CYBER-VIOLENCES CONJUGALES

REPÉRER, ACCOMPAGNER, ORIENTER LES VICTIMES

GUIDE POUR LES PROFESSIONNEL·LES
EN CONTACT AVEC DES FEMMES VICTIMES
DE VIOLENCES CONJUGALES

centre hubertine auclert

Région îledeFrance

INTRODUCTION

9 FEMMES SUR 10 VICTIMES DE VIOLENCES CONJUGALES DÉCLARENT AVOIR SUBI DES **CYBER**VIOLENCES CONJUGALES DE LA PART DE LEUR PARTENAIRE OU EX

L'objectif de cet outil est d'aider les professionnel·les à mieux comprendre les cyberviolences conjugales, à mieux les repérer et à proposer un accompagnement spécialisé aux victimes.

Ce guide s'adresse en premier lieu aux professionnel·les spécialisé·es dans l'accompagnement des femmes victimes de violences conjugales pour renforcer leurs connaissances sur les cyberviolences conjugales et les aider à adapter leurs pratiques d'accompagnement des victimes. Cependant, ce guide peut être utilisé par tout·e professionnel·le en contact avec une femme victime de violences conjugales[1].

Ce guide se compose :

- **de deux parties,** qui permettent de mieux comprendre les cyberviolences conjugales et leurs conséquences ;
- de **8 fiches pratiques** pour mieux repérer, accompagner et orienter les victimes des cyberviolences conjugales ;
- **d'un poster** qui peut être affiché dans les locaux pour faciliter le repérage et la parole des victimes des cyberviolences conjugales.

Le guide et le poster sont disponibles ensemble ou séparément par téléchargement ou commande sur le site du Centre Hubertine Auclert.

1
Ce guide n'a pas pour objectif d'apporter des connaissances fondamentales sur les violences conjugales et leurs mécanismes (le cycle des violences conjugales, les mécanismes d'emprise, etc.). Si vous souhaitez vous former sur cette thématique, vous pouvez contacter le Centre Hubertine Auclert pour une orientation vers une offre de formation spécialisée. Vous pouvez également trouver des informations utiles sur le site : www.comprendre-egalite.com

VOTRE (EX) PARTENAIRE VEUT **LIRE TOUS VOS MESSAGES.**

IL SURVEILLE VOS **DÉPLACEMENTS.**

IL VEUT **VOUS JOINDRE** TOUT LE TEMPS.

IL EXIGE DE SAVOIR **OÙ** ET **AVEC QUI VOUS ÊTES.**

CE SONT DES (CYBER)**VIOLENCES CONJUGALES.**

SOMMAIRE

LES CYBERVIOLENCES CONJUGALES C'EST QUOI ?

Les violences conjugales prennent de **multiples formes** (violences psychologiques, verbales, physiques, sexuelles, administratives et économiques). Le numérique offre aux auteurs de violences conjugales des moyens faciles, accessibles et instantanés pour **davantage surveiller, contrôler et humilier les femmes**. Cela peut entraîner de **nouvelles formes de violences ou renforcer des violences déjà présentes** au sein du couple (notamment des violences psychologiques). Ces violences peuvent être perpétrées par le partenaire, l'ex partenaire (mariage/PACS), un concubin ou ex concubin, un compagnon ou ex compagnon, un petit ami ou ex, … L'expression « partenaire ou ex » sera utilisée dans ce document pour recouvrir toutes les situations.

DIFFERENTS TYPES DE CYBERVIOLENCES CONJUGALES

Une recherche-action menée par le Centre Hubertine Auclert en 2018 a montré que 9 femmes victimes de violences conjugales sur 10 déclarent avoir subi également des cyberviolences de la part de leur partenaire ou ex. Ces différents types de cyberviolences conjugales sont généralement cumulés et répétés. Vous trouverez ci-dessous des données extraites de cette recherche-action[2].

Il existe une **forte imbrication entre violences conjugales et cyberviolences**. Les cyberviolences commencent souvent en même temps que les autres formes de violences conjugales et durent jusqu'à la séparation ou après. Les cyberviolences peuvent également commencer et se renforcer au moment de la séparation lorsque l'agresseur cherche à maintenir le contrôle à distance, y compris à travers des communications avec les enfants ou leurs outils numériques.

2
Si vous souhaitez en savoir plus, vous pouvez consulter la synthèse et le rapport complet sur le site Internet du Centre Hubertine Auclert : https://www.centre-hubertine-auclert.fr/outil/rapport-cyberviolences-conjugales-2018 Vous pouvez également demander des rapports et synthèses sous format papier en écrivant à contact@hubertine.fr

LE CYBERCONTRÔLE

Définition

Comportements répétés du partenaire (ou ex) visant à connaître et vérifier régulièrement au moyen des outils numériques les déplacements et les relations sociales de sa partenaire (ou ex).

8 FEMMES SUR 10 déclarent que leur partenaire (ou ex) a exigé qu'elles soient **joignables en permanence**.

7 FEMMES SUR 10 déclarent qu'il leur a **interdit de communiquer** avec quelqu'un.

1 FEMME SUR 3 déclare qu'il a exigé qu'elle lui **envoie une photo pour prouver où elle se trouve**.

LA MOITIÉ DES FEMMES a déclaré qu'il lui a **confisqué son téléphone**.

93% DES FEMMES INTERROGÉES ont subi **au moins une forme de cybercontrôle** de la part de leur partenaire (ou ex).

LE CYBERHARCÈLEMENT

Définition

Utilisation des appels, SMS ou autres communications via les réseaux sociaux avec la volonté de faire du mal et qui par leur fréquence visent à envahir à distance le quotidien de sa partenaire (ou ex).

80% DES FEMMES déclarent avoir reçu de **manière répétée des insultes ou injures** via leur téléphone de la part de leur partenaire (ou ex).

LA MOITIÉ DES FEMMES a **déjà été menacée de mort** par son partenaire (ou ex).

82% DES RÉPONDANTES ont subi **au moins une fois des insultes ou du cyberharcèlement** de la part de leur partenaire (ou ex).

LA CYBERSURVEILLANCE

Définition

Ensemble d'agissements du partenaire (ou ex) qui visent à assurer un contrôle continu des déplacements, agissements et relations sociales au moyen des outils numériques.

Cybersurveillance « à l'insu » :

21% DES FEMMES déclarent avoir été surveillées à distance sans leur accord par leur partenaire (ou ex) via un logiciel espion.

Cybersurveillance « imposée » :

62% DES FEMMES déclarent que leur partenaire (ou ex) a exigé de connaître leurs codes (téléphone, réseaux sociaux, mails, compte bancaire…).

69% DES FEMMES pensent que leur partenaire (ou ex) a eu **accès à des informations** contenues dans leur téléphone, sans savoir comment il les a obtenues.

64% DES RÉPONDANTES ont subi **au moins une forme de cybersurveillance** de la part de leur partenaire (ou ex).

LES CYBERVIOLENCES ÉCONOMIQUES OU ADMINISTRATIVES

Définition

Comportements facilités par les outils numériques visant à réduire l'autonomie financière et/ou à contraindre les démarches notamment administratives de sa partenaire (ou ex).

35% DES FEMMES déclarent que leur partenaire (ou ex) **a changé les mots de passe** (compte bancaire, administratifs – Pôle Emploi, OFII, CAF – ou abonnements) en ligne pour y interdire l'accès ou pour un usage personnel.

31% DES FEMMES déclarent que leur partenaire (ou ex) **a utilisé des informations privées** obtenues sur son téléphone pour lui nuire, notamment dans une procédure judiciaire.

58% DES FEMMES déclarent avoir subit **au moins une forme** de cyberviolences économiques ou administratives.

LES CYBERVIOLENCES SEXUELLES

Définition

Utilisation de moyens technologiques pour filmer ou prendre des photos pendant un acte sexuel et menacer de les diffuser – ou mettre la menace à exécution – pendant la relation ou après la fin de celle-ci afin d'humilier.

1 FEMME SUR 3 déclare **avoir été menacée par son partenaire** (ou ex) de diffusion de contenus intimes.

15% DES FEMMES déclarent que leur partenaire (ou ex) **a exigé de filmer des pratiques sexuelles** sans leur accord.

16% DES FEMMES déclarent qu'il **a diffusé un contenu intime** sans leur accord.

34% DES FEMMES déclarent avoir subi **au moins une forme** de cyberviolences sexuelles.

LES CYBERVIOLENCES VIA LES ENFANTS

Définition

Prise de contact avec les enfants par l'ex partenaire pour continuer d'exercer un contrôle sur les actions et déplacements de sa partenaire (ex) et/ou pour la menacer.

34% DES FEMMES SÉPARÉES ayant des enfants à charge (58) déclarent avoir **subi des violences via les communications de leurs enfants**.

CONSÉQUENCES DES CYBERVIOLENCES CONJUGALES

Les conséquences des cyberviolences conjugales sont bien **réelles et multiples**. Pour 93% des répondantes les cyberviolences conjugales subies ont eu des conséquences : **sociales** (isolement), sur leur **santé mentale** (perte de confiance en soi, hypervigilance) ou sur leur **santé physique** (perte de sommeil, maux de ventre…). Ainsi, les victimes ont besoin d'un **accompagnement pluri-professionnel**.

2

LE RÔLE DES PROFESSIONNEL·LES

COMMENT AGIR POUR MIEUX REPÉRER, ACCOMPAGNER ET ORIENTER LES VICTIMES ?

POURQUOI PRENDRE EN COMPTE LES CYBERVIOLENCES ?

La prise en compte des cyberviolences dans l'accompagnement des victimes de violences conjugales est importante pour plusieurs raisons :

1/ Elle permet de **mieux repérer et caractériser l'ensemble des violences** subies par la victime.

Le fait de mieux caractériser les violences subies permet d'aider la victime à mieux constituer leur dossier et **renforcer les preuves** des violences subies. Les cyberviolences ont la particularité de laisser des traces : ce sont autant de preuves (par exemple, des captures d'écran) qui font souvent défaut dans les procédures pour violences conjugales (en particulier les violences psychologiques).

2/ Elle permet de **mieux évaluer la situation globale** de la femme, et notamment le danger encouru. En effet, le contexte des cyberviolences est un indicateur supplémentaire de l'emprise et du contrôle exercé par l'agresseur.

3/ Cela permet d'**adapter les conseils et stratégies de protection** en conséquence, en incluant le volet numérique.

Les conseils de protection numérique vont aider la victime à sécuriser ses outils et lutter contre le sentiment de la toute-puissance de l'agresseur.

COMMENT AGIR ?

ÉTAPE 1

Afficher dans votre salle d'attente et vos bureaux le poster joint à ce guide pour informer les victimes qu'elles peuvent parler aussi avec vous des cyberviolences.

Poser des questions ciblées à toutes les victimes pour repérer les cyberviolences, car elles n'en parlent pas spontanément et/ou elles les banalisent.

Vous utilisez la FICHE N°1 *« Repérer les cyberviolences conjugales ».*

ÉTAPE 2

Aider la victime à décrypter la stratégie de l'agresseur dans le numérique.

Vous utilisez la FICHE N°2 *« La stratégie de l'agresseur dans les cyberviolences ».*

ÉTAPE 3

Expliquer à la victime ses droits, la possibilité de porter plainte et comment rassembler les preuves des violences subies.

Vous utilisez :
FICHE N°3 *« Que dit la loi ? »*
FICHE N°4 *« Aider les victimes à faire valoir leurs droits et collecter des preuves »*

ÉTAPE 4

Apporter à la victime des conseils spécifiques sur la sécurité numérique et l'orienter vers des ressources pour se protéger des logiciels espions et d'autres dispositifs de surveillance.

Vous utilisez les FICHES N°5 À 8 *sur la protection numérique.*

LES FICHES PRATIQUES

OUTILS
D'AIDE AU REPÉRAGE

COMMENT AUTO-ÉVALUER LES CYBERVIOLENCES ?

Une relation de couple saine et égalitaire, dans laquelle je n'ai pas peur et je me sens en confiance, se traduit également par ce que mon partenaire (ou ex) se permet ou non de faire concernant mes informations personnelles sur mon téléphone, mon ordinateur et mes réseaux sociaux.

☑ **JE ME SENS EN SÉCURITÉ** DANS MON COUPLE ET JE N'AI PAS PEUR QUAND...	
/ Je peux communiquer librement par téléphone ou par mail et via les réseaux sociaux avec qui je veux et quand je veux, sans avoir à me justifier. / Il me fait confiance, et ne cherche pas à fouiller mon téléphone, à « tracer » mes déplacements, ni à vérifier avec qui je suis. / Il s'assure de mon accord pour tout enregistrement vidéo dans notre relation. / Il commente mes publications sur les réseaux sociaux de manière bienveillante.	Je vis une relation de couple SAINE, **y compris dans ma vie numérique**

⚠ **JE SUIS EN DANGER.** IL EST IMPORTANT QUE JE DEMANDE DE L'AIDE ET DES CONSEILS POUR ME PROTÉGER QUAND...	
/ Il exige que je sois joignable en permanence. / Il contrôle toutes mes publications sur les réseaux sociaux et celles de mes ami·es. / Il m'interdit de communiquer avec certaines personnes. / Il me confisque mon téléphone.	**Je suis VICTIME de cybercontrôle**
/ Il m'envoie des insultes et des injures par sms. / Il m'adresse des messages humiliants plusieurs fois par jour. / Il me menace de mort.	**Je suis VICTIME de cyberharcèlement**
/ Il exige de connaître mes mots de passe. / Il se connecte à mes comptes à mon insu. / Il a possiblement installé un logiciel espion sur mon téléphone.	**Je suis VICTIME de cybersurveillance**
/ Il menace de diffuser mes photos intimes à mon entourage. / Il exige de filmer nos relations sexuelles sans mon accord. / Il a partagé des images intimes de moi sur les réseaux sociaux.	**Je suis VICTIME de cyberviolences sexuelles**
/ Il s'est connecté à mes comptes bancaires et administratifs pour se faire verser mes allocations et mon argent ou pour modifier des informations personnelles. / Il a envoyé des mails administratifs en se passant pour moi. / Il a utilisé mes informations privées qu'il a volées sur mon ordinateur pour me nuire dans mes démarches administratives/judiciaires.	**Je suis VICTIME de cyberviolences économiques / administratives**
/ Il communique avec nos enfants pour savoir où et avec qui je suis. / Il surveille mes activités sur les réseaux sociaux à travers les comptes de nos enfants. / Il a possiblement installé un logiciel espion sur le téléphone ou la tablette des enfants.	**Je suis VICTIME de cyberviolences via mes enfants**

QUESTIONS COMPLÉMENTAIRES À POSER LORS DE L'ENTRETIEN

VIOLENCES PSYCHOLOGIQUES
Avez-vous déjà subi des insultes, injures, menaces, humiliations, chantages, etc. ?

LE CYBERCONTRÔLE
Votre partenaire ou ex :
- ☐ Vous a-t-il déjà contacté par SMS, appels ou via les réseaux sociaux de façon très insistante uniquement pour savoir où vous êtes / ce que vous faites / avec qui vous êtes ?
- ☐ Vous fait-il souvent des reproches quand vous n'êtes pas joignable en permanence par téléphone ou sur les réseaux sociaux et / ou quand vous ne répondez pas immédiatement ?
- ☐ A-t-il déjà exigé de lire vos sms, mails, de voir les appels passés ou reçus, de voir vos photos partagées, et/ou vos communications sur des réseaux sociaux (*Facebook,Twitter, Instagram, Snapchat, etc.*), messageries (*WhatsApp, Viber, etc*) alors que vous n'en aviez pas envie car c'est privé ?
- ☐ A-t-il déjà exigé de vous l'envoi de photo ou vidéo pour confirmer où vous êtes / ce que vous faites / avec qui vous êtes?
- ☐ Vous a-t-il déjà fait des reproches sur les appels que vous passez, sur vos messages ou publications sur les réseaux sociaux ?
- ☐ Vous a-t-il déjà empêché de répondre à un appel, d'envoyer un message depuis votre téléphone ou ordinateur, ou a-t-il exigé de supprimer des contacts?
- ☐ Vous a-t-il déjà confisqué votre téléphone, ordinateur ou tablette ?

LA CYBERSURVEILLANCE
Votre partenaire ou ex :
- ☐ Semble-t-il connaître vos déplacements et rendez-vous alors que vous ne lui en avez pas parlé ? (*et vous ne savez pas exactement comment il a pu faire cela*) ?
- ☐ Semble-t-il avoir accédé à votre téléphone, ou à votre boîte mail ou vos comptes de réseaux sociaux sans votre accord ? (*et vous ne savez pas exactement comment il a pu faire cela*) ?
- ☐ Vous a-t-il obligé à partager vos codes de votre boîte mail ou vos comptes de réseaux sociaux ?
- ☐ Vous a-t-il déjà surveillé avec des logiciels espions (*) installés sur votre téléphone ou via votre GPS (*téléphone, voiture*) ?

(*) un logiciel espion est un dispositif installé sur votre téléphone ou ordinateur sans que vous n'ayez donné l'accord par une autre personne et qui enregistre et transmets vos contacts, vos messages, vos appels

LE CYBERHARCÈLEMENT
Votre partenaire ou ex :
- ☐ Vous a-t-il envoyé plusieurs messages d'insultes ou d'injures par téléphone, par SMS ou via les réseaux sociaux ?
- ☐ Vous a-t-il déjà menacé de mort par téléphone, SMS ou via les réseaux sociaux ?

VIOLENCES SEXUELLES
Avez-vous déjà subi des rapports sexuels non consentis, pratiques sexuelles forcées, attouchements non consentis, etc ?

Votre partenaire ou ex :
- ☐ Vous a-t-il menacé de diffuser vos photos ou informations personnelles ou intimes (*par mail, par sms ou sur les réseaux sociaux*) sans votre accord ?
- ☐ A-t-il déjà diffusé vos photos ou informations personnelles ou intimes (*par mail, par SMS ou sur les réseaux sociaux*) à vos ami·es, collègues ou famille sans votre accord dans le but de vous nuire ?
- ☐ Vous a-t-il forcé à filmer des pratiques sexuelles alors que vous n'en aviez pas envie ?

VIOLENCES ÉCONOMIQUES ET ADMINISTRATIVES
Avez-vous déjà subi la privation d'accès aux ressources, vols de biens, contrôle des dépenses, etc. ?
Avez-vous déjà été empêchée de faire vos démarches administratives, votre conjoint a-t-il confisqué vos papiers, etc. ?

Votre partenaire ou ex :
- ☐ A-t-il déjà accédé à vos comptes bancaires ou administratifs (*CAF, Ameli, Pôle Emploi...*) ou à vos abonnements (*électricité, internet,...*) en ligne pour modifier vos informations personnelles ou pour les utiliser à son bénéfice (*exemple : achats, versement d'allocation sur son compte*) ?
- ☐ S'est-il déjà fait passer pour vous en envoyant des SMS depuis votre téléphone ; ou des mails depuis votre boîte mail personnelle ; ou en créant un faux compte à votre nom sur un réseau social pour vous nuire ?
- ☐ A-t-il déjà utilisé des informations privées obtenues en accédant à votre téléphone, ordinateur dans le but de vous nuire ou vous décrédibiliser (*par exemple dans une procédure auprès du juge aux affaires familiales*) ?

VIOLENCES VIA LES ENFANTS

Votre partenaire ou ex :
- ☐ A-t-il déjà pris des contacts avec vos enfants (*par téléphone, réseaux sociaux*) pour savoir où vous êtes/ ce que vous faites/ avec qui vous êtes ?

***Aborder le sujet de la cybersurveillance, notamment à travers des logiciels espions installés à l'insu de la victime**, peut paraître anxiogène pour elle et renforcer l'impression de la toute-puissance de l'agresseur. La victime peut se sentir démunie. Le rôle des professionnel·les est essentiel pour la rassurer, lui expliquer ses droits ainsi que des démarches pour renforcer sa sécurité numérique.*

FICHE N°2

LA STRATÉGIE DE L'AGRESSEUR DANS LES CYBERVIOLENCES CONJUGALES

La stratégie du partenaire ou ex violent - qui vise à isoler, dévaloriser, intimider la victime et garantir son impunité - **va être renforcée par le numérique.**

LA STRATÉGIE DU PARTENAIRE OU EX VIOLENT	LE NUMÉRIQUE RENFORCE CETTE STRATÉGIE	LES CONSÉQUENCES POUR LA VICTIME
INSTAURER UN CLIMAT DE PEUR ET D'INSÉCURITÉ	/ **Les outils numériques rendent possible un contrôle à distance en continu** et tout au long de la journée, à travers l'envoi de messages de menaces, d'appels incessants, l'exigence de joindre la victime à tout moment.	/ La victime peut avoir le sentiment que son partenaire ou ex est « tout puissant », qu'il sait tout et peut tout contrôler. / La victime n'a plus d'espace de répit, de liberté, elle a l'impression que l'agresseur contrôle toutes les sphères de sa vie (sa vie amicale, professionnelle, etc.).
ISOLER LA VICTIME	/ L'agresseur peut limiter ou interdire à la victime de téléphoner/écrire à ses ami·es et à sa famille. / L'agresseur peut utiliser les réseaux sociaux pour renforcer une bonne image de lui et **diffuser une image négative de la victime** pour l'isoler de son entourage et **renforcer son impunité** à lui.	/ En se trouvant isolée, la victime aura plus de difficultés à solliciter une aide externe. / Elle aura peur que le conjoint violent apprenne ses échanges. / L'isolement va rendre encore plus difficile pour la victime le fait de s'extraire de l'emprise qu'il exerce sur elle. / La victime aura peur de ne pas être crue, d'être considérée comme « paranoïaque » si elle parle du contrôle permanent de l'agresseur via des outils numériques.
HUMILIER, DÉVALORISER, LA TRAITER COMME UN OBJET	/ **Le numérique permet l'envoi de messages dégradants et humiliants** de manière continue à la victime. / **Le numérique permet la diffusion des images ou vidéos à caractère intime ou sexuel** dont la captation peut être imposée à la victime. La menace de la diffusion de ces images crée un chantage permanent qui renforce l'humiliation ressentie par la victime.	/ Le sentiment de honte, de culpabilité, d'humiliation (par exemple pour avoir donné son accord au moment de la production de ces images) vont réduire la capacité de la victime à solliciter une aide externe et vont renforcer l'emprise du conjoint violent.
INVERSER LA CULPABILITÉ	/ **Le cybercontrôle et la cybersurveillance** permettent de collecter des informations qui vont ensuite être utilisées pour des reproches sur les déplacements, agissements et relations sociales de la victime. / **Ces informations peuvent être collectées à l'insu de la victime** *(via une application de surveillance etc.)* ou exigées, notamment dans le cadre d'un chantage affectif *(par exemple : « si tu m'aimes, tu dois me donner accès à ton compte Facebook etc. »)*. L'agresseur va reprocher en permanence à la victime de chercher à lui cacher des choses, installant l'idée que c'est elle qui a un problème dans leur couple.	/ La victime a l'impression qu'elle est responsable des actes de violences qu'elle subit. Elle a peur de provoquer des violences à nouveau et elle a le sentiment d'être paralysée. / Elle ressent que le risque de représailles est élevé.
AGIR EN METTANT EN PLACE LES MOYENS D'INSTAURER L'IMPUNITÉ	/ L'agresseur peut avoir accès au téléphone de la victime, **effacer des données ou des preuves** pour garantir son impunité. **Il peut installer des dispositifs de surveillance à l'insu**, ou **obliger la victime à partager les informations privées**.	/ Dans le cadre de la surveillance à son insu, la victime a l'impression de ne pas pouvoir prouver le cybercontrôle exercé par son partenaire. / Dans le cadre de la surveillance imposée, quand la partenaire a été obligée de partager ses codes, elle est déstabilisée car elle a le sentiment de participer activement à sa mise sous surveillance. / Ainsi, la victime aura des difficultés à engager des démarches contre l'agresseur (par ex. porter plainte).

FICHE N°3

QUE DIT LA LOI FACE AUX CYBERVIOLENCES CONJUGALES ?

Le tableau suivant rassemble les textes applicables concernant les différentes formes de cyberviolences conjugales. Plusieurs textes du Code pénal sont mobilisables, et la loi a récemment été renforcée pour prendre en compte la spécificité des relations de couple (circonstance aggravante).

	EXEMPLES	TEXTES APPLICABLES	CIRCONSTANCES AGGRAVANTES SI CONJOINT (OU EX)
CYBERCONTRÔLE	(Exiger de) Lire les sms, mails personnels, de consulter l'historique d'appels…	Délit de violation du secret des correspondances (art. 226-15) : **1 an de prison et 45 000 € d'amende**	2 ans de prison et 60 000 € d'amende
	Confiscation du téléphone, ordinateur, tablette	Vol, y compris si commis par le conjoint (art. 311-12) : **3 ans de prison et 45 000 € d'amende**	Élément constitutif de l'infraction
	Être empêchée de répondre à un appel, d'envoyer un message	Harcèlement moral (art. 222-33-2-1) : **de 3 à 5 ans d'emprisonnement et de 45000 à 75000 € d'amende** dans le cadre du couple	Non, mais élément constitutif de l'infraction
	Exiger de savoir et de prouver où on se trouve, d'être joignable en permanence etc.	Harcèlement moral (art. 222-33-2-1) : **de 3 à 5 ans d'emprisonnement et de 45 000 à 75 000 € d'amende**	Non, mais élément constitutif de l'infraction
CYBERHARCÈLEMENT	SMS d'insultes ou humiliations	Délit d'envoi réitéré de messages ou d'appels malveillants (art. 222-16) : **1 an de prison et 15 000 € d'amende**	3 ans de prison et 45 000 € d'amende
		Voire harcèlement moral (art. 222-33-2-1) : **de 3 à 5 ans d'emprisonnement et de 45 000 à 75 000 € d'amende** dans le cadre du couple	Non, élément constitutif de l'infraction
	Si connotation sexuelle ou sexiste	Harcèlement sexuel (art. 222-33) : **3 ans et 45 000 € d'amende**	Oui
	SMS avec menaces de mort	Menaces de mort (art. 222-18-3) : **7 ans de prison et 100 000 € d'amende** dans le cadre du couple	Oui
CYBERSURVEILLANCE IMPOSÉE	Exiger de partager ses codes et mots de passe	Harcèlement moral (art. 222-33-2-1) : **de 3 à 5 ans d'emprisonnement et de 45 000 à 75 000 € d'amende** dans le cadre du couple	Non, élément constitutif de l'infraction
		En cas d'usage de mauvaise foi, aux fins d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues : délit de violation du secret des correspondances (art. 226-15) : **1 an de prison et 45 000 € d'amende**	2 ans de prison et 60 000 € d'amende

	EXEMPLE	TEXTES APPLICABLES	CIRCONSTANCES AGGRAVANTES SI CONJOINT (OU EX)
CYBERSURVEILLANCE À L'INSU	Mise en place de logiciels espions	Délit de géolocalisation en temps réel sans l'accord (art. 226-1-3) : **1 an de prison et 45 000 euros d'amende**	2 ans de prison et 60 000 € d'amende
		Délit de violation du secret des correspondances (art. 226-15) : **1 an de prison et 45 000 € d'amende**	2 ans de prison et 60 000 € d'amende
		Délit d'atteinte aux systèmes de traitement automatisé des données (art. 323-1 et 321-3) : **accès : 2 ans prison et 60 000 € d'amende et modifications : 5 ans et 150 000 € d'amende**	Non
CYBERVIOLENCES ÉCONOMIQUES OU ADMINISTRATIVES	Accéder aux comptes bancaires personnels en ligne (voire les modifier)	Délit d'atteinte aux systèmes de traitement automatisé des données (art. 323-1 et 321-3) : **accès : 2 ans prison et 60 000 euros d'amende et modifications : 5 ans et 150 000 euros d'amende**	Non
	Utiliser des données privées obtenues frauduleusement en ligne (par exemple pendant une procédure judiciaire)	Délit de collecte frauduleuse de données personnelles (art. 226-18) : **5 ans de prison et 300 000 €**	Non
	Se faire passer pour sa partenaire en ligne en vue de lui nuire socialement, professionnellement etc.	Délit d'usurpation d'identité (art. 226-4-1) : **1 an de prison et 15 000 € d'amende**	2 ans de prison et 30 000 € d'amende
CYBERVIOLENCES SEXUELLES	Conserver ou diffuser des images intimes sans consentement	Délit renforcé d'atteinte à la vie privée (art. 226-2-1) : **2 ans de prison et 60 000 € d'amende**	Non
	Menace de diffusion d'images intimes	Menace de commettre un délit (art. 222-17) : **2 ans de prison et 30 000 € d'amende**	Oui
	Être forcée à filmer des actes sexuels	Délit d'atteinte à la vie privée (art. 226-2-1) : **2 ans de prison et 60 000 € d'amende**	Non
		Viols (art. 222-23) : **20 ans de prison**	Oui
		Agressions sexuelles (art. 222-28) : **7 ans d'emprisonnement et 100 000 € d'amende**	Oui
CYBERVIOLENCES VIA LES ENFANTS	Communiquer avec l'enfant pour obtenir des informations privées sur sa mère, en cas de séparation	Délit d'envoi réitéré de messages ou d'appels malveillants (art. 222-16) : **1 an de prison et 15 000 € d'amende**	3 ans de prison et 45 000 € d'amende
	Mise en place d'un système de géolocalisation de l'enfant en temps réel, permettant d'avoir des informations sur sa mère en cas de séparation	Délit de géolocalisation en temps réel sans l'accord (art. 226-1-3) : **en cas d'enfant mineur·e, l'accord doit être donné par les titulaires de l'autorité parentale (art. 226-1-4).**	2 ans de prison et 60 000 € d'amende

Une première version de ce tableau a été réalisée avec l'appui du Bureau de la Politique Pénale Générale de la Direction des Affaires Criminelles et des Grâces du Ministère de la Justice en 2018. Mise à jour : août 2020.

Voir la dernière version à jour : https://centre-hubertine-auclert.fr/outil/fiche-juridique-que-dit-la-loi-face-aux-cyberviolences-conjugales

FICHE N°4

AIDER LES VICTIMES DES CYBERVIOLENCES CONJUGALES **À FAIRE VALOIR LEURS DROITS**

La plupart des cyberviolences conjugales correspondent à des délits.
Voir la FICHE N°3 : « Que dit la loi face aux cyberviolences conjugales »

Pour faire valoir ses droits, conseiller à la victime d'agir en 3 étapes :
1/ **Rassembler**
2/ **Conserver**
3/ **Faire constater les preuves de cyberviolences conjugales.**

1. RASSEMBLER LES PREUVES

QUELLES PREUVES CONSERVER EN CAS DE CYBERVIOLENCES CONJUGALES ?

Conserver le journal des appels téléphoniques (et/ou les relevés d'appels téléphoniques sur les factures), les messages vocaux, les SMS, les mails, les publications sur les réseaux sociaux, les relevés d'appels téléphoniques sur les factures, etc.

Conserver systématiquement et autant que possible les preuves car certains contenus peuvent être supprimés automatiquement au bout d'un certain temps, et/ou pourraient être supprimés aussi par l'agresseur. **Sauvegarder les messages d'origine ET réaliser des captures d'écran complètes** - avec date, heure, expéditeur, type de messagerie, et/ou lien URL du contenu (c'est-à-dire où il est hébergé s'il est en ligne). Pour les emails, il est important de conserver les originaux complets - avec le code source de l'en-tête (rechercher dans les paramètres « afficher l'original » ou « afficher la source du message »).

En matière pénale, il est aussi possible de produire des **enregistrements vocaux** car la preuve est libre (article 427 du Code de procédure pénale). Toutefois, produire un enregistrement « clandestin » ne doit pas conduire à se mettre en danger. Une personne qui réaliserait qu'elle est enregistrée à son insu pourrait en effet réagir de manière violente.

Points de vigilance sur les réponses des victimes par SMS :

/ Au cours d'une procédure, l'ensemble des conversations SMS pourrait être analysé par la justice. Aussi, inviter la victime dans la mesure du possible à **ne pas répondre, ou de manière la plus neutre possible** (« Laisse-moi tranquille »). Dans d'autres situations, il est préférable que la victime répète clairement qu'elle ne veut plus être contactée (le fait que l'agresseur continue à la relancer à plusieurs reprises peut constituer un harcèlement).

/ Si l'auteur est déjà sous le coup d'une interdiction d'entrer en contact (contrôle judiciaire, précédente condamnation, ordonnance de protection), inviter la victime à ne pas répondre et à déposer plainte.

QUELLES PREUVES CONSERVER EN CAS DE PIRATAGE DE COMPTES EN LIGNE, OU D'INSTALLATION DE LOGICIELS ESPIONS ?

/ Conseiller d'abord de collecter toutes les **preuves matérielles** : capture d'écran des anomalies (message d'erreur de la boîte mail) ou de la boîte de dialogue de l'anti-virus qui a détecté un logiciel malveillant. **Attention** : il peut être préférable de réaliser une photo de l'écran d'ordinateur et l'enregistrer via DIGIPOSTE (pour

éviter que la capture ne soit interceptée par l'agresseur, dans le cas où il aurait accès aux comptes).

Important : **en cas de détection de logiciel espion via un anti-virus, il est recommandé de le mettre en quarantaine*** à travers l'antivirus. Ensuite demander rapidement auprès des services de police une analyse forensique* du téléphone/ordinateur piraté, afin de collecter toutes les informations sur la date et source de l'installation.

/ Rassembler toutes les **informations** pour prouver que c'est bien l'(ex) partenaire violent qui en est l'auteur, et ainsi **contextualiser** le piratage avec d'autres formes de (cyber)violences conjugales qui peuvent être prouvées et dont l'auteur est identifiable. Par exemple, demander à la victime si son partenaire exige de savoir où elle se trouve et avec qui, et conserver des preuves de ce harcèlement par SMS. Des témoignages de proches[3], des certificats médicaux ou autres attestations de professionnel·les peuvent être ajoutés.

Important : les preuves peuvent aussi être collectées sur les téléphones des enfants. En cas de séparation en particulier, le partenaire violent peut conserver un pouvoir et un contrôle sur la victime via les communications avec leurs enfants, soit directement avec eux (en leur demandant des informations par SMS par exemple), soit à leur insu (remettre un smartphone à un enfant et procéder à sa géolocalisation, surveiller les communications des enfants via les réseaux sociaux).

2. CONSERVER CES PREUVES EN LIEU SÛR

Les preuves numériques pourront être jointes au moment d'un dépôt de plainte (ou transmises après). En attendant, les **stocker dans un lieu inaccessible au partenaire violent**. Le stockage peut être sur une clé USB ou un disque dur externe/cloud protégé par un mot de passe sûr et remis à un·e tiers de confiance, et/ou sur un dispositif en ligne comme DIGIPOSTE.

Il pourra être utile de conseiller à la victime de tenir un « **journal** » rassemblant l'ensemble des informations sur les cyberviolences (date, lieu, témoins, type de technologie utilisée, type de preuves) et de le conserver en lieu sûr : par exemple sur l'application Mémo de Vie.

3. ENCOURAGER À FAIRE CONSTATER CES CONTENUS LITIGIEUX PAR UN·E HUISSIER OU HUISSIÈRE DE JUSTICE

Ce sera utile dans le cadre d'une éventuelle procédure judiciaire. Il/elle pourra par exemple retranscrire les conversations SMS ou les mails.

BON À SAVOIR : l'aide juridictionnelle ou certaines assurances (habitation, voiture, banque) comprennent des clauses de protection juridique permettant la **prise en charge des frais importants d'huissier** (en plus des contrats de protection juridique en tant que tels).

Le dispositif *« 5000 actes gratuits pour les femmes victimes de violences »* est proposé par l'Association des femmes huissières de justice et la Fédération nationale Solidarité Femmes. Prendre contact avec la FNSF qui oriente vers un huissier de justice.

* Voir glossaire

3 Lien vers le formulaire de témoignage : https://www.service-public.fr/particuliers/vosdroits/R11307

Plus d'informations sur le site : www.stop-cybersexisme.com

FICHE N°5

CONSTRUIRE UNE STRATÉGIE DE PROTECTION NUMÉRIQUE

Le ou la professionnel·le doit pouvoir accompagner les femmes victimes de violences conjugales afin de construire une **stratégie de protection numérique adaptée** en fonction de la situation de violences, du profil numérique de l'agresseur et des habitudes numériques de la victime. Cette stratégie peut aussi évoluer dans le temps.

Cette stratégie doit être construite avec la femme victime et discutée régulièrement afin de pouvoir proposer des ajustements. Pour éviter de susciter trop d'anxiété, la discussion sur la stratégie peut faire l'objet d'une réflexion par étapes.

ATTENTION !
PENSER À SÉCURISER VOS COMMUNICATIONS AVEC LA VICTIME

- **Lors des entretiens dans vos locaux** : proposer par exemple de mettre le téléphone dans la pièce à côté et de désactiver la géolocalisation.
- **Identifier avec la victime les moyens de communication avec vous les plus « sûrs » (téléphone, mails).** En cas d'échanges par mail, il est recommandé à la victime de créer une adresse confidentielle avec un mot de passe fort et de limiter les documents envoyés.
- **Avant un 1er rendez-vous dans vos locaux :** des conseils de précaution peuvent déjà lui être proposés, tout en la rassurant.

ÉTAPE 1 :
ÉTABLIR AVEC LA VICTIME UN DIAGNOSTIC SUR SA SÉCURITÉ NUMÉRIQUE

QUESTIONS À POSER	POINTS DE VIGILANCE
1. ÉVALUER LE NIVEAU D'INTRUSION DU PARTENAIRE DANS LES OUTILS ET LES COMPTES NUMÉRIQUES DE LA VICTIME ☐ *Est-elle à l'aise avec le numérique ?* ☐ *A-t-elle configuré elle-même ses outils ?* ☐ *L'agresseur peut-il connaître ses mots de passe (tel, mail, comptes) ?* ☐ *A-t-il (eu) régulièrement accès à son téléphone ?* ☐ *Ont-ils un ordinateur ou un cloud partagé ?*	En cas de forte intrusion du partenaire (ou ex), ne pas changer immédiatement les habitudes numériques car cela peut éveiller les soupçons de l'agresseur *(ex : si elle change un mot de passe, une notification pourrait être envoyée à l'agresseur).* Si la victime maîtrise peu le numérique, il pourra lui être **proposé un appui pour renforcer sa confiance dans le numérique** *(ex : atelier Orange Solidarités, Voir Ressources complémentaires).*
2. ÉVALUER LE NIVEAU DE COMPÉTENCE NUMÉRIQUE DE L'AGRESSEUR : ☐ *Travaille-t-il dans le domaine de l'informatique ?* ☐ *A-t-il des proches qui sont spécialisés ?* ☐ *A-t-il un profil geek ?*	En cas de compétences numériques très élevées de l'agresseur, des **mesures de protection renforcées** seront à privilégier. **ATTENTION !** du fait de l'emprise et d'une possible dévalorisation de ses propres compétences numériques, la victime peut avoir une tendance à surévaluer les compétences de l'agresseur (impression de la toute-puissance).

3. ÉVALUER LES RISQUES DE GÉOLOCALISATION DE LA VICTIME : ☐ *La géolocalisation est-elle activée sur son téléphone/tablette ?* ☐ *Utilise-t-elle Google maps ?* ☐ *Publie-t-elle des photos qui peuvent l'identifier en ligne (ou quelqu'un d'autre) ?*	**Recommander d'avoir le réflexe de désactiver la géolocalisation** et/ou de régler les paramètres pour ne permettre la géolocalisation qu'avec une demande d'autorisation préalable. Attention cependant à la sécurité de la victime par rapport au partenaire violent (voir étape 2).
4. ÉVALUER LE SENTIMENT DE SURVEILLANCE : ☐ *A-t-elle le sentiment qu'il connait ses déplacements ?* ☐ *Qu'il la surveille à la maison ?* ☐ *A-t-elle le sentiment qu'il sait avec qui elle communique ?* ☐ *Qu'il est au courant de rdv ou d'informations, ou de ce qu'elle fait à la maison ?* ☐ *Ces informations sont disponibles en SMS ou mails ?* **ATTENTION !** Les dispositifs de surveillance sont aujourd'hui nombreux et facilement accessibles. Même si le récit des victimes paraît incroyable, il est important de prendre en compte leur instinct et leur sentiment de surveillance.	**Si OUI, vérifier le téléphone ou la tablette.** *Voir la Fiche n°8 « Se protéger des logiciels espions et d'autres dispositifs de surveillance »* **Faire un test** pour savoir si ce sont les déplacements en voiture qui sont connus, et vérifier dans ce cas la présence d'un dispositif de surveillance placé à l'insu, de type « tracker ». Faire de même en cas de sentiment de surveillance sur ce qu'elle fait à la maison.
5. ÉVALUER LE NIVEAU DE RISQUE DANS LES USAGES DES RÉSEAUX SOCIAUX ☐ *Quels réseaux sociaux utilise-t-elle ?* ☐ *Avec qui ?* ☐ *A quelle fréquence ?* ☐ *Poste-t-elle des photos ?* ☐ *Sur quels réseaux sociaux le partenaire est-il également impliqué/non impliqué ?*	Le retrait des réseaux sociaux peut être anxiogène et peu adapté pour certaines victimes car c'est un espace de soutien social important. En fonction de l'activité habituelle de la victime et de son agresseur sur les réseaux sociaux, **envisager des solutions adaptées** et à réévaluer régulièrement : / Stratégie ciblée sur le retrait de réseaux à haut risque (l'agresseur y est actif, contenus publics). / Stratégie de moindre visibilité (publier moins/pas de photos).
6. ÉVALUER LE NIVEAU D'INTRUSION VIA LES COMMUNICATIONS DES ENFANTS : ☐ *Leur père leur a-t-il donné un téléphone /tablette ?* ☐ *Les enfants sont-ils autonomes ou non dans les usages ?* ☐ *Fréquentent-ils des réseaux sociaux ?* **ATTENTION !** aux jouets qui peuvent circuler dans les deux domiciles (en cas de garde partagée) où des dispositifs de surveillance peuvent être insérés.	**Adopter des mesures de protection pour les outils** et usages numériques des enfants et bien expliquer aux adolescent·es les réglages de géolocalisation et confidentialité sur les réseaux sociaux notamment.

ÉTAPE 2 :
GARANTIR LA SÉCURITÉ DE LA VICTIME DANS LA STRATÉGIE DE PROTECTION NUMÉRIQUE

Lorsque les agresseurs utilisent la technologie pour exercer des violences, il est naturel de vouloir jeter ou changer des appareils ou de fermer des comptes en ligne pour stopper ces violences. Cependant, certains agresseurs peuvent intensifier leur contrôle et leur comportement dangereux s'ils sentent qu'ils perdent l'accès à la victime. Donc, avant de changer un mot de passe que l'agresseur semblait connaître, avant de retirer une caméra cachée ou un traceur GPS, **réfléchissez avec la victime à la façon dont l'agresseur peut réagir, et planifiez sa sécurité avec elle en fonction.**

CONSEIL N°1

ADOPTER LE DOUBLONNAGE DES APPAREILS ET DES COMPTES EN LIGNE

Il s'agit d'utiliser un appareil numérique plus sûr pour certaines interactions, mais de continuer également à utiliser l'autre appareil même s'il est (ou risque d'être) surveillé par l'agresseur. Cela peut limiter la surveillance et le contrôle à distance, sans pour autant éveiller les soupçons de l'agresseur, y compris si la victime cohabite avec lui.

Cette solution peut être transitoire : une fois en sécurité, les femmes pourront utiliser à nouveau un seul téléphone. L'ancien téléphone pourra cependant être utile après la séparation pour suivre les échanges relatifs aux enfants si besoin.

Avoir un nouveau téléphone personnel :

/ Se procurer un téléphone basique non connecté à internet (limitant ainsi toute surveillance en cas de danger immédiat et/ou si l'agresseur est un « geek »). Si la victime souhaite maintenir un téléphone connecté, privilégier un abonnement simple pour éviter un surcoût.
/ La victime devra prévenir ses nouveaux contacts de l'importance de ne pas divulguer ce nouveau numéro à l'agresseur.
/ **Paramétrer ce téléphone** pour assurer une meilleure sécurité.

Voir la Fiche n°6 « Créer un nouvel univers sécurisé sur un téléphone /une tablette »

/ Réfléchir avec la victime à la meilleure manière de cacher ce téléphone dans un lieu sûr, et penser à le mettre en mode silencieux.

Conserver l'ancien téléphone pour les communications avec le partenaire violent :

/ Pour éviter la surveillance à distance sans supprimer la géolocalisation qui peut être imposée par l'agresseur, la victime pourra **diminuer ses déplacements avec ce téléphone** : ne prendre ce téléphone que pour les déplacements qui n'éveilleront pas les soupçons de l'agresseur, et conserver le téléphone au domicile (ou au travail) lors des démarches d'aide par exemple.
/ Pour éviter l'espionnage à distance, **ne pas consulter les applications de messagerie et les réseaux sociaux via ce téléphone**, et désinstaller ces applications sur son téléphone si cela ne risque pas d'alerter l'agresseur.
/ Consulter ce téléphone le moins possible.

Adapter ces stratégies pour l'ensemble des appareils numériques :

/ Pour éviter la surveillance via l'ordinateur familial, utiliser des ordinateurs publics (à la bibliothèque par exemple). Privilégier dans ce cas la navigation en mode « privée ».

Créer de nouveaux comptes en ligne qui ne seront pas accessibles à l'agresseur :

/ Ce afin de limiter l'accès de l'agresseur aux informations privées et confidentielles, notamment concernant les démarches d'aide en cas de préparation de départ.
/ Créer une nouvelle adresse email et limiter les interactions sur l'ancienne, plutôt que de changer de mot de passe d'un ancien compte ce qui pourrait alerter l'agresseur.

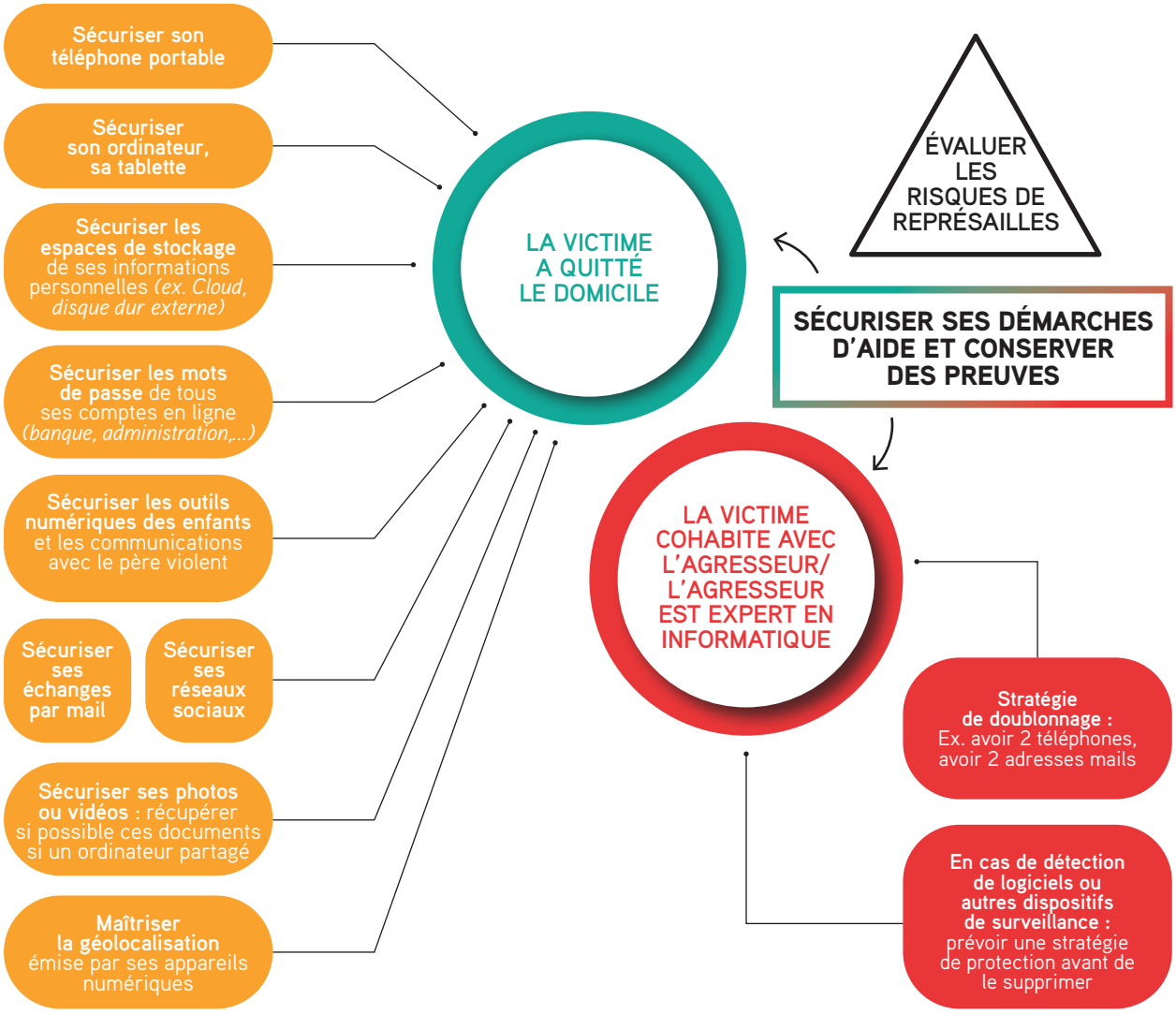
CONSEIL N°2

NE PAS RETIRER IMMÉDIATEMENT UN LOGICIEL ESPION OU TOUT AUTRE DISPOSITIF DE SURVEILLANCE UNE FOIS DÉTECTÉ PAR LA VICTIME

/ L'agresseur recevrait une notification et cela pourrait mettre en danger la victime.
/ Développer la stratégie de **doublonnage des appareils**, pour limiter la surveillance à partir de l'appareil espionné.
/ Le logiciel espion ne sera retiré qu'une fois la victime en sécurité, et après avoir conservé des preuves du piratage ou de l'espionnage.

Voir la Fiche n°4 « Aider les victimes à faire valoir leurs droits »

ÉTAPE 3 :
ADOPTER UNE STRATÉGIE DE PROTECTION NUMÉRIQUE GLOBALE



Voir des conseils plus détaillés dans les fiches suivantes :
Fiche n°6 « Sécuriser son téléphone »
Fiche n°7 « Sécuriser son ordinateur /une tablette »
Fiche n°8 « Se protéger des logiciels espions »

Voir plus d'information sur les différentes démarches sur le site : www.guide-protection-numerique.com

FICHE N°6

SÉCURISER
SON TÉLÉPHONE/SA TABLETTE

Cette fiche donne un aperçu des principales étapes de sécurisation d'un téléphone portable smartphone[4]. Pour des conseils plus détaillés sur **comment réaliser ces manipulations techniques** sur un appareil en autonomie, vous pouvez consulter la page « *Je suis victime de cyberviolences* » du site « *Je protège ma vie privée en ligne* » **www.guide-protection-numerique.com**

ATTENTION !

Si des modifications sont apportées au téléphone surveillé, l'agresseur peut en être averti par des notifications ou par l'impossibilité d'accéder à certaines informations. Il est important de faire ces paramétrages en ayant réfléchi en amont à sa sécurité, ou de les faire sur un appareil auquel l'agresseur n'a pas accès.

Toutes ces actions de sécurisation doivent aussi être réalisées sur les appareils de vos enfants en leur expliquant la nécessité de cette démarche.

FOCUS

La réinitialisation du téléphone

/ Pour les appareils avec le système d'exploitation **Android**, choisir dans « Réglages ou Paramètres » la fonction « Rétablir la configuration d'usine ».

/ Pour les appareils **Apple,** il est nécessaire de connecter le téléphone à l'ordinateur et d'activer, à travers le panneau de configuration, la fonction « restaurer les réglages par défaut ».

SÉCURISER UN TÉLÉPHONE EN 6 ÉTAPES :

1. SE PROCURER UN NOUVEAU TÉLÉPHONE OU RÉINITIALISER UN ANCIEN TÉLÉPHONE

Il est possible de réinitialiser* un ancien téléphone pour le sécuriser. On parle aussi de le remettre aux paramètres d'usine. Réinitialiser permet de supprimer les logiciels espions et d'autres applications de surveillance (voir le focus).

Cependant les données personnelles, contacts, SMS, photos et toutes les applications installées seront supprimées. En amont, il est primordial de **faire des sauvegardes des informations personnelles et des preuves des violences**.
Voir la Fiche n°4 « Aider les victimes à faire valoir leurs droits »

2. CRÉER UNE NOUVELLE ADRESSE MAIL QUI SERA RELIÉE AU NOUVEAU TÉLÉPHONE *(OU TÉLÉPHONE RÉINITIALISÉ)*

Pour qu'un smartphone fonctionne, il doit être **associé à un compte avec une adresse mail**. Cette adresse doit être **inconnue de l'agresseur et protégée par un mot de passe fort avec une authentification à deux niveaux*.**

3. SÉCURISER LE CLOUD RELIÉ AU TÉLÉPHONE

/ **Créer un nouveau compte Cloud*** (*Google Drive* ou *ICloud* par ex.) sécurisé par un mot de passe fort et une authentification à deux niveaux* et associé à la nouvelle adresse mail.

/ **Sauvegarder les données uniquement sur ce nouveau compte Cloud**.

/ **Paramétrer et limiter** les informations qui seront **automatiquement sauvegardées** dans le Cloud.

/ **Supprimer la synchronisation** de ce nouveau compte Cloud avec d'autres appareils.

4
Ces conseils sont également valables pour une tablette avec un système d'exploitation Android ou Apple.

*
Signifie le renvoi au glossaire pour la définition des termes.

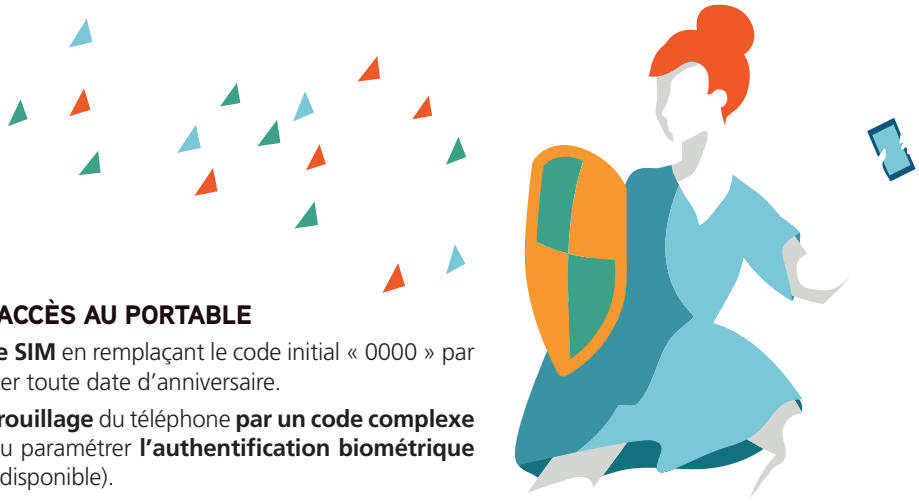
FOCUS

Renforcer les mots de passe du Cloud, de la boîte mail et des autres comptes

/ Pour chaque compte, choisir des **mots de passe différents, longs et robustes** (avec au moins une majuscule, un chiffre et une ponctuation, voire une phrase entière).

/ Utiliser un **logiciel gestionnaire des mots de passe** pour créer des mots de passe complexes et les sauvegarder sur un site sécurisé (ex : Bitwarden, Keepass). Il est également possible de noter les mots de passe sur une liste, ensuite la scanner et la sauvegarder dans un espace numérique sécurisé avec l'application Digiposte. Penser à supprimer la liste papier ensuite.

/ Activer si possible l'**authentification à deux facteurs***. C'est un mode de protection supplémentaire : en plus du mot de passe, un code d'accès sera demandé et envoyé sur le portable de la personne qui détient le compte (ex : Google Authenticator).



4. SÉCURISER LES CODES D'ACCÈS AU PORTABLE

/ **Renforcer le code de la carte SIM** en remplaçant le code initial « 0000 » par un code difficile à deviner. Eviter toute date d'anniversaire.

/ **Paramétrer un mode de verrouillage** du téléphone **par un code complexe différent de la carte SIM**, ou paramétrer **l'authentification biométrique par empreintes digitales** (si disponible).

/ Activer le **verrouillage automatique de la session** après une courte période d'inactivité (idéalement 30 secondes ou 1 minute). Ne pas laisser le téléphone sans surveillance.

5. LIMITER L'ACCÈS À LA GÉOLOCALISATION* :

/ **Désactiver le bouton de géolocalisation* (ainsi que le Wi-FI* et le Bluetooth*)** dans le panneau de commande du téléphone dès que vous n'en avez plus l'utilité.

/ **Paramétrer les autorisations d'accès** à la géolocalisation par des applications sur le téléphone et les **vérifier régulièrement**.

/ **Paramétrer le compte Google pour désactiver l'enregistrement de la localisation et l'historique des positions** (via *Googlemaps*, par exemple).

* Signifie le renvoi au glossaire pour la définition des termes.

6. SÉCURISER LA NAVIGATION SUR INTERNET À PARTIR DU TÉLÉPHONE

/ **Installer un anti-virus** qui permet la détection des logiciels espions comme *Kaspersky, Avast, ZoneAlarm*, et faire régulièrement des mises à jour sur le téléphone.

/ **Régler les paramètres de confidentialité** de manière restrictive de tous les comptes et réseaux sociaux pour mieux protéger les informations personnelles.

/ **Utiliser la « navigation privée »** lors de la navigation sur internet, qui n'enregistre pas la liste des sites consultés.

/ **Supprimer** régulièrement **les historiques de navigation.**

/ **Se déconnecter de tous les comptes après usage.**

FICHE N°7

SÉCURISER
SON ORDINATEUR

Cette fiche donne un aperçu des principales étapes de sécurisation d'un ordinateur. Pour des conseils plus détaillés, vous pouvez consulter la page « *Je suis victime de cyberviolences* » du site « *Je protège ma vie privée en ligne* » **www.guide-protection-numerique.com**

ATTENTION !

Toutes ces actions de sécurisation doivent aussi être réalisées sur les appareils de vos enfants en leur expliquant la nécessité de cette démarche.

SÉCURISER UN ORDINATEUR EN 5 ÉTAPES :

Ces conseils visent la sécurisation d'un ordinateur portable personnel.
Si un ordinateur a été partagé avec l'(ex)conjoint, il est important, si possible, de supprimer les informations privées qui y figurent, désactiver la synchronisation des comptes personnels avec cet appareil et changer les mots de passe des comptes personnels consultés sur cet ordinateur.

1. PROTÉGER L'ACCÈS À L'ORDINATEUR PAR MOT DE PASSE FORT

- **Créer un mot de passe robuste** pour protéger l'accès à l'ordinateur lors de son ouverture.
- Activer le **verrouillage automatique de la session** après une courte période d'inactivité.

2. PROTÉGER LES FICHIERS

- **Ajouter un mot de passe** pour accéder à chacun des fichiers.
- **Crypter*** **les fichiers** contenant des données personnelles.

3. SAUVEGARDER LES DONNÉES DANS UN LIEU SÛR

- Sauvegarder régulièrement les données personnelles sur un **disque dur externe** protégé par un mot de passe fort.
- **Stocker les données personnelles dans un Cloud*** (espace de stockage numérique virtuel, comme *Google Drive* etc.) sécurisé par un mot de passe robuste.

* Signifie le renvoi au glossaire pour la définition des termes.

4. SE PROTÉGER DES LOGICIELS ESPIONS

- **Installer des anti-virus gratuits** comme *Kaspersky* ou *ZoneAlarm* pour détecter et supprimer des logiciels espions. Activer des mises à jour des anti-virus régulièrement et lancer le scan de l'ordinateur périodiquement.
- Faire régulièrement des **mises à jour de l'ordinateur** et des programmes installés.
- Ne pas télécharger ni installer de logiciels provenant de **liens présents dans des emails**.

Voir la Fiche n°8 « Se protéger des logiciels espions et d'autres dispositifs de surveillance ».

5. SÉCURISER SA NAVIGATION INTERNET

- **Régler les paramètres de confidentialité** de manière restrictive de tous les comptes et réseaux sociaux pour mieux protéger les informations personnelles.
- **Utiliser la « navigation privée »** lors de la navigation sur internet, qui n'enregistre pas la liste des sites consultés.
- **Supprimer** régulièrement **les historiques de navigation**. Ne pas sauvegarder ses mots de passe dans son navigateur.
- **Se déconnecter de tous les comptes après usage**.
- Se connecter aux services en ligne (Google, Twitter, Facebook, etc) et **vérifier la liste des « appareils connectés » à ces comptes**.
- **Occulter la caméra** de l'ordinateur après chaque usage pour éviter toute surveillance.

FOCUS

Renforcer les mots de passe de la boîte mail et des autres comptes

- Pour chaque compte, choisir des **mots de passe différents, longs et robustes** (avec au moins une majuscule, un chiffre et une ponctuation, voire une phrase entière).
- Utiliser un logiciel **gestionnaire des mots de passe** pour créer des mots de passe complexes et les sauvegarder sur un site sécurisé (ex : Bitwarden, Keepass).

  Il est également possible de noter les mots de passe sur une liste, ensuite la scanner et la sauvegarder dans un espace numérique sécurisé avec l'application Digiposte. Penser à supprimer la liste papier ensuite.
- Activer si possible **l'authentification à deux facteurs***. C'est un mode de protection supplémentaire : en plus du mot de passe, un code d'accès sera demandé et envoyé sur le portable de la personne qui détient le compte (ex : Google Authenticator).

FICHE N°8

SE PROTÉGER
DES LOGICIELS ESPIONS ET D'AUTRES DISPOSITIFS DE SURVEILLANCE

Cette fiche donne quelques conseils de protection. Pour des conseils plus détaillés, vous pouvez consulter la page « *Je suis victime de cyberviolences* » du site « *Je protège ma vie privée en ligne* » **www.guide-protection-numerique.com**

ATTENTION !

Toutes ces actions de sécurisation doivent aussi être réalisées sur les appareils de vos enfants en leur expliquant la nécessité de cette démarche.

LES DIFFÉRENTS TYPES DE LOGICIELS ET DISPOSITIFS DE SURVEILLANCE :

Les logiciels espions et autres dispositifs de surveillance permettent de surveiller à distance les activités, les communications et les déplacements d'une personne : appels, messages, photos, vidéos, localisation, utilisation des applications, etc.

Les logiciels espions

Les logiciels espions installés sur un téléphone ou un ordinateur sont difficilement détectables. Les logiciels les plus utilisés sont *Cerberus, Hoverwatch, Mobile Tracker, mSpy, Snoopza, Spyzie*. Leur installation à l'insu les rend illégaux, maisils peuvent être facilement achetés en ligne. **Pour les installer l'agresseur a besoin d'avoir accès au téléphone de la victime, soit directement, soit via le compte Cloud* relié à ce téléphone.**

Les applications de surveillance

- **Les applications de surveillance légales, comme celles de surveillance parentale** *(FamilySafe, SafeKid)* peuvent être utilisées pour surveiller la victime. Il est facile de les repérer sur son téléphone car l'icône de l'application va apparaître dans la liste des applications installées.
- **Plusieurs applications préinstallées sur les téléphones** (*Google Maps*, ou les applications pour retrouver son appareil en cas de perte/vol comme l'application « Localiser mon téléphone ») peuvent être activées à distance et transmettre des données sur les déplacements.

La surveillance via le compte Cloud

Il est possible d'accéder aux informations personnelles via **le compte Cloud*** (contacts, communications, photos), en connaissant ou en devinant le mot de passe.

Les objets de surveillance

Il peut s'agir d'un **tracker GPS*** installé sur une voiture, de **caméras** installées à la maison et gérées à distance, ou d'**objets** qui permettent un **enregistrement audio** (intégrés de manière cachée dans les peluches des enfants par exemple). L'agresseur peut aussi utiliser les **webcams** des ordinateurs, des **assistants personnels** (tels que *Google Home* ou *Alexa*) ou des systèmes de sécurité de la maison gérés à distance.

1. SE PROTÈGER DES LOGICIELS ESPIONS

Signaux d'alerte

/ L'(ex)conjoint connaît des informations qu'il n'est pas censé connaître ?

/ Le téléphone chauffe, est plus lent que d'habitude, sa batterie tient beaucoup moins bien et la mémoire est saturée ?

/ La géolocalisation et le Wifi s'activent régulièrement malgré la désactivation ?

/ Des applications inconnues sont présentes sur le portable ?

/ Les applications Cydia (Apple), F-Droid (Android) ou SuperSU, qui permettent de télécharger certains logiciels espions, ont été installées sur le portable à l'insu ?

Pour se protéger de l'installation d'un logiciel espion

/ **Protéger le compte Cloud*** associé au téléphone/ordinateur par un mot de passe fort et l'authentification à deux facteurs* ;

/ Toujours **avoir le téléphone physiquement avec soi** (y compris salle de bains / toilettes).

/ Renforcez les **codes d'accès** au téléphone/ordinateur.

/ Faire des **mises à jour régulières** pour mieux protéger les appareils.

/ **Ne pas ouvrir les liens suspects envoyés** par mail, SMS ou sur les réseaux sociaux.

Repérer et supprimer un logiciel espion

/ **Installer un anti-virus** pour ordinateur et/ou téléphone (*Kaspersky, ZoneAlarm*) qui détecte la plupart des logiciels espions, et **réaliser régulièrement des scans et vérifications**.

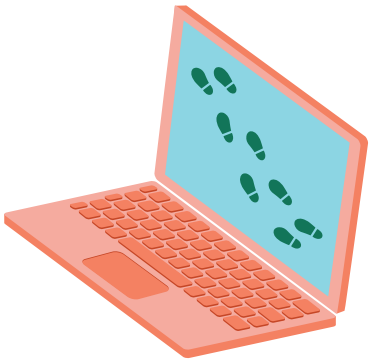
Attention ! Le système d'exploitation Apple ne permet pas l'installation d'un antivirus. Pour détecter un logiciel espion sur un appareil Apple, référez-vous aux signaux d'alerte ci-dessus.

/ **Si un logiciel espion est détecté sur l'appareil, attention à la suppression immédiate** car l'agresseur pourrait en être averti par des notifications ou par l'impossibilité d'accéder aux informations. Il est important de réfléchir à une **stratégie de protection** en amont.

/ **Si un logiciel espion est détecté** sur l'appareil par un anti-virus, en vue des démarches judiciaires : faire une **capture d'écran de sa détection** par l'anti-virus, **puis mettre le logiciel espion en quarantaine*** par l'anti-virus, ce qui l'empêchera de fonctionner.

Voir la Fiche n°4 « Aider les victimes à faire valoir leurs droits »

* Signifie le renvoi au glossaire pour la définition des termes.



/ **Pour vérifier que le logiciel espion a été bien supprimé**, il est recommandé de relancer une nouvelle vérification par l'anti-virus. En cas de doute, il est possible de **réinitialiser*** **le téléphone et l'ordinateur**. Cela supprimera toutes les données et applications installées, y compris les logiciels espions. Il est important de penser à sauvegarder les données personnelles en amont.

Voir la Fiche n°6 « Sécuriser son téléphone » et la Fiche n°7 « Sécuriser son ordinateur ».

2. SE PROTÉGER DES APPLICATIONS DE SURVEILLANCE :

/ **Désactiver le bouton de géolocalisation* (ainsi que le Wi-FI* et le Bluetooth*)** dans le panneau de commande du téléphone.

/ **Paramétrer les autorisations d'accès** à la géolocalisation par des applications sur le téléphone et les **vérifier régulièrement**.

/ **Paramétrer le compte Google pour désactiver l'enregistrement de la localisation et l'historique des positions** (via *Googlemaps* par exemple).

/ Désactiver la **fonction « localiser mon portable » en cas de perte ou vol**.

3. PROTÉGER SON COMPTE CLOUD :

Protéger le compte Cloud associé au téléphone/ordinateur par un mot de passe fort et l'authentification à deux facteurs*.

4. SE PROTÉGER DES OBJETS DE SURVEILLANCE :

/ Recouvrir d'un morceau de ruban amovible les **caméras intégrées** sur l'ordinateur/la tablette.

/ **Désactiver des assistants personnels** (tels que *Google Home* ou *Alexa*) dès que vous n'en avez plus l'utilité.

/ **Inspecter régulièrement la voiture** pour essayer de détecter un tracker qui pourrait y être installé.

/ **Inspecter régulièrement les jouets des enfants** (peluches etc.), notamment quand ils retournent au domicile de leur père en cas de garde partagée.

/ Certains logiciels peuvent aider à détecter une **caméra gérée à distance** installée au domicile de la victime. Voir le site : www.guide-protection-numerique.com

* Signifie le renvoi au glossaire pour la définition des termes.

GLOSSAIRE

GLOSSAIRE

Certains termes techniques présentés avec une (*) dans ce guide sont ici explicités.
Pour plus d'informations, consulter le site **www.guide-protection-numerique.com**

/ Analyse forensique
Signifie l'**analyse d'un système informatique après incident**. Une analyse forensique peut être effectuée après une attaque de virus ou de logiciel espion. Elle permet de comprendre le procédé utilisé pour cette attaque. Elle est utile dans le cadre d'une plainte si un logiciel espion a été détecté sur un téléphone par exemple.

/ Authentification à deux facteurs (A2F)
L'authentification à deux facteurs (A2F) permet un **haut niveau de protection des comptes en ligne**. En plus du mot de passe, un code d'accès est demandé et envoyé sur le portable de la personne qui détient le compte.

/ Bluetooth
Technique qui permet la **communication sans fil** entre divers appareils et l'échange de données à très courte distance en utilisant des ondes radio.

/ Cloud
Système de stockage des données sur internet, évitant d'avoir des données stockées sur l'appareil. Il en existe plusieurs : *Dropbox, Google Drive, Skydrive, Amazon Cloud Drive, iCloud...* Un seul mot de passe permet d'accéder aux nombreuses données personnelles qui y sont stockées (mails, photos, documents).

/ Cryptage des données
Le cryptage (ou chiffrement) est une méthode qui consiste à **protéger ses documents en les rendant illisibles** par toute personne n'ayant pas accès à une clé dite de déchiffrement. La CNIL propose un tutoriel.

/ Débrider *(jailbreaker)*
Le système d'exploitation *Apple* ou *Android* préinstallé sur un smartphone offre une protection à l'appareil. Le fait de débrider (ou jailbreaker) un téléphone consiste à **supprimer les protections mises en place par le système d'exploitation**. Cela permet par exemple d'installer des applications intrusives comme des logiciels espions.

/ Géolocalisation
Technologie permettant de déterminer la **localisation d'un objet ou d'une personne** avec une certaine précision. La technologie s'appuie sur le système GPS ou sur les interfaces de communication d'un téléphone mobile.

Certaines applications permettent à leurs utilisateurs de partager leur localisation. C'est le cas de *Google Maps*, qui dispose d'une option « partage de position », à durée déterminée.

Ces positions sont enregistrées et peuvent être accessibles via un logiciel espion, ou via l'historique d'un compte mail si les mots de passe sont connus. Cela permet ainsi l'espionnage des déplacements d'une personne.

/ Logiciel espion, ou de surveillance, ou mouchard
Logiciel malveillant installé dans un ordinateur ou appareil mobile à l'insu, dans le but de **transférer des informations vers l'environnement de la personne qui a installé le mouchard**. Certains logiciels de surveillance utilisés dans le cadre d'un contrôle parental peuvent être détournés pour espionner.

/ Mettre un logiciel espion en quarantaine
Quand un anti-virus détecte un logiciel espion, il propose de le supprimer ou de le mettre en quarantaine. La mise en quarantaine signifie que les **fonctionnalités d'un logiciel espion sont désactivées** mais qu'il n'est pas supprimé de l'appareil. Cela peut permettre de faire une analyse forensique* de ce logiciel espion pour comprendre comment il a été installé.

/ Réinitialiser
Manipulation du téléphone/tablette/ordinateur qui permet d'**effacer toutes les données** et donc de supprimer tout logiciel malveillant. On parle aussi de restaurer les paramètres d'usine.

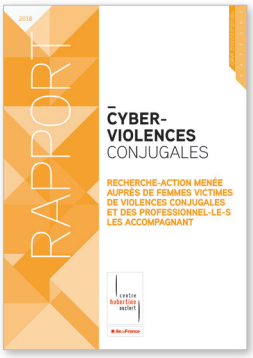
/ Réseaux sociaux
Applications en ligne qui permettent de partager des informations, photos et documents en créant un compte. Ex : *Facebook, Instagram, Messenger, WhatsApp, Snapchat, Skype, Telegram, TikTok.*

/ Tracker ou traceur GPS
Petit boîtier composé d'un récepteur GPS et d'un émetteur GSM. Il reçoit des **informations de localisation d'une personne** et les transmet grâce à la connexion GSM. Il peut être placé à l'insu dans une voiture ou sur des objets du quotidien (porte-manteau, jouets...).

/ Wi-Fi
Technologie de **connexion sans fil** à Internet, qui permet également la communication sans fil entre divers appareils.

RESSOURCES COMPLÉMENTAIRES

RESSOURCES COMPLÉMENTAIRES



#stopcybersexisme

JE PROTÈGE
MA VIE PRIVÉE
EN LIGNE

LES RESSOURCES DU CENTRE HUBERTINE AUCLERT

/ **Recherche-action sur les cyberviolences conjugales :**
La première étude statistique en France sur les cyberviolences conjugales menée par le Centre Hubertine Auclert. Elle vise à mesurer l'ampleur des cyberviolences dans le contexte des violences conjugales, à les caractériser et à identifier les modalités d'accompagnement des professionnel·les.
www.centre-hubertine-auclert.fr/outil/rapport-cyberviolences-conjugales-2018

/ **www.stop-cybersexisme.com :**
Un site d'information sur les cyberviolences sexistes et sexuelles, pour les décrypter, se protéger et agir en prévention.

/ **www.guide-protection-numerique.com :**
Un site-guide avec des conseils techniques pour protéger ses appareils, et avec des conseils spécifiques pour les victimes de cyberviolences conjugales.

/ **www.centre-hubertine-auclert.fr :**
Le site du Centre Hubertine Auclert avec toutes les informations sur les publications et activités du Centre et de l'Observatoire régional des violences faites aux femmes.

POUR UN CONSEIL SUR LES DÉMARCHES FACE AUX CYBERVIOLENCES CONJUGALES

/ Le tchat de l'association ***En avant toute(s)*** sur les violences dans les relations intimes est animé de manière anonyme et gratuite par des professionnelles. Elles apportent écoute et conseils spécialisés sur les cyberviolences pour les victimes et les professionnel·les.
www.commentonsaime.fr

POUR SE RENFORCER SUR LE NUMÉRIQUE

/ ***Echap*** est une association et un collectif de hackeuses féministes qui lutte contre l'utilisation de la technologie dans les violences faites aux femmes. L'objectif est d'accompagner sur les questions de technologie les associations luttant contre les violences faites aux femmes. L'association propose des ressources et des guides sur son site. Elle vise également à proposer l'animation d'ateliers autour de ce sujet.
www.echap.eu.org ; contact@echap.eu.org

/ **L'association *ARCA-F***, spécialisée dans l'auto-défense numérique, et **la coopérative La Boussole**, spécialisée dans la vulgarisation des connaissances numériques, proposent des formations spécialisées sur la sécurité numérique pour les associations qui accompagnent les femmes victimes de violences.
www.assoarcaf.wordpress.com
www.laboussole.coop

/ ***Orange Solidarité***, l'association du numérique solidaire de la Fondation Orange assiste les associations dans leur digitalisation. La structure propose des ateliers spécialisés sur le numérique aux associations qui accompagnent les femmes victimes de violences.
www.fondationorange.com/Orange-Solidarite

DES INFORMATIONS SUR LES LOGICIELS ESPIONS

/ **La Coalition internationale contre les logiciels espions** regroupe des associations d'aide aux victimes et des entreprises spécialisées sur la sécurité numérique. Elle propose des ressources en ligne qui aident à mieux comprendre le fonctionnement des logiciels espions et comment s'en protéger.
www.stopstalkerware.org

La recherche-action Cyberviolences conjugales : recherche-action menée auprès de femmes victimes de violences conjugales et des professionnel·les les accompagnant conduite en 2017-2018 par le Centre Hubertine Auclert permet de mesurer et de mieux comprendre les cyberviolences subies par les femmes victimes de violences conjugales de la part de leur partenaire (ou ex) : https://www.centre-hubertine-auclert.fr/outil/rapport-cyberviolences-conjugales-2018

Le site https://www.stop-cybersexisme.com du Centre Hubertine Auclert comporte des informations qui aident à comprendre les cyberviolences sexistes et sexuelles, y compris au sein du couple, et expliquent des démarches de protection que les victimes peuvent engager.

Ce guide a été réalisé par l'Observatoire régional des violences faites aux femmes du Centre Hubertine Auclert avec l'appui de plusieurs professionnelles d'associations spécialisées dans l'accompagnement des femmes victimes de violences conjugales. Nous les remercions pour leur contribution :

/ Union régionale Solidarité Femmes
/ En Avant Toute(s)
/ SOS Femmes 93
/ Paroles de Femmes - Le Relais
/ CIDFF 92 Nord Nanterre
/ Fondation des Femmes

D'autres partenaires comme le ***Barreau de la Seine-Saint-Denis***, ***La Fondation Orange Solidarités***, ***Kaspersky France***, l'association ***Echap***, sont également remercié·es pour leurs apports.

RÉDACTION
Iman Karzabi
Aurélie Latourès

ÉDITEUR
Centre Hubertine Auclert
Septembre 2020
Mise à jour :
Novembre 2022

MISE EN PAGE
Delphine Hugueny

ILLUSTRATIONS
Marianne Balabaud

IMPRIMERIE
Groupe Sprint - Alliance
Partenaires Graphiques

Le Centre Hubertine Auclert, centre francilien pour l'égalité femmes-hommes, contribue avec l'ensemble de ses membres, à la lutte contre les inégalités et les discriminations fondées sur le sexe et le genre.

Ses missions se déclinent en quatre pôles :

/ Construire une plateforme régionale de ressources et d'échanges sur l'égalité femmes-hommes : « l'égalithèque ».

/ Renforcer le réseau des acteurs et actrices franciliennes de l'égalité femmes-hommes à travers des accompagnements individuels et l'organisation de cadres d'échanges collectifs.

/ Promouvoir l'éducation à l'égalité, notamment via la réalisation d'études et d'analyses des représentations sexuées et sexistes dans les outils éducatifs.

/ Lutter contre toutes les formes de violences faites aux femmes, avec l'Observatoire régional des violences faites aux femmes intégré au Centre Hubertine Auclert.

centre hubertine auclert

Région îledeFrance

www.centre-hubertine-auclert.fr