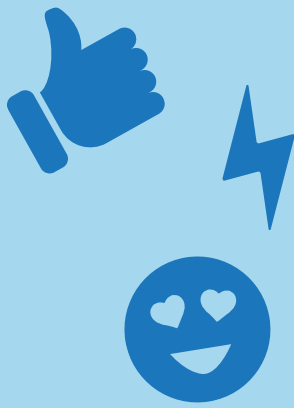


Guide pour accompagner à la protection des cyber- violences





Qu'est-ce qu'il y a dans ce guide ?

I. Contexte.....	3
Pourquoi ce guide ?.....	4
Comment utiliser ce guide ?.....	5
Qui sommes-nous ?.....	6
 II. De quoi parle-t-on ?.....	 7
Violences et cyber-violences.....	8
Harcèlement et cyber-harcèlement.....	10
Expressions de cyber-violences.....	12
Signes de mal-être.....	15
 III. Que peut-on faire ?.....	 18
Le recueil de la parole.....	19
Le sentiment de sécurité en ligne.....	22
Des bons réflexes avec Mémo de vie.....	27
 IV. Et maintenant ?.....	 30
Résumé et premiers pas pour les usagers.....	31
Ressources boussole.....	32
Services d'aide.....	33
 V. Approfondir.....	 34
Précisions juridiques.....	35
Nos données personnelles.....	38
Sources d'information.....	39



I. Contexte

Pourquoi ce guide ?.....	4
Qui sommes-nous ?.....	5
Comment utiliser ce guide ?.....	6



Pourquoi ce guide ?

Internet, les écrans, les réseaux sociaux font partie de notre quotidien. Ce sont des outils qui nous accompagnent à travers les différentes sphères de la vie (sociale, familiale, administrative, médicale, scolaire, académique, professionnelle...) et dont il est important de parler afin de pouvoir choisir comment les utiliser, avec conscience et en sécurité.

POURQUOI PARLER DE “CYBER-VIOLENCES” ?

Les cyber-violences sont les violences qui se déroulent dans les espaces numériques et/ou via des outils digitaux. Certaines sont transposées directement du monde physique dans le monde digital (ex : insulte par texto) tandis que d'autres émergent spécifiquement de ce que la technologie numérique permet notamment via les IA génératives (ex : deep fake, deep nudes).

Ces violences ont des spécificités propres à garder en tête pour pouvoir à la fois les prévenir et y réagir. L'interposition d'un écran, l'impression d'éloignement et l'absence de communication kinésique limitent le niveau d'empathie des auteurs, qui ne sont pas nécessairement confrontés aux effets de leurs actes sur la personne ciblée. Les capacités d'adaptation de la victime sont également réduites. N'étant parfois pas certaine de l'identité de son ou ses agresseurs, elle peut se trouver en situation de déséquilibre de pouvoir et ressentir un sentiment d'impuissance accru couplé à une impression de non-recours et d'impunité.

Les cyber-violences peuvent avoir de graves impacts sur le court et le long termes, des incidences aussi bien sur la santé physique et mentale des individus que sur l'équilibre sociétal, la vie en ligne étant aujourd'hui indissociable de la vie physique.



Tout le monde peut être touché par de la cyber-violence. Cependant, comme dans d'autres espaces, nous retrouvons des structures systémiques d'inégalité affectant différemment les individus selon leurs groupes sociaux : les victimes sont ici aussi principalement des femmes et minorités de genre***.

Les cyber-violences ne se limitent pas à la sphère publique mais s'étendent également à la sphère privée. Effectivement, dans des contextes d'intimité, de relation amoureuse ou de couple, la violence peut s'exercer par des moyens numériques ; ce sont autant d'opportunités de contrôle, de manipulation et autre abus, en effet, 9 femmes sur 10 victimes de violences conjugales ont subi des cyber-violences**.

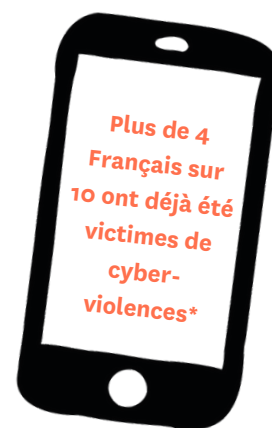
Il est alors spécialement important de comprendre les possibilités de fonctionnement de ces outils pour trouver des façons de vivre en ligne le plus en sécurité possible.

C'est pour accompagner, informer et transmettre de bonnes pratiques autour des situations de cyber-violences que Mémo de vie et Respect Zone s'associent dans la création de ce guide.

POUR QUI EST CE GUIDE ?

Pour vous, qui exercez des métiers en lien avec des personnes en situation de violence.

Pour MIEUX comprendre le sujet des cyber-violences et pouvoir accompagner à la reprise de pouvoir sur ces outils afin de MIEUX se protéger et (ré)agir.



*Enquête Féministes contre le cyberharcèlement, IPSOS 2022

**Étude “cyberviolences conjugales”, Centre Hubertine Auclert, 2018

***Rapport Haut Conseil à l'égalité entre les femmes et les hommes, 2018



Qui sommes-nous ?

France Victimes

La fédération France Victimes, fondée en 1986, regroupe 130 associations d'aide aux victimes agréées par le ministère de la Justice. Ces associations, composées de professionnels (juristes, psychologues, travailleurs sociaux), offrent accueil, écoute, aide psychologique, information juridique et accompagnement social aux victimes d'atteintes personnelles ou matérielles.

France Victimes administre le 116 006, la plateforme téléphonique nationale d'aide aux victimes.

Elle propose également des formations spécialisées pour son réseau et ses partenaires. Avec plus de 1 350 lieux d'accueil, les services sont gratuits et confidentiels, garantissant l'autonomie et la liberté des victimes.

La plateforme Mémo de vie offre un espace digital sécurisé pour les victimes de violences répétées, accessible via téléphones, tablettes et ordinateurs.

Respect Zone

Association 1901 créée en 2014, Respect Zone œuvre pour la protection des personnes dans l'espace numérique. Elle soutient l'exercice d'une liberté d'expression responsable et la participation engagée de tous à créer un environnement de respect en ligne. Elle mobilise et sensibilise les internautes aux cyber-violences, au cyber-harcèlement et à la haine en ligne.

Héritière des grands combats pour l'acceptation des différences, l'association entend asseoir la notion de dignité numérique tout en développant des outils de prévention positifs comme le label et la charte Respect Zone.

Elle utilise le droit et l'éducation pour agir positivement sur ces enjeux sociétaux en intervenant auprès de différents publics pour les sensibiliser et les former.

Grâce à sa Clinique Juridique, son Cercle des Juristes et ses réseaux partenaires, l'association participe à des chantiers législatifs et offre une aide juridique aux victimes. L'application Respect Zone, accessible gratuitement, est un de ses derniers outils développés pour accompagner les personnes en situation de cyber-violence, qu'elles soient cibles, témoins ou autrices.



Comment utiliser ce guide ?

Le but de ce guide est de comprendre les cyber-violences dans leur complexité afin que vous puissiez vous faire une idée de différentes situations dans lesquelles peuvent se trouver les personnes que vous accompagnez et ainsi ouvrir les possibilités pour les aider à se protéger, en prévenant ces abus et en y (ré)agissant.

Pour que le guide puisse parler à un large public de professionnels aux savoirs variés, nous avons inclus des explications de notions basiques sur lesquelles il nous semblait important de s'entendre. Ce sont des propositions de définitions dans le contexte de notre sujet et de notre guide ; elles sont là pour construire un cadre commun dans lequel échanger et non pas pour figer des vérités officielles.

Nous avons aussi fait le choix d'exclure, limiter ou simplifier certains points du guide pour ne pas le surcharger d'informations qui auraient pu le rendre indigeste. Il ne sera jamais exhaustif et notre souhait est qu'il serve de base pour permettre d'aller plus loin tout en proposant des actions concrètes à mettre en place dès sa lecture.

Voici déjà ce à quoi vous devriez pouvoir avoir accès avec ce guide :

- 1 - les points d'attention concernant l'usage des outils numériques pour une personne en situation de violence
- 2 - des idées d'actions à proposer aux personnes que vous accompagnez pour prévenir et (ré)agir à ces violences
- 3 - des services d'aide spécifiques vers lesquels les orienter pour davantage d'information ou une prise en charge
- 4 - d'autres ressources pour approfondir votre compréhension du sujet des violences en ligne

Nous avons créé ce guide en même temps qu'un guide à destination directe des usagers. Beaucoup de contenus se croisent. Notre envie pour ce guide "professionnel" était aussi de pouvoir vous aider à animer le guide "utilisateurs" auprès des personnes que vous accompagnez, introduire les enjeux du sujet et faciliter leur autonomisation autour de ces outils.

Soyez libre ! De prendre ce qui vous aide et de l'adapter selon ce qui a du sens dans l'exercice de votre activité, en fonction de la particularité des parcours de vie que vous rencontrez.



Nous n'avons pas besoin d'être des experts du numérique, ni d'être nous-mêmes des pratiquants, pour pouvoir comprendre le sujet et mettre en place (ou aider à mettre en place) de bons réflexes de sécurité. Comme toute chose, le plus important est de se poser des questions et chercher une réponse adaptée !



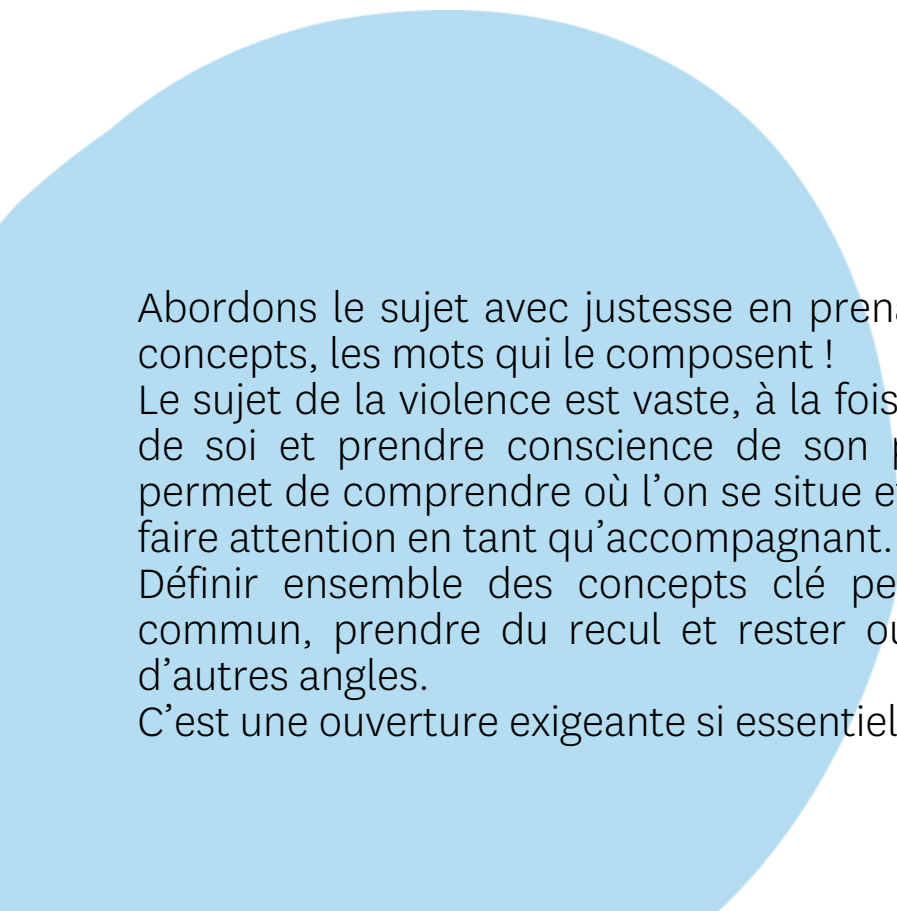
II. De quoi parle-t-on ?

Violences et cyber-violences.....	8
Harcèlement et cyber-harcèlement.....	10
Expressions de cyber-violences.....	12
Signes de mal-être.....	15





Violences, cyber-violences



Abordons le sujet avec justesse en prenant un temps pour définir les concepts, les mots qui le composent !

Le sujet de la violence est vaste, à la fois universel et personnel. Partir de soi et prendre conscience de son propre rapport à la violence permet de comprendre où l'on se situe et quels sont les biais auxquels faire attention en tant qu'accompagnant.

Définir ensemble des concepts clé peut aider à former un cadre commun, prendre du recul et rester ouvert à d'autres expériences, d'autres angles.

C'est une ouverture exigeante si essentielle au rôle d'accompagnant-e.

Violences et cyber-violences

VIOLENCES

Nous entendons par violence le fait de "faire mal" et cela peut prendre différentes formes :

- **verbale** (insulte, moquerie, dénigrement)
- **non verbale** (grimace, imitation, geste obscène)
- **psychologique** (propagation de rumeur, processus d'isolement, pression, contrainte, chantage)
- **et/ou physique** (coup, restriction, attouchement, viol, intimidation).



Les **micro-violences** sont des "petites" violences ordinaires, dans le sens où elles sont imperceptibles, invisibles, silencieuses, diffuses. Elles peuvent être petites, nombreuses, multiformes et sont souvent banalisées, normalisées. *

Ex : nier ou invisibiliser la contribution d'une personne à une tâche, remettre en question sa force ou capacité à faire quelque chose, ne pas la consulter pour un choix qui la concerne...

Dans un contexte d'intimité, de relation amoureuse ou de couple :

Il peut être spécialement difficile de se rendre compte des violences que l'on vit.

Le **contrôle coercitif** est une forme continue de violence relationnelle caractérisée par des micro-violences quotidiennes. Cela passe par l'utilisation de techniques de manipulation, domination et contrôle, incluant l'isolement social, la surveillance, les menaces, les humiliations et le contrôle des finances. L'agresseur peut avoir recours à la force et/ou la privation pour que la victime lui obéisse, la rendre dépendante et lui ôter son sentiment de liberté dans la relation.

Pour en savoir plus, rendez-vous page 14

CYBER-VIOLENCES

Ce sont **l'ensemble** des violences

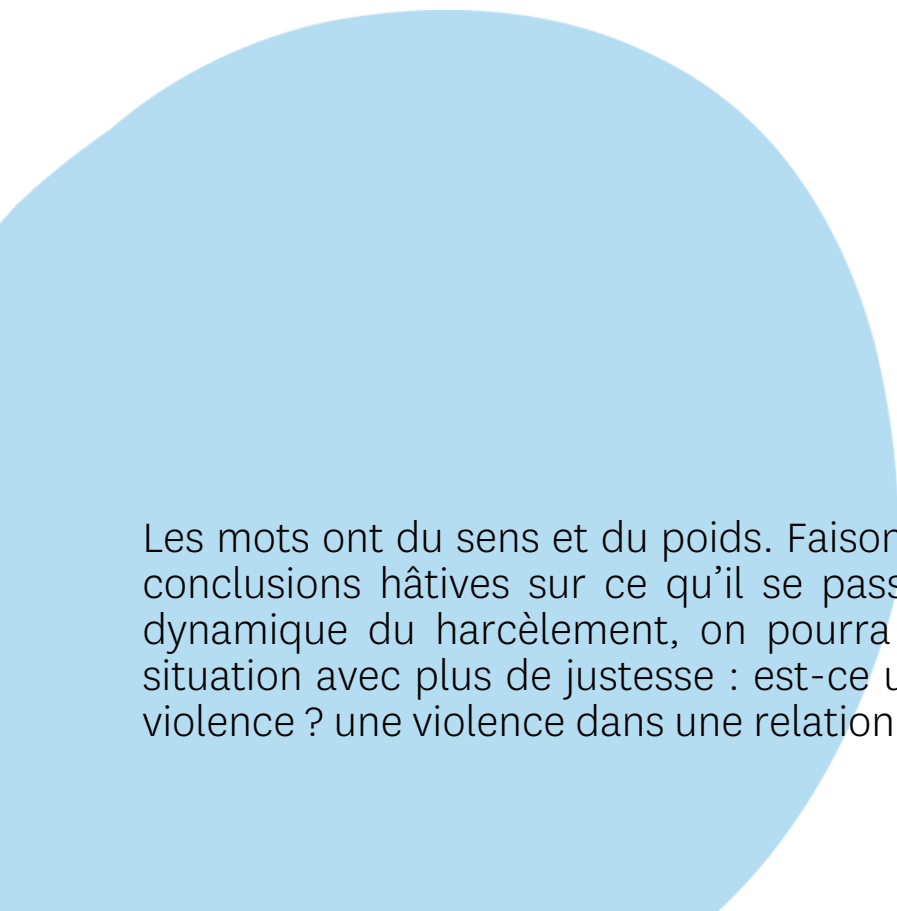
menace, injure, insulte, exclusion, prise ou partage d'image ou d'information privée sans le consentement, photo-montage, intimidation, incitation à la violence, usurpation d'identité, etc... tout acte portant atteinte à la dignité d'une personne ou d'un groupe de personnes

qui se déroulent dans un **espace digital et/ou avec des outils numériques**.

Les cyber-violences peuvent se pratiquer sous différents formats (texte, image, photographie, vidéo, audio..) et par différents moyens (téléphone portable, messagerie instantanée, forum, chat, jeux en ligne, courrier électronique, réseaux sociaux, application, site de partage de photographie..).



Harcèlement, cyber- harcèlement



Les mots ont du sens et du poids. Faisons attention à ne pas faire des conclusions hâtives sur ce qu'il se passe ! En comprenant mieux la dynamique du harcèlement, on pourra reconnaître et nommer une situation avec plus de justesse : est-ce un conflit ? un acte unique de violence ? une violence dans une relation d'emprise ?

Harcèlement et cyber-harcèlement

Le harcèlement est de la **répétition de violences**, par une ou plusieurs personnes ; intensive, graduelle ou régulière ; pouvant survenir dans toutes sphères de la vie.

Quand il est commis “par l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique”, on parle de **cyber-harcèlement**.

Le harcèlement peut combiner les différentes formes de violence déjà citées. Parmi les éléments spécifiques à une dynamique de harcèlement, l'on retrouve la répétition mais aussi le **déséquilibre de pouvoir** entre la victime et l'agresseur.



Quand on traite un mal-être, le point de vue qui importe est celui de la victime ; peu importe si l'auteur n'a pas eu conscience de son impact ou n'a agi qu'une seule fois TANT que cela nuit à la victime. Cela peut être le cas dans le "harcèlement de meute" ou raid numérique.



Le cyber-harcèlement (art.222-33-2-2 code pénal) est puni de peines pouvant aller jusqu'à **2 ans d'emprisonnement et 30 000 € d'amende**.



Si la victime a moins de 15 ans, la peine peut être de **3 ans et 45 000 €** (art.222-33-2-2 code pénal).

Si le harcèlement moral et le cyber-harcèlement viennent d'un actuel ou ex partenaire, la peine peut aller jusqu'à **5 ans d'emprisonnement et 75 000 €** (art. 222-33-2-1 code pénal).



Si le harcèlement est à caractère sexuel, la peine peut aller jusqu'à **3 ans et 45 000 €** (art. 222-33 code pénal).

Envoyer des insultes par message et commenter les publications de son ex-partenaire, lui suscitant angoisse et auto-censure

Le cyber-sexisme



Le sexisme peut s'exprimer par des paroles et attitudes préjudiciables, discriminatoires et/ou violentes envers des personnes en raison de leur sexe et leur genre. En ligne, on parle de “cyber-sexisme”.

Ex : commentaire de dénigrement physique, envoi de photo de partie génitale (dick pic), menace de diffusion d'image intime, groupe de partage de photo-montage pornographique, comportement visant à exclure les femmes d'un espace en ligne..

SLUT SHAMING
"honte à la salope"

Forme de dénigrement, qui consiste à dévaloriser la personne dont la tenue vestimentaire, le maquillage, l'attitude, voire les activités sexuelles, ne correspondent pas aux normes en vigueur dans un groupe de personnes.

Reprocher à une femme qui porte un décolleté de ne pas avoir un comportement professionnel

VICTIM BLAMING
"blâmer la victime"

Tenir partiellement ou entièrement responsable une victime de ce qu'elle a subi.

Dire que c'est normal de se faire insulter si on poste une photo de soi en maillot de bain



Le “slut shaming”, le “victim blaming” peuvent être des formes de cyber-violences participant à du cyber-harcèlement.



Expressions de cyber-violence

Connaître des exemples et phénomènes de cyber-violences peut aider à comprendre et reconnaître la situation dans laquelle une personne se trouve peut-être. Vous pouvez aussi vous appuyer sur ces exemples dans certaines des questions que vous posez pour évaluer la situation de la personne et/ou l'accompagner dans son auto-évaluation, afin de lui permettre de prendre du recul, comprendre que ce n'est pas de sa faute et connaître des recours possibles.

Expressions de cyber-violence

Il existe différentes formes de cyber-violences, en voici quelques exemples.

LES CYBER-VIOLENCES QUI TOUCHENT À LA VIE PRIVÉE

Porter atteinte à la vie privée signifie mener des actions qui nient le droit d'une personne à préserver ses **informations personnelles et ses activités privées**.



C'est une **infraction** (art. 266-1 code pénal) qui peut être punie de **2 ans d'emprisonnement et 60 000 € d'amende** si elle est commise par un ex ou actuel partenaire car il s'agit d'une circonstance aggravante.

En ligne, cela peut prendre différentes formes :

DOXING

Transmettre des informations sur une personne qui permettent de l'identifier ou de la localiser, dans le but de lui nuire, à elle ou aux ses membres de sa famille.

*infraction punissable de **3 ans d'emprisonnement et de 45 000 € d'amende** (art. 223-1-1)*

OUTING

Révéler des informations intimes sur une personne sans "extérioriser" son consentement.

*infraction punissable de **1 an d'emprisonnement et de 45 000 € d'amende** (art.226-1)*

USURPATION D'IDENTITÉ

Toute action qui consiste à utiliser les informations personnelles de quelqu'un pour se faire passer pour elle.

*infraction punissable de **1 an d'emprisonnement et de 15 000 € d'amende** (art.226-4-1)*

Publier le numéro de téléphone ou l'adresse d'une personne

Faire un post dévoilant l'orientation ou les pratiques sexuelles d'une personne

Créer un compte au nom et à l'image d'une personne pour se faire passer pour elle

Des exemples dans un contexte d'intimité, de relation amoureuse ou de couple :

- vérifier la communication de son/sa partenaire (texto, appel, message, e-mail..)
- utiliser les appareils et comptes sans l'accord de son/sa partenaire
- monitorer les déplacements de son/sa partenaire (géolocalisation..)
- empêcher que son/sa partenaire communique (contrôler ce qui est dit et à qui, confisquer les appareils, changer les mots de passe)
- se faire passer pour sa partenaire en vue de lui nuire socialement, professionnellement etc.

Ces cyber-violences peuvent être des faits constitutifs de harcèlement moral qui est punissable de **3 à 5 ans d'emprisonnement et de 45 000 à 75 000 € d'amende** dans le cadre du couple (art. 222-33-2-1).

LES CYBER-VIOLENCES QUI TOUCHENT À L'IMAGE

Porter atteinte à l'image d'une personne signifie mener des actions qui nient son droit à contrôler l'utilisation de son image. Cela inclut la publication ou l'utilisation non autorisée de photos ou vidéos sans le consentement de la personne dont c'est le corps.



C'est une **infraction** (art. 226-1 code pénal) qui peut être punie de **2 ans d'emprisonnement et 60 000 € d'amende** si elle est commise par un partenaire, conjoint, ex.... car il s'agit d'une circonstance aggravante.

DIFFUSION D'UN PHOTOMONTAGE

Diffuser, publiquement (ex : site internet) ou en privé (ex : groupe de messagerie), un montage (son, image..) sans le consentement de la personne qui y figure et sans indiquer qu'il s'agit d'un montage.

Envoyer ou publier une photo d'un animal mort avec le visage d'une personne collé dessus

*infraction punissable de **2 ans d'emprisonnement et de 45000 € d'amende** (art. 226-8).*

*Si a caractère sexuel : **2 ans et 60 000 € d'amende**, et de **3 ans et 75000 €** s'il s'agit d'un deepfake (art.226-8)*

DIFFUSION DE CONTENU INTIME NON CONSENTIE

Diffuser, publiquement (ex : sur les réseaux) ou en privé (ex : par messagerie), un contenu intime sans le consentement de la personne qui y figure.

Partager un nude de son/sa partenaire sans son accord OU d'une personne à son insu



Un contenu intime peut être une photo, une vidéo, un texte, un audio. Un "nude" (=nu) désigne une photo nue ou dénudée, suggestive ou sexuellement explicite.

*infraction punissable de **2 ans d'emprisonnement et de 60000 € d'amende** (art. 226-2-1)*

Des exemples dans un contexte d'intimité, de relation amoureuse ou de couple :

- imposer de prendre ou de recevoir des contenus intimes
- conserver ou diffuser des contenus intimes sans consentement
- diffuser ou menacer de diffuser des contenus intimes

Ces cyber-violences peuvent être des faits constitutifs du délit renforcé d'atteinte à la vie privée (atteinte à l'image) qui est punissable de **2 ans d'emprisonnement et de 60 000 € d'amende** cf ci-dessus. Voir d'agressions sexuelles (art. 222-28) si votre partenaire vous force à filmer des actes sexuels.





Signes de mal-être

Avoir conscience des signes indicatifs de mal-être peut aider à se rappeler comment la personne avec qui l'on échange peut se sentir, l'état dans lequel elle est peut-être. Vous pouvez aussi vous appuyer sur ces signes dans certaines des questions que vous posez pour évaluer la situation de la personne et/ou l'accompagner dans son auto-évaluation.



Signes de mal-être

Les cyber-violences peuvent avoir des conséquences sur les individus qui sont similaires aux violences situées dans le monde physique.

Voici des exemples de signaux / symptômes manifestés par une personne qui peuvent indiquer une situation de mal-être :



- Nervosité, angoisse
- Agressivité, irritabilité
- Perte d'estime de soi, perte de confiance en soi
- Changements radicaux dans son apparence, ses habitudes, ses humeurs, ses envies
- Baisse de motivation, de performance, de résultat
- Phobie scolaire/du travail, absentéisme, arrêt maladie



- Isolement
- Angoisse lors de consultation des réseaux sociaux/réception de messages
- Fréquentation augmentée des réseaux sociaux ou au contraire retrait total et soudain
- Maux de ventre/tête
- Perte / perturbation de sommeil
- Troubles alimentaires, addictions
- Atteinte à son corps, pensées morbides, envie de mourir, tentative de suicide



Des exemples de changements d'attitude qui peuvent alarmer dans un contexte d'intimité, de relation amoureuse ou de couple :

- changer sa photo de profil ou supprimer des photos parce que son/sa partenaire nous critique
- ne plus poster ce que l'on veut par crainte de ce que son/sa partenaire en dira
- être toujours connecté à son téléphone pour pouvoir répondre tout le temps et tout de suite à son/sa partenaire
- quitter les groupes de messagerie parce que son/sa partenaire n'en fait pas partie

Impacts du harcèlement et de la violence sur une personne

Exemple d'une liste de questions qu'une personne peut se poser pour réfléchir à l'impact de la situation sur son bien-être :

Est-ce que j'ai ... ?

- du mal à réfléchir, me concentrer
- souvent mal au ventre, à la tête
- du mal à m'endormir, à me lever
- l'impression que la tristesse déborde et que mon moral s'effondre, je me sens découragé
- la sensation que rien ne m'intéresse, que rien ne m'amuse
- un fort sentiment d'isolement
- moins ou plus du tout envie de voir mes proches, de faire une activité que j'aime
- moins ou plus du tout envie d'aller au travail, au club de sport ou autre lieu d'activité ou de socialisation ; j'angoisse de devoir y aller
- l'impression de ne pas y arriver - au travail, dans mes activités...je vois une baisse de mes résultats, de mes performances
- de la difficulté à supporter mon environnement, je suis irritable, voire agressif, à bout de nerfs
- envie de soulager un mal-être, de me faire du mal, de mourir
- de l'angoisse quand je vais sur les réseaux sociaux / quand je reçois des messages / appels / e-mails
- l'impression de devoir vérifier mon téléphone, mes réseaux sans arrêt, m'assurer de ce qui s'y passe

GESTION DES ÉMOTIONS

La gestion des émotions n'est facile pour personne. Ressentir une émotion, comprendre ce que l'on ressent sur le moment, le nommer pour soi-même, choisir si et comment le communiquer sont des choses qui demandent beaucoup d'attention et de recul.

Dans une situation de violence, la gestion des émotions est spécialement difficile. Prendre le temps d'y faire face, poser ses ressentis (notamment par écrit) peut aider à digérer ce qui nous arrive, avoir du recul pour pouvoir accepter ses émotions et affects, les légitimer, jusqu'à peut-être reconnaître sa position de "victime".

La personne autrice de violence a elle aussi une gestion problématique de ses émotions. Le comprendre (et non pas l'accepter) peut permettre de mieux se protéger en anticipant les réactions qui suivraient, ainsi que de délégitimer les propos et actes de l'auteur.



III. Que peut-on faire ?

Le recueil de la parole.....	19
Le sentiment de sécurité en ligne.....	22
Des bons réflexes avec Mémo de vie.....	27





Le recueil de la parole

Rappel et partage de bonnes pratiques

Dans beaucoup de situations de violence, un des enjeux prioritaires pour l'enclenchement d'un processus de protection est de pouvoir permettre à la personne ciblée de sortir de l'isolement.

Cet isolement peut se manifester physiquement, numériquement, émotionnellement et peut être contraint, imposé. Il peut aussi être lié à l'incapacité sur le moment de prendre conscience de ce que l'on vit.

En tant que professionnel, il y a un rôle de responsabilité à jouer dans ces premiers moments clef, en se rendant disponible, en mettant en place un climat de confiance propice au partage, en accompagnant la prise de conscience dans un cadre sécurisant et respectueux du pouvoir d'agir de la personne.

Quand une personne se confie :

Plutôt faire

- Écouter
- Rassurer
- Respecter la confidentialité
- Respecter le rythme de la personne
- Se rappeler que les situations de mal-être sont complexes et délicates
- Rester dans une posture d'écouter
- Encourager la personne à en parler à des proches/des associations, l'informer de ses possibilités et de ses droits
- Respecter sa volonté et ses besoins
- Reprendre les mots de la personne pour se définir ou décrire son vécu (ex : ne pas dire "victime" si la personne ne l'a pas dit)
- Signaler si vous avez un doute ou si danger grave (informer la personne dans ce cas)
- Échanger entre accompagnants autour de comment l'on se sent

Éviter de faire

- Essayer de résoudre la situation seul
- Interrompre, couper la parole, finir les phrases de la personne
- Forcer à en dire plus, essayer de convaincre d'agir d'une certaine façon
- Laisser son expérience personnelle prendre le dessus, prendre toute la place
- Faire culpabiliser (victime, témoin, harceleur/auteur), laisser entendre son jugement
- Remettre en cause la parole, minimiser ou banaliser la gravité de la situation
- Utiliser la violence (menace, insulte, coup) envers l'auteur
- Oublier que l'on n'est pas des experts ou des héros mais que l'on est simplement là pour écouter et faire de notre mieux



Signaler un contenu en ligne, c'est [avertir](#) la plateforme ou les personnes compétentes qu'[une publication doit être supprimée](#) car elle enfreint les règles de la plateforme ou de la loi, notamment en portant atteinte à une personne.

Un [signaleur de confiance](#) est une entité compétente, directement en lien avec les réseaux sociaux, et [capable d'agir rapidement](#) pour supprimer une publication (voir Services d'aide p.33).



Comment réagir ? Accompagner



OBJECTIFS DE L'ACCOMPAGNANT :

1

Faire que la personne se sente écoutée et non isolée dans son mal-être.

2

Relever des informations pour évaluer la situation (est-ce que l'action s'est arrêtée, est-ce que la personne est en sécurité sur le moment).

Si ce n'est pas une urgence immédiate, chercher à comprendre dans quel état se trouve la personne et quel impact cela a sur elle (changement de comportement, isolement, confiance en soi...).

3

Aider à la réflexion d'un "plan" d'action :

Suggérer des actions concrètes, comme informer l'entourage de la situation, parler à des professionnels/associations, limiter l'accès à ses informations personnelles en ligne, signaler, faire des captures d'écran, porter plainte... etc.

EXEMPLES DE SITUATIONS

Face à une personne en difficulté devant des problématiques cyber l'accompagnement doit être bienveillant et sans jugement. L'objectif est d'écouter, d'évaluer la situation et d'agir pour assurer la sécurité de la personne. Voici quelques situations et pistes actions possibles.

Que faire si une personne vous dit qu'une photo d'elle est en train de circuler ?

1

Que se passe-t-il ? Que pense la personne de ce qu'il se passe ?

Quel est le contenu de la photo ? Qui sont les acteurs concernés (ex : âge) ? Sur quel espace/plateforme ? Est-ce un fait isolé / répété ? L'action est-elle toujours en cours ?

2

Que peut-on faire pour stopper l'action ?

Bloquer, signaler, paramétrer ? Communiquer avec les acteurs concernés (auteur, témoin, administrateur) ? Demander de l'aide technique (ex : Point de contact si contenu intime, 3018 si mineur - voir Services d'aide) ? Prévenir / reporter la situation (direction, autorités) ?

3

Que peut-on faire pour éviter que cela se reproduise ?

Bloquer, changer d'appareil, supprimer son compte, reparamétrer les outils ? Communication, actions de prévention, charte ? Porter plainte, mesures envers les responsables ?

Que faire si une personne vous dit qu'elle est cyber-harcelée ?

1

Que se passe-t-il ? Que pense la personne de ce qu'il se passe ?

Quels sont les faits ? Y a-t-il répétition ? Si oui, par une ou plusieurs personnes ? Qui sont les acteurs concernés (ex : fonction, interne/externe, connu/inconnu) ? Sur quelle plateforme/espace ? Par quel moyen (ex : appel, message) ? L'action est-elle toujours en cours ?

2

Que peut-on faire pour stopper l'action ?

Bloquer, signaler, paramétrer ? Communiquer avec les acteurs concernés (auteur, témoin, administrateur) ? Demander de l'aide technique (voir Services d'aide) ? Prévenir / reporter la situation (direction, autorités) ?

3

Que peut-on faire pour éviter que cela se reproduise ?

Bloquer, changer d'appareil, supprimer son compte, reparamétrer les outils ? Communication, actions de prévention, charte ? Porter plainte, mesures envers les responsables ?



Le sentiment de sécurité

Comment permettre de se sentir en sécurité en ligne ?

Ne pas comprendre comment fonctionne un outil peut parfois mener à ne pas l'utiliser, parce que l'on ne saurait pas contrôler ce qu'il s'y passe. Pour éviter que les personnes s'auto-censurent et s'isolent par crainte de "mal" utiliser les écrans, internet, les réseaux sociaux, il est essentiel de s'intéresser aux usages de la personne pour comprendre ce qu'elle peut mettre en place pour se sentir en sécurité en ligne, c'est-à-dire en se sentant libre, en contrôle et sans crainte de ses outils.

Toute cette prochaine partie s'adresse directement à la personne que vous accompagnez.

Le sentiment de sécurité en ligne

Une première question à se poser est : est-ce que je me sens en sécurité en ligne ?

Pour vous aider à y répondre, voici 3 questions :

1. Est-ce que je peux accéder librement aux outils numériques ?
2. Est-ce que j'ai le contrôle sur mes appareils, comptes et applications ?
3. Est-ce que je peux exister en ligne sans limite ou crainte ?

Si vous avez des doutes ou si vous répondez non à l'un ou plusieurs de ces 3 points, il peut être utile d'explorer pourquoi. La suite de ce guide propose des choses à faire pour se sentir plus en sécurité dans ses activités et plus à l'aise avec ses propres outils.

1

Accès libre

Avoir une adresse e-mail, des mots de passe et des comptes dont on est le seul à avoir accès.

Comme première étape de sécurisation, il vous faut une [adresse e-mail à laquelle vous seul avez accès](#), (elle vous est notamment nécessaire pour créer votre compte [Mémo de vie](#) !) ainsi que des mots de passe dont vous seul avez connaissance.



Si ce n'est pas le cas, vous pouvez en créer une depuis un [appareil jamais utilisé](#) (celui d'un proche, d'une bibliothèque ou d'un cyber-café) + sélectionner un moyen de récupération (autre adresse e-mail, numéro de téléphone ou question de sécurité) qui ne soit pas accessible à d'autres personnes que vous + choisir un mot de passe fort (voir ci-après) + se déconnecter dès que vous quittez l'appareil.



VOTRE CONFIDENTIALITÉ AVEC MÉMO DE VIE

Vos données sont sauvegardées sur un hébergeur certifié et sécurisé en Europe. Vous pouvez optimiser ces mesures avec les conseils « Confidentialité & Sécurité » et ceux de l'article « Comment optimiser mes mesures de confidentialité et de sécurité sur [Mémo de Vie](#) ».

Votre historique est quasiment inexistant.

Vite, je quitte

De plus, vous pouvez quitter [Mémo de Vie](#) à tout moment en cliquant sur le bouton "Vite je quitte", toujours en bas à droite de la page qui vous redirigera vers un autre site.

BIEN CHOISIR SES MOTS DE PASSE



Choisissez des mots de passe complexes, différents et non-signifiants ! Ne les communiquez pas ! Même à votre partenaire ou autre proche. On sait que ce n'est pas évident et voici les 4 choses importantes à suivre :

1

Ils doivent être **forts** : + de 12 caractères (dont des majuscules, chiffres, minuscules et caractères spéciaux... Pas de suite de chiffres !).

2

Un mot de passe différent pour chaque **compte**, site et application. Ou au moins pas le même partout ! Vous pouvez utiliser un générateur de mots de passe et coffre-fort pour vous aider.

3

Ne jamais les **écrire** sur des post-it ou sur des documents accessibles sur vos appareils.

4

Ils ne doivent pas avoir un rapport avec **votre identité ou vos proches** (pas de nom, surnom, adresse, date d'anniversaire !)



Précision : quitter une app ou fermer une page est différent que se déconnecter ! La session peut encore être accessible sur ces appareils ou même en communication avec d'autres appareils connectés ou applications ouvertes. Pour empêcher que d'autres aient accès à votre compte ou session après vous, déconnectez-vous.

2

Contrôle de ses comptes et appareils

Vérifier quels appareils et quelles applications sont connectées à vos outils.

VÉRIFIER QUI A ACCÈS À VOS COMPTES

Si vous utilisez des plateformes comme google ou microsoft, des smartphones et des objets connectés, vous pouvez aller vérifier dans la partie "compte" quels appareils et applications sont reliées et même actuellement connectées.

1

Si vous remarquez des connexions ou appareils connus ou inconnus: prendre une capture d'écran avec l'identification de l'appareil, date et heure.

2

Éjecter l'appareil pour révoquer l'accès (si c'est possible dans votre situation sans vous mettre en danger).

3

Désactiver la liaison avec d'autres applications si vous n'êtes pas sûres qu'elles sont sécurisées (ex : youtube).

4

Changer le mot de passe de votre compte.

5

Mettre en place une double authentification. Toute tentative de connexion nécessitera un code reçu par sms ou e-mail.

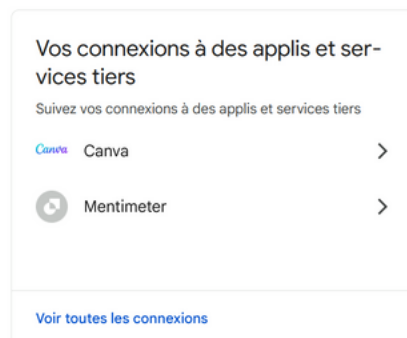
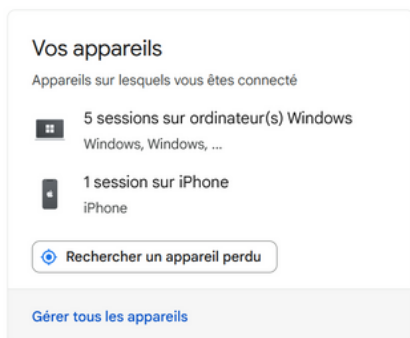
6

Mettre en place des fonctions qui vous alertent si un nouvel appareil tente de se connecter à votre compte.



Réfléchir à une variété de comptes que vous utilisez :

e-mail, liaison entre appareils (télévision, téléphone, tablette, ordinateur), comptes communs (banques, cartes de fidélité supermarché/magasins, service de livraison (nourriture, objet), taxi/service de transport, plateforme d'achat en ligne, etc).



EST-CE QU'IL Y A DES LOGICIELS OU DES OBJETS QUI ME SURVEILLENT ?

La surveillance électronique peut avoir lieu via des caméras, microphones, "mouchards" (ou appareils de mise sur écoute), réseaux sociaux ou e-mails. Cela peut aussi inclure l'abus de logiciels ou applications de surveillance installées sur un ordinateur, une tablette ou un smartphone pour suivre les activités de l'utilisateur. Des traceurs de localisation peuvent également être utilisés. Vous pouvez déjà faire un tour dans votre maison, bureau, voiture pour vérifier qu'il n'y a pas de trackers (ex : air tag).



Attention aux micros et aux caméras des ordinateurs, tablettes et smartphones qui peuvent être activés à distance par d'autres appareils connectés !

Pour des activités délicates : utiliser un appareil sécurisé, la navigation privée et effacer l'historique.

D'autres points d'attention :

- Téléchargement

Ne téléchargez des documents que lorsque vous êtes sur un appareil sécurisé et dans un espace temps où vous vous sentez en sécurité. Les charger dans Mémo de Vie. Supprimer les documents téléchargés dans les dossiers Téléchargements et Captures d'écrans. Vider la corbeille. Les supprimer aussi dans le Cloud !

- Applications connectées

Ex : sur android, les photos prises sur le téléphone peuvent être directement reliées à Google Photos ou à Google Drive.

Ex : sur iphone, la prise de photo peut préciser la localisation.

**« Ça me rassure d'avoir mes papiers importants et ceux de mes enfants sécurisés et accessibles en ligne ! Ça me permet d'être autonome. »
- une utilisatrice de Mémo de vie**

3

Régulation de ses comptes et appareils

Vérifier les paramétrages (tous écrans, réseaux sociaux, e-mail, applications) pour savoir ce que vous partagez et à qui.

Les réseaux sociaux fonctionnent tous avec des paramètres “par défaut” concernant le partage d’information sur votre vie privée, votre profil (photo, âge..), vos activités (like, partage, commentaire) et vos publications, etc... Vous pouvez bien évidemment les modifier pour protéger votre compte en régulant les interactions, les contenus et les informations que vous partagez.

Quelques exemples :



- Whatsapp : déterminer si les personnes qui ne sont pas dans vos contacts peuvent ou non vous ajouter à des groupes de discussion, choisir si les photos que l’on vous envoie sont directement enregistrées dans la galerie de votre téléphone
- Instagram : stopper temporairement toutes les interactions sur votre compte grâce à l’outil “limites”
- Snapchat : décider du caractère éphémère ou non des messages et des photos échangés sur Snapchat (attention tout de même aux captures d’écran), autoriser ou refuser l’accès à votre géolocalisation

Il existe plusieurs options pour restreindre les interactions avec un utilisateur spécifique :

1. Bloquer totalement la personne (elle ne peut plus vous contacter. Attention : elle peut sans rendre compte)
2. “Muter” (=mettre en sourdine) la personne (vous continuez de recevoir ce qu’elle vous envoie mais sans notification et avec enregistrement des conversations, si vous souhaitez regarder parfois ce qu’elle vous envoie, garder des preuves)
3. Pas de blocage mais filtrage de mots (la personne peut vous contacter mais vous pouvez, par exemple, décider de cacher les insultes)

En plus de ces paramètres, un parcours de signalement est proposé sur l’ensemble des réseaux sociaux.





Les bons réflexes avec **Mémo de vie**

Afin de se projeter dans un environnement familial, nous vous proposons de mettre en pratique toutes ces idées avec l'outil Mémo de Vie.

Cette prochaine partie s'adresse directement à la personne que vous accompagnez.

Comment réagir face à une cyber-violence

Face à une cyber-violence, il est important de réagir et rapidement si possible. Nous vous proposons de suivre ces 3 étapes simples.

1

Garder les preuves

capture(s) d'écran avec date, heure et pseudonyme, stockée(s) dans le coffre fort Mémo de vie, sur clé usb ou disque dur.



RASSEMBLER SES DOCUMENTS DANS LE COFFRE-FORT MÉMO DE VIE

Ce coffre fort numérique sécurisé et confidentiel est à votre disposition, pour stocker des documents officiels mais aussi des photos, vidéos, captures d'écran qui pourront constituer des preuves.

« Je regrette de ne pas avoir connu Mémo de vie avant ! J'ai perdu beaucoup d'indices dont j'aurais bien eu besoin avant ! Maintenant je garde tout, on ne sait jamais ! » - une utilisatrice de Mémo de vie



UTILISER LE JOURNAL POUR RACONTER SON VÉCU



Raconter et enregistrer les situations que l'on vit (positives comme négatives) le plus régulièrement possible permet de structurer les événements dans le temps et construire un récit cohérent. Le journal est consultable quand vous le souhaitez.

« Ça m'aide à prendre du recul pour analyser, puis une fois que l'événement est enregistré, on a dit les choses qui nous pesaient, on sait que c'est sauvegardé, donc c'est libérateur. Ça fait prendre conscience et c'est aussi un travail que je continue avec ma psychologue. » - une utilisatrice de Mémo de vie

Si l'on s'aperçoit que l'on éprouve des émotions négatives durant plusieurs jours d'affilée alors peut être que l'on traverse une situation difficile.



Renseigner ses émotions, ses humeurs permet de prendre du recul et peut être un signal d'alerte quant à la situation que vous traversez. N'oubliez pas le journal !

Comment vous sentez-vous ?

Afin de suivre votre évolution, indiquez l'émotion qui vous correspond le plus aujourd'hui.



"Contacter un professionnel a été la première étape dans mon chemin vers la liberté." - utilisatrice de *Mémo de vie*

2

Signaler, bloquer le contenu / compte

via la plateforme en question, signaleur de confiance, pharos (voir Services d'aide p.33)

Signaler un contenu, c'est **avertir** la plateforme ou les personnes compétentes qu'une **publication doit être supprimée** car elle enfreint les règles de la plateforme ou qu'elle porte atteinte à une personne ou à soi.

Un **signaleur de confiance** est une entité compétente, directement en lien avec les réseaux sociaux, et **capable d'agir rapidement** pour supprimer une publication.



Si un contenu intime circule sans votre consentement, signalez-le à l'association Point de contact !

En cas de cyber-harcèlement, l'association Respect Zone et le 3018 sont là pour vous aider.

3

En parler !

à une personne de confiance ou à un professionnel. Il est également possible de porter plainte.



TROUVER DE L'AIDE ET DES RÉPONSES

Une liste de **ressources** (documents utiles, outils, articles...) est accessible depuis **Mémo de vie** pour vous renseigner, répondre à vos questions et vous aider dans vos démarches. L'application mobile Respect Zone - gratuite - peut aussi vous accompagner en cas de cyber-violence.

Vous trouverez **une liste de contacts, de numéros d'assistance ainsi qu'un tchat anonyme pour vous aider** quelque soit votre situation. Ainsi, vous pourrez entrer en contact avec des professionnels qui sont là pour vous accompagner à tout moment.





IV. Et maintenant ?

Résumé et premiers pas pour les usagers.....	31
Ressources boussole.....	32
Services d'aide.....	33





Résumé et premiers pas pour les usagers

POUR COMMENCER DÈS MAINTENANT UN PLAN DE SÉCURISATION EN LIGNE :



Est-ce que j'ai une **adresse e-mail** dont je suis la seule personne à avoir accès ?

Si non, en créer une !



Est-ce que je suis la seule à connaître mes **mots de passe**, surtout pour mes comptes les plus importants ?

Si non, changer mes mots de passe et en choisir des "forts" !



Est-ce que je sais quels **appareils** sont connectés à mes téléphone/ tablette/ ordinateur ?

Si non, aller vérifier dans les paramètres de téléphone/ tablette/ ordinateur !



Est-ce que je suis sûre de ne pas exposer d'**informations privées** en ligne, sans le savoir ?

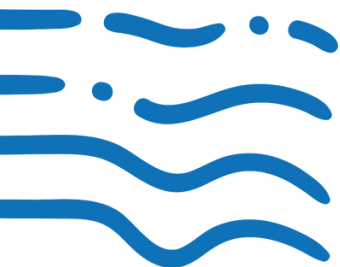
Si non, aller vérifier les paramètres par défaut de mes appareils et comptes les plus importants, dont :

- accès public/privé ou restreint
- géolocalisation
- affichage de prénom, nom, numéro de téléphone, adresse
- bluetooth, air drop/nearby share

Pas besoin d'être des experts de la technologie pour mettre en place de bons réflexes de sécurité.

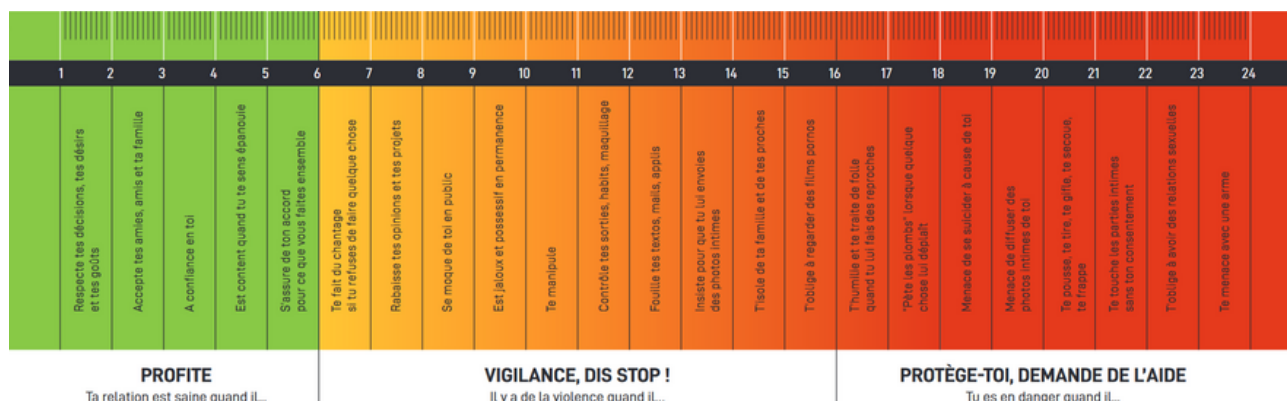


**Dire
aujourd'hui pour
préserver demain**



Ressources boussole

Violentomètre / harcèlomètre



Suis-je victime de cyber-violences conjugales ?

Pour en savoir plus
[cliquer ici](#)

DANS UNE RELATION RESPECTUEUSE ET ÉGALITAIRE MON OU MA PARTENAIRE :

- ☐ Respecte ma vie privée et ne cherche pas à consulter mon téléphone
- ☐ Me fait confiance et ne me demande pas de me justifier sur mes communications
- ☐ Me demande mon autorisation avant de prendre une photo de moi ou de la montrer à d'autres personnes
- ☐ Demande mon accord avant de m'envoyer un contenu à caractère sexuel
- ☐ Commente mes publications sur les réseaux sociaux d'une manière qui ne me met pas mal à l'aise
- ☐ Ne conserve pas mes *nudes* (images intimes) après la séparation

MON OU MA PARTENAIRE N'A PAS LE DROIT DE :

- ☒ Exiger que je sois tout le temps joignable
- ☒ Consulter mes communications (sms, mails, réseaux sociaux, comptes administratifs, etc.) sans mon consentement
- ☒ Me harceler pour savoir ce que je fais, où je suis et avec qui
- ☒ M'insulter par messages, m'envoyer des menaces
- ☒ M'interdire de communiquer avec certaines personnes
- ☒ Répondre à ma place à des messages ou des appels sans mon accord
- ☒ Exiger que j'envoie des photos pour prouver où je suis
- ☒ Exiger que je partage ma géolocalisation lors de mes déplacements
- ☒ Contrôler mes publications sur les réseaux sociaux
- ☒ Exiger d'avoir les mots de passe de mon téléphone/ma tablette/mon ordinateur ou de mes comptes (mails, réseaux sociaux, administratifs, etc.)
- ☒ Me confisquer mon téléphone/ma tablette/mon ordinateur
- ☒ Insister pour que je prenne des photos intimes, me faire du chantage si je refuse
- ☒ Me forcer à filmer nos relations sexuelles
- ☒ Me menacer de diffuser ou diffuser des images/informations intimes
- ☒ Me forcer à regarder du contenu pornographique
- ☒ Obtenir des informations pour savoir où je suis et avec qui, en surveillant ou en communiquant avec mes enfants/mes proches
- ☒ Utiliser des informations en ligne pour me surveiller après la séparation





Services d'aide



Tous ces services sont gratuits, anonymes et/ou confidentiels. Certains sont accessibles 7j/7 et 24h/24*



**Retrouver tous les contacts
de Mémor de Vie**

Cyber-harcèlement, cyber-violences



Écrire à Respect Zone

app, site, réseaux sociaux

(Cyber)harcèlement, cyber-violences,
haine en ligne



Appeler ou écrire au 3018

9h-23h

Cyber-harcèlement, harcèlement scolaire,
exposition à des contenus violents - mineurs

Signalement de contenu interdit



Pharos (police), internet-signalement.gouv.fr

Plateforme de signalement de contenu
interdit en ligne



pointdecontact.net (association)

Signalement de contenu illicite, contenu
à caractère intime

Autres sujets spécialisés



Appeler le 119

Service national d'accueil
téléphonique de l'enfance en danger



Écrire au 114

Service d'aide aux personnes en situation
de handicap



Appeler le 116 006

9h-19h

Aide aux personnes victimes,
renseignement juridique



Appeler le 3919

*Accessible en 12 langues ainsi qu'aux personnes
sourdes et malentendantes*

Violences faites aux femmes



Appeler le 3977

9h-19h (sauf de 13h à 14h le WE)

Maltraitance des personnes âgées et des
adultes en situation de handicap



Contacter SOS Homophobie

horaires variables selon le jour

Aide aux personnes victimes de LGBTphobie



Appeler le 3928

du Lundi au Vendredi, 9h30-19h

Service gouvernemental contre les
discriminations



*sauf indication contraire





V. Approfondir

Précisions juridiques.....	35
Nos données personnelles.....	40
Sources d'information.....	41



Précisions juridiques : porter plainte



Cette rubrique offre des informations clés pour guider les victimes de cyber-violences et de cyber-harcèlement. Vous y trouverez des précisions pour éclairer les démarches à suivre et répondre aux interrogations fréquentes sur les droits en ligne et les procédures légales (les étapes pour porter plainte, les données personnelles, les discriminations).

Y A-T-IL UN DÉLAI POUR PORTER PLAINTE ?

Le délai dépend de la nature du préjudice, mais il vaut mieux agir au plus vite.

Concernant les cyber-violences (injure, diffamation et provocation à la haine, discrimination ou violence en raison du sexe ou de l'orientation sexuelle), le délai est de maximum 1 an et concernant le cyber-harcèlement, 6 ans.



Concernant les injures, les propos diffamatoires, etc... le délai court à partir du jour de la publication, mais chaque repost est considéré comme une nouvelle publication ; la date est donc renouvelée et le délai rallongé.

COMMENT PORTER PLAINTE ?

Les cyber-violences sont généralement des infractions et il est donc possible de porter plainte dans n'importe quel commissariat ou gendarmerie, ou par courrier. Les mineur-es peuvent porter plainte seul-es.



Dans tous les cas nous recommandons d'arriver avec le maximum de preuves possible (captures d'écran, liens actifs, preuves des signalements) pour faciliter la constatation de l'infraction.

De plus, nous vous conseillons de conserver une preuve de vos démarches (le récépissé, le PV de plainte).



QUE FAIRE EN CAS DE REFUS DE PLAINTE ?

Les représentants des forces de l'ordre sont dans l'obligation de recevoir votre plainte (art. 15-3_code de procédure pénale) mais il arrive que certains, par manque d'information ou autre raison, peuvent vous faire douter de l'opportunité de la poursuite.



En cas de difficultés, vous pouvez écrire directement au procureur pour porter plainte, mais aussi saisir le Défenseur des droits pour signaler ces manquements.

Vous pouvez aussi vous rendre dans un autre commissariat pour poursuivre vos démarches.

EST-CE QUE JE PEUX PORTER PLAINTE SI JE NE CONNAIS PAS L'AGRESSEUR ? (ANONYMAT EN LIGNE)

Si la victime ne connaît pas les véritables identités du ou des auteurs, elle peut porter plainte contre X.

Les forces de l'ordre, mais aussi le procureur peuvent faire des actes d'enquêtes pour identifier auprès des hébergeurs/plateformes des sites l'adresse IP et puis les informations personnelles du ou des auteurs.

Dans ce cas, il est également conseillé de signaler le contenu en ligne via la plateforme publique du Ministère de l'Intérieur (Pharos), qui dispose d'un service d'enquête spécialisé sur la cyber-criminalité.

Précisions juridiques : la discrimination

La discrimination se définit comme le traitement inégal ou défavorable d'une personne ou d'un groupe de personnes en raison de caractéristiques spécifiques (vraies ou supposées), telles que l'origine, le sexe, l'appartenance religieuse ou l'âge. Ce traitement injuste repose souvent sur des préjugés ou des stéréotypes, et il conduit à des exclusions ou des désavantages dans divers aspects de la vie, tels que l'emploi, l'éducation, ou l'accès aux services.

En d'autres termes, la discrimination consiste à traiter quelqu'un de manière moins favorable que d'autres personnes dans des situations similaires en raison de ses attributs personnels ou de son identité.



Commettre une discrimination à l'égard d'une personne physique ou morale est une infraction (art. 225-2 code pénal) qui peut être punie de **3 ans d'emprisonnement et 45 000 € d'amende**.

Refuser un entretien/ emploi à une personne "à cause" de son identité de genre ou de son sexe

La loi (art. 225-1 code pénal) liste plus de **25 critères** de discrimination, parmi lesquels :

- Âge
- Apparence physique
- Caractéristiques génétiques
- Domiciliation bancaire
- État de santé
- Grossesse
- Handicap
- Identité de genre
- Langue parlée
- Lieu de résidence
- Mœurs
- Opinions philosophiques
- Opinions politiques
- Orientation sexuelle
- Origine
- Patronyme
- Particulière vulnérabilité liée à la situation économique
- Perte d'autonomie
- "Race" prétendue, ethnie, nation : appartenance ou non-appartenance
- Religion : croyance ou appartenance ou non-appartenance
- Sexe
- Situation de famille
- Syndicalisme
- Qualité de lanceur d'alerte, de facilitateur ou de personne en lien avec un lanceur d'alerte

Refuser de louer un appartement à une personne "à cause" de son appartenance religieuse (vraie ou supposée).

Précisions mineurs : le harcèlement

Le harcèlement est une violence qui peut se dérouler entre mineurs ; de nombreux enfants et adolescents sont concernés, que ce soit à l'école, sur les réseaux sociaux ou dans d'autres espaces de socialisation (activités extrascolaires, jeux vidéo en ligne). Il peut prendre différentes formes : insultes, moqueries, menaces, violences physiques, exclusion, et peut évidemment être cyber.

Avec les réseaux sociaux, le harcèlement devient envahissant et (pseudo)anonyme, pouvant impacter gravement la santé mentale des victimes.

Il vient amplifier et prolonger d'autres formes de violences : moqueries, brimades, insultes, discriminations, violences physiques, exclusion du groupe de pairs - un élément essentiel de la sociabilité juvénile.

Comme nommé précédemment, il recouvre différentes formes :

- Publication ou modification de photos sans autorisation,
- Actes de violence provoqués, filmés et diffusés,
- Diffusion d'images à caractère sexuelle, pornographique,
- Usurpation d'identité et violation de la vie privée,
- Menaces, diffamation via courriels, SMS, réseaux sociaux ou jeux en ligne

**21% des 11-15 ans ont déjà été harcelés en ligne (OMS, 2023).
16% des 16-25 ans l'ont aussi été (BDM, 2023), dont :**

- 57% par des inconnus,
- 44% par des camarades,
- 22% par des connaissances rencontrées sur internet
- et 14% par des amis.

Il existe un droit pénal des mineurs qui permet un aménagement des peines et des sanctions adaptées en fonction de l'âge. Dès 10 ans, les jeunes peuvent être sanctionnés, mais c'est à partir de 13 ans qu'une vraie responsabilité pénale émerge.

D'après le sondage de l'éducation nationale réalisé en 2023, le harcèlement touche +1 élève/ classe, soit :

- 19 % des écoliers du CE2 au CM2
- 6 % des collégiens
- 5 % des lycéens.



En cas de cyber-harcèlement, un auteur qui est mineur risque :

- Si victime < 15 ans : 18 mois et 7 500 €
- Si victime > 15 ans : 1 an et 7 500 €

Depuis 2022, le harcèlement scolaire est une infraction (Art. 222-33-2-3 code pénal) dont la sanction est proportionnelle à l'incapacité physique ou mentale de la victime.

Harceleur mineur +13 ans

- Si pas d'ITT ou -8j : 1,5 ans et 7 000 €
- Si ITT 8j : 2,5 ans et 7 500 €
- Si tentative de suicide : 5 ans et 7 500 €

Précisions mineurs : le harcèlement

En cas de plainte, les procureurs de la République doivent faire leur possible pour apporter une réponse rapide et graduée aux infractions de harcèlement scolaire, tout en tenant compte de la présomption de non-discernement pour les mineurs de moins de 13 ans.

Lorsque la saisine d'un juge des enfants n'est pas nécessaire, des mesures alternatives aux poursuites peuvent être envisagées, telles que :

- Stage de citoyenneté ou formation civique,
- « Bannissement numérique » interdisant l'utilisation des réseaux sociaux impliqués dans l'infraction pendant une durée maximale de 6 mois.

QUE FAIRE EN CAS DE HARCELEMENT SCOLAIRE ?



Si vous êtes confronté à une situation de harcèlement scolaire, il faut avoir conscience que c'est un sujet qui mobilise différents types d'acteurs avec des rôles et des responsabilités.

Exemples :

- Établissements scolaires : obligation de prévention et de traitement des situations.
- Enseignants : vigilance, signalement, intervention.
- Chefs d'établissement : mise en place d'un plan de prévention, actions de sensibilisation, sanctions.

Si un parent vous dit que leur enfant est victime de harcèlement scolaire (incluant une forme cyber ou non) :

1

Évaluer la situation

Que se passe-t-il ? Que pense la personne de ce qu'il se passe ? Y-a-t'il un volet cyber (penser aux bons gestes : bloquer, signaler, paramétrer) ? Qui sont les acteurs concernés (ex : âge) ? L'action est-elle toujours en cours ?

2

Vérifier si la situation est signalée à l'établissement scolaire

Si oui : comprendre ce qu'il s'est passé, ce qu'il va se passer.

Si non : dire au parent de prendre contact avec l'établissement, idéalement la cellule du programme Phare.

3

Penser à l'après

En fonction de la situation : contacter des associations (Respect Zone, 3018), porter plainte, prendre des mesures envers les responsables ?

S'assurer de l'état et du suivi psychologiques de la victime et de ses proches.



Nos données personnelles



Nos données personnelles nous appartiennent, et nous avons des droits y compris en ligne. Lorsque des organismes collectent nos informations, ils doivent nous informer clairement sur leur utilisation et nous expliquer nos droits. Ces droits nous permettent de contrôler nos données, de savoir comment elles sont utilisées, de les rectifier si nécessaire, et même de demander leur suppression ou leur retrait. En connaissant et en exerçant ces droits, nous pouvons mieux protéger notre vie privée.

Voici la liste des droits que nous pouvons invoquer :

LE DROIT D'INFORMATION

Un organisme qui collecte des informations sur moi doit me fournir une information claire sur l'utilisation de mes données et sur l'exercice de mes droits

LE DROIT D'OPPOSITION

Je peux m'opposer à tout moment à ce qu'un organisme utilise certaines de mes données.

LE DROIT D'ACCÈS

Je peux demander à un organisme s'il détient des données sur moi (site web, magasin, banque...) et demander à ce que l'on me les communique pour en vérifier le contenu.

LE DÉFÉREMENT D'UN CONTENU DANS UN MOTEUR DE RECHERCHE

Je peux demander aux moteurs de recherche de ne plus associer un contenu qui porte préjudice à mon nom et prénom.

LE DROIT DE RECTIFICATION

Je peux demander la rectification des informations inexactes ou incomplètes me concernant. Il permet d'éviter qu'un organisme utilise ou diffuse des informations erronées sur moi.

LE DROIT DE RETRAIT

Je peux demander le retrait d'un contenu sur moi qui a été publié sans mon consentement, à l'auteur ou à l'hébergeur du site qui devra dépublier (ou anonymiser).

LE DROIT À L'EFFACEMENT

J'ai le droit de demander à un organisme de geler temporairement l'utilisation de certaines de mes données.



Pour exercer vos droits : identifiez l'organisme concerné et envoyez-lui directement votre demande. Pensez à conserver une copie de vos démarches. Si vous n'obtenez pas de réponse ou en cas de refus, vous pouvez faire appel à la CNIL (Commission nationale de l'informatique et des libertés).

Attention toutefois, certains droits peuvent être limités, notamment pour garantir la liberté d'expression, l'information, ou pour respecter des obligations légales comme le délai de conservation des factures (par exemple, 10 ans).

Sources d'information

Sur le harcèlement

- violentomètre/ harcèlomètre
- [application 3018](#)
- [application Respect Zone](#)
- Plateforme pour arrêter la diffusion de contenu intime non consenti : [Point de contact](#)

Sur les cyberviolences conjugales



Relation écrans enfants-parents

- Usage selon les âges : www.36912.org
- Signalétique des jeux vidéos : www.pegi.info/fr
- Signalétique des films/séries : www.arcom.fr

Sur la sécurisation en ligne



Les mots de passe



Les conseils de la CNIL pour un bon mot de passe

Banque, e-commerce, messagerie électronique, documents, administration : de nombreuses démarches de notre vie quotidienne passent désormais par Internet et par la création de comptes sur les...

cnil.fr