directes. Ceci oblige la victime à mettre sur pied d'autres dispositifs de «premiers soins» lorsqu'elle est confrontée à une situation de harcèlement en ligne. Nous les abordons en BOÎTE 2.

En effet, le temps juridique est long, il ne permet pas l'action ou la réparation urgente, imminente.

### C) TERRITORIALITÉ

La notion de frontières administratives ne s'appliquant pas à l'espace digital, la question de la juridiction compétente peut se poser lorsqu'un litige met en cause des individus issus de plusieurs territoires.

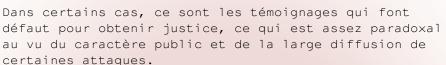
Pourtant, la territorialité est un des principes fondamentaux du droit belge. Ainsi, en Belgique, une infraction commise en dehors du royaume, par un belge ou un étranger, ne sera punie que dans des cas spécifiquement cités par la loi. Ce qui n'est pas encore le cas des violences commises sur internet.

Dans le cas où vous seriez concernée par ce cas de figure, signalez-le lors de votre dépôt de plainte et discutez-en avec votre avocate qui vous aidera à mettre en place une stratégie.

### D) LA CHARGE DE LA PREUVE

Sur internet, les éléments matériels et preuves de harcèlement sont extrêmement volatiles. Il n'est pas difficile d'effacer ou de modifier un message, de bloquer un utilisateur pour lui empêcher l'accès à vos contenus, etc. Bien souvent, l'absence de ces contenus à charge empêchent les poursuites d'aboutir. Vous trouverez nos conseils relatifs à la collecte de preuves en Boîte 2.

### E) LES TÉMOINS



Lors de votre dépôt de plainte, n'hésitez pas à fournir le nom, et pseudos si besoin, des personnes que vous pensez pouvoir témoigner.

### F) RÉGULATION DU WEB

Si en Belgique, ainsi qu'en Europe (notamment grâce au Digital Service Act<sup>9</sup>), nous assistons à certaines avancées en termes de contrôle sur l'espace numérique, l'autorégulation est encore très largement la norme dans ce domaine. Cette absence d'intervention étatique claire engendre des conséquences perverses en normalisant un certain nombre de comportements immoraux ou abusifs. Ce constat soulève un problème de taille ; cette politique du «tout est permis» n'impose-t-il pas un principe d'impunité contraire à l'ordre social défendu par un Etat de droit ?

Pour y répondre, les législateurs tentent depuis quelques années d'imposer un cadre général aux pratiques en ligne, se heurtent inévitablement à de nombreuses difficultés dans sa mise en œuvre concrète. L'entrave principale réside en l'architecture même du réseau internet qui n'a pas été conçu pour se soumettre à une autorité centralisée et ne présente donc pas de structure stricte, observable et maîtrisable.

Dans certaines démarches permettant d'établir la responsabilité de harcèlement, de modification des lois, ainsi que dans certains essais de régulation des acteurs du web, les services publics et gouvernements entrent en conflits de territoire avec les normes préexistantes sur le web. En effet, quand des normes nouvelles viennent essayer de réguler cet espace, elles ne sont pas toujours perçues comme légitimes par les 3 grandes fédérations et autorités du web: L'ICANN (Société pour l'attribution des noms de domaine et des numéros sur Internet. Elle gère l'adressage IP et coordonne les acteurs techniques), W3C (L'organisme de standardisation des techniques permettant de générer



des langages communs: HTML, PNG, etc.) et l'IETF (l'organisme qui établit des standards techniques d'internet). Des parties-prenantes très techniques, des informaticiens, confrontées à des interlocuteurs étatiques, politiques ou encore associatifs auxquels ils ne prêtent pas de légitimité. Ces autorités bloquent ainsi parfois certaines avancées de régulation.

## GESTION DU CYBERHARCÈLEMENT SUR LES PLATEFORMES

Chaque plateforme possède aujourd'hui ses propres dispositifs de protection et de contrôle de ses usagers. Sur Facebook, par exemple, il existe effectivement un guide, ainsi qu'un espace consacré au cyberharcèlement, mais ceux-ci sont malheureusement très dissimulés.

D'autre part, nous ne vous rappellerons jamais assez la nécessité d'effectuer des captures d'écrans et copies avant tout signalement. En effet, la grande majorité des protocoles de censure consiste en une suppression pure et simple des contenus indésirables. D'autre part, comme nous l'avons évoqué plus haut dans ce guide, le signalement doit être massif pour être pris en compte. Veillez donc à vous assurer du soutien d'autres utilisateurs dans cette démarche.

Néanmoins, les algorithmes restent aléatoires et relativement opaques (car protégés par le secret d'entreprise) et leur délai de réactivité parfois assez longs.

### LES LIGNES BOUGENT...

Si la loi n'a pas encore pris la mesure du phénomène de cyberharcèlement, les mentalités semblent évoluer en faveur d'une relative prise de conscience de la part de la société, en général. Nous notons certaines avancées significatives qui sont, notamment, le fruit de l'acharnement de victimes et autres associations concernées.

- Le premier juillet 2020, est entrée en vigueur en Belgique une nouvelle loi punissant «la diffusion non consensuelle d'images/d'enregistrements à caractères

sexuels», relevant de ce que nous avons désigné sous le terme de revenge porn.

- Le 30 mars 2020, après un an de travaux et d'auditions, le Parlement fédéral a voté une résolution sur la régulation des plateformes numériques et leur impact.
- Un groupe de travail pour l'égalité entre les femmes et les hommes réunissant des expert(e)s et des organisations de terrains a été lancé par Sarah Schiltz, la Secrétaire d'État belge à l'Égalité des genres, à l'Égalité des chances et à la Diversité. Cette initiative a aboutit à un plan d'action national de lutte contre la violence basée sur le genre. Ce plan prend en compte la question des cyberviolences, leur cadre juridique et opérationnel. 

  https://sarahschlitz.be/wp-content/uploads/sites/300/2021/11/20211125-PAN-2021-2025-clean-FR.pdf

- La majorité du Parlement bruxellois a voté une résolution requérant une étude sur les cyberviolences afin d'apporter de la lumière sur leur ampleur. Celle-ci prévoit également l'organisation d'une campagne d'information et de sensibilisation, notamment dans les écoles.

### ET EN ATTENDANT?

En attendant que l'Etat belge se dote d'un cadre légal plus adapté aux différentes formes de harcèlement en ligne et aux supports numériques, voici les quelques textes existants sur lesquels vous pouvez vous appuyer:

### - ARTICLE 442 BIS DU CODE PÉNAL

(que nous avons déjà mis en avant dans l'introduction de ce quide)

Ce texte précise que «quiconque aura harcelé une personne, alors qu'il devait savoir qu'il affecterait



gravement la tranquillité de la personne visée» peut se voir condamné à des peines de prison ferme allant de 15 jours à 2 ans et/ou à une amende s'élevant de 50 à 300 euros.

Pour rappel, les «conditions à remplir pour qu'une situation soit acceptée juridiquement comme du harcèlement» sont:

- Le comportement doit être répétitif et abusif
- Il doit y avoir une atteinte à la tranquillité
- Le harceleur devait savoir qu'avec ses agissements, il allait préjudicier la victime.

### - CHAPITRE V - TITRE 7 DU CODE PÉNAL

Loi contre la diffusion non consensuelle d'images/ d'enregistrements à caractère sexuel. Cette loi condamne, d'une peine de prison ferme allant de 6 mois à 5 ans, toute personne qui aura:

- Observé, filmé (...) une personne, sans autorisation ou à son insu, alors que celle-ci était dénudée ou se livrait à une activité sexuelle explicite (...).
- Montré, rendu accessible ou diffusé des images ou l'enregistrement (...) d'une personne dénudée ou se livrant à une activité sexuelle explicite, sans son accord ou à son insu, même si cette personne a consenti à sa réalisation.»
- Il faut noter que l'infraction sera reconnue à partir du moment où l'acte aura été initié. D'autre part, la peine se verra amplifiée si la diffusion des images ou des enregistrements a été commis dans l'intention de nuire ou dans un but lucratif.

### - ARTICLE 145 DE LA LOI DU 13 JUIN 2005

relative aux communications électroniques:
À l'alinéa 3 (bis) de cet article, peut se voir
punie d'une amende de 30 à 300 euros et/ou d'une
période d'emprisonnement allant de 15 jours à 2 ans,
«la personne qui utilise un réseau ou un service de
communications électroniques ou d'autres moyens de
communications électroniques afin d'importuner son
correspondant ou de provoquer des dommages ainsi que
la personne qui installe un appareil quelconque destiné
à commettre l'infraction susmentionnée, ainsi que la
tentative de commettre celle-ci.»

Nous observons que le terme harcèlement n'est pas mentionné dans cette disposition. La nécessité de récurrence des actes est donc incertaine.



## ARTICLES 443 ET 444 DU CODE PÉNAL RELATIFS À LA CALOMNIE ET À LA DIFFAMATION:

L'article 443 du code pénal indique que: «Celui qui, dans les cas ci-après indiqués, a méchamment imputé à une personne un fait précis qui est de nature à porter atteinte à l'honneur de cette personne ou à l'exposer au mépris public, et dont la preuve légale n'est pas rapportée, est coupable de calomnie lorsque la loi admet la preuve du fait imputé, et de diffamation lorsque la loi n'admet pas cette preuve.»

Pour faire suite à ce texte, l'une des dispositions de l'article 444 institue qu'il y a calomnie ou diffamation, lorsqueles imputations auront été faites:

- Soit dans des réunions ou lieux public ;
- Soit en présence de plusieurs individus, dans un lieu non public, mais ouvert à un certain nombre de personnes ayant le droit de s'y assembler ou de le fréquenter;
- Soit dans un lieu quelconque, en présence de la personne offensée et devant témoins ;
- Soit par des écrits imprimés ou non, des images ou des emblèmes affichés, distribués ou vendus, mis en vente ou exposés aux regards du public ;
- Soit enfin par des écrits non rendus publics, mais adressés ou communiqués à plusieurs personnes.»

### - ARTICLE 448 DU CODE PÉNAL RELATIF À L'INJURE

Cet article condamne «quiconque aura injurié une personne soit par des faits, soit par des écrits, images ou emblèmes, dans l'une des circonstances indiquées à l'article 444» à «un emprisonnement de huit jours à six mois et à une amende de vingt-six euros à cinq cents euros.»

### - ARTICLE 383 DU CODE PÉNAL

Cet article déclare que: «Quiconque aura exposé, vendu ou distribué des chansons, pamphlets ou autres écrits imprimés ou non, des figures ou des images contraires aux bonnes mœurs, sera condamné à un emprisonnement de huit jours à six mois et à une amende de vingt-six euros à cinq cents euros.»

## - L'ARTICLE 210BIS DU CODE PÉNAL : LE FAUX EN INFORMATIQUE.

Cet article déclare que:

(§ 1er) «Celui qui commet un faux, en introduisant dans un système informatique, en modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.»

(§ 2) «Celui qui fait usage des données ainsi obtenues, tout en sachant que celles-ci sont fausses, est puni comme s'il était l'auteur du faux.»

(§ 3) «La tentative de commettre l'infraction visée au § ler et est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cinquante mille euros ou d'une de ces peines seulement.»

### - ARTICLE 231 DU CODE PÉNAL : L'USURPATION D'IDENTITÉ

Cet article déclare que «quiconque aura publiquement pris un nom qui ne lui appartient pas sera puni d'un emprisonnement de huit jours à trois mois, et d'une amende de vingt-cinq à trois cents euros, ou d'une de ces peines seulement».

### - ARTICLES 550 BIS ET 550TER DU CODE PÉNAL

Ces articles condamnent notamment les atteintes à la confidentialité des données stockées et des systèmes informatiques les hébergeant. Cela concerne donc majoritairement les situations de piratage ou de hacking.

Ainsi l'article 550bis condamne «celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient.»



Pour sanctionner le hacking, deux éléments matériels sont requis, d'après l'article 550ter:

- Le système de traitement des données concernées doit être automatisé
  - Il doit y avoir une absence d'autorisation.

#### AUTRES DISPOSITIONS

D'autres dispositions peuvent encore être mobilisés dans certains cas de violences ou de propos haineux, que l'infraction ait lieu en ligne ou non. Un(e) avocat(e) pourra vous aider pour les identifier grâce aux éléments que vous lui fournirez.

C'est notamment le cas des manifestations racistes et xénophobes, homophobes ou sexistes.



CHAYN Belgium

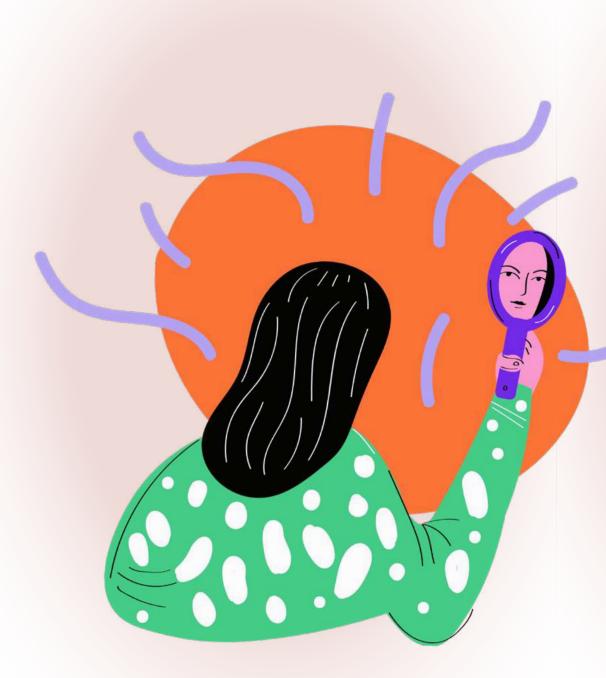
Vous avez rencontré une ou plusieurs situations de harcèlement ou de violence dans l'espace digital ? Vous souhaitez contribuer à notre wiki sur le sujet ? Pour mieux nous armer, n'hésitez pas à nous proposer:

- Des réflexes ou réactions efficaces qui n'ont pas été mentionnées
  - Toute information ou conseil absent de ce guide

Si vous avez envie de nous aider à porter la voix de celles qui ont vécu cette expérience douloureuse, n'hésitez pas à prendre contact avec nous pour témoigner de votre expérience. Nous nous engageons bien sûr à respecter votre anonymat.

**z** collective@chayn.be





## BOÎTE 10: PLAIDOYERS ET SYNERGIES

Vous avez des connaissances particulières touchant aux sujets abordés dans ce guide ? Vous êtes une association active dans ce domaine ? Vous êtes spécialisé e dans l'accueil des victimes de harcèlement? Vous souhaitez proposer des pistes de réflexion en lien avec notre propos ?

**⋾** collective@chayn.be





## BOÎTE 11: RESSOURCES

Si vous souhaitez des informations complémentaires sur les différents sujets abordés, nous avons compilé l'ensemble des sources que nous avons consultées pour rédiger ce guide. Si vous souhaitez contribuer à ce wiki ou encore agrémenter cette bibliographie, n'hésitez pas à nous contacter :

collective@chayn.be

GUIDE sur chayn.be

- Fiche thématique de l'UNICEF sur le cyberharcèlement:
- https://www.unicef.fr/sites/default/files/fichethematique-myunicef-lecyberharcelement.pdf
- Dix types de cyberharcèlement:
- https://blog.securly.com/2018/10/04/the-10-types-ofcyberbullying/
- La plateforme de conseil du gouvernement français, à destination des mineurs, de leurs parents, professeurs et écoles. Qu'est-ce que le cyberharcèlement ?
- faire/quest-ce-que-le-cyberharcelement/
- Se protéger contre le doxing:
- ## https://onlineharassmentfieldmanual.pen.org/fr/se-proteger-du-doxing/
- Reconnaître et masquer des faux comptes sur Facebook:
- <u>fhttps://fr.wikihow.com/d%C3%A9masquer-un-faux-compte-Facebook</u>
- S'informer et signaler des incidents lié à la cybersécurité en Belgique:
- Thttps://www.safeonweb.be/fr/liens

CHAYN Belgium

OUTILS OSINT (Open Source Investigation)
Pour les curieuses ou passionnée d'outils informatiques,
l'outil «OSINT» (Open source investigation) <a href="https://osintframework.com/">https://osintframework.com/</a> investigations sur base des données et informations accessibles librement mais parfois bien cachées, sur le web.

- Outils Instagram - filtrer les messages privés. Outil Instagram développé par deux victimes de cyberharcèlement:

<u>If https://siecledigital.fr/2021/04/22/instagramoutils-cyberharcelement-messsages-prives/</u>

- Filtrer les spams Twitter:
- <u>Inttps://www.ladn.eu/tech-a-suivre/block-party-twitter-troll/</u>
- Détecter le cyber buylling avec une app (Kindly):
- https://time.com/5916772/kid-of-the-year-2020/
- Des ressources à destination des enfants, ou de leurs parents, des enseignants et autres professionnels de l'enfance, confrontés à des situations de harcèlement et/ou de violences dans l'espace digital:
- php?page=27461&navi=4106
- En France, il existe un numéro vert : 3018, et un site internet
- <u> https://www.netecoute.fr/</u> destiné à aider les enfants et adolescents victimes de cyber violences.
- Application Cyberhelp, initiée par la fondation Child Focus:
- \*\* https://www.childfocus.be/fr/nouvelle/lancement-de-cyber-help-lapplication-qui-vole-au-secours-du-jeune-en-cas-de-cyber
- Comment identifier un faux profil sur facebook?

  Thttps://fr.wikihow.com/d%C3%A9masquer-un-faux-compte-Facebook

### WWW.CHAYN.BE

Ce guide a été créé grâce au soutien de Equal.Brussels dans le cadre de l'appel à projet de lutte contre les violences faites aux femmes\*

Chayn Belgium est le chapitre belge de Chayn HQ.

Chayn est une association mondiale, dirigée par des survivant·e·s et des allié·e·s du monde entier, qui crée des ressources pour soutenir les survivant·e·s de violence sexiste. L'association crée de ressources ouvertes et des services en ligne intersectionnels, multilingues et féministes pour soutenir les survivant·e·s d'abus.

www.chayn.co

Ce guide est publié sous la licence «Attribution-NonCommercial 4.0 International (CC BY-NC 4.0)" et peut être partagé ou adapté, pour autant qu'il soit dûment attribué et qu'il ne soit pas utilisé à des fins commerciales.

Si vous avez des suggestions sur la façon d'améliorer ce guide ou de le distribuer plus largement, veuillez nous envoyer un courriel à collective@chayn.be

### Remerciements

Equipe Chayn Belgium:

Manon Brulard, Clémentine Delisse, Manon El Assaïdi,

Saadia Sahraoui, Kevin Tassi.

Graphisme: Chayn UK, Julie P. et C.S

( Bye Bye Binary )



