Abus des moyens de télécommunication et réseaux sociaux

Sommaire

Généralités

Une part de notre existence se déroule sur les réseaux sociaux et par l'intermédiaire de nos téléphones portables dits « intelligents ». Leur utilisation ouvre la voie à des abus, qui vont du démarchage publicitaire à des formes éprouvantes de harcèlement. Il existe certaines mesures dissuasives d'ordre technique ou judiciaire pour se prémunir, se défendre ou mettre fin aux désagréments ou aux atteintes entraînés par l'utilisation abusive de moyens de télécommunication.

Descriptif

Démarchage téléphonique

Les appels publicitaires sont autorisés. Toutefois, les entreprises qui recourent à ce type de démarchage doivent respecter certaines règles.

- Les appels publicitaires de tiers à des personnes qui ont fait ajouter un astérisque (*) à leur inscription dans l'annuaire sont interdits.
- Une entreprise n'a pas le droit d'automatiser complètement le démarchage ; le destinataire doit être mis en liaison avec une personne une fois la communication établie.
- L'appel publicitaire doit respecter les lois, en matière de protection de la personnalité selon le code civil suisse (art. 28 ss. CC), la loi fédérale sur la protection des données (art. 8 et 12 LPD) et la loi fédérale contre la concurrence déloyale (art. 2 et 3 al. 1 let. u, v et w LCD).

Souvent, c'est l'appelé lui-même qui a divulgué son numéro de téléphone en participant à un concours ou à une vente, avec l'autorisation d'utiliser les données à des fins de marketing. Lorsque des informations ne sont pas obligatoires, comme c'est souvent le cas pour le numéro de téléphone, il est loisible de ne pas le transmettre.

Mesures contre le démarchage téléphonique

Ajout d'un astérisque

Afin de se prémunir contre les appels indésirables, il est possible de demander à son opérateur d'ajouter un astérisque à côté de son numéro inscrit dans l'annuaire. Depuis avril 2012, le non-respect de l'astérisque est considéré être une pratique déloyale (art. 3 let. u LCD). Les appels indésirables peuvent être annoncés au Secrétariat d'Etat à l'économie (SECO) et aux associations de protections des consommateurs, comme la FRC (site dans les liens utiles).

Refus des appels masqués

S'agissant du téléphone fixe, l'opérateur auquel est affilié l'abonné propose généralement des procédures permettant de refuser les appels anonymes, c'est-à-dire ceux dont le numéro ne s'affiche pas sur le combiné. S'agissant du téléphone portable, certains appareils ont une fonction permettant de configurer le blocage des appels anonymes. Cela peut parfois poser des difficultés, notamment parce que certaines administrations publiques utilisent des numéros masqués. L'appelant est cependant avisé du refus des numéros masqués. Il existe aussi des appareils qui permettent de refuser des appels masqués.

Demande du nom de l'appelant à son opérateur téléphonique

En cas d'appels abusifs, vous pouvez demander à votre opérateur le nom et l'adresse du titulaire du numéro. Vous devez néanmoins prouver que ces données sont nécessaires pour démontrer un abus et dès lors indiquer l'heure et la durée des appels que votre opérateur doit vérifier. Toutefois, il n'est pas toujours possible de savoir à qui appartient le numéro, parfois parce que l'appel provient de l'étranger et parfois pour des raisons techniques. Il est en effet possible de remplacer un numéro par un autre (Caller-ID Spoofing).

Obtention d'un nouveau numéro de téléphone et disparition de l'annuaire

Il est par ailleurs possible d'obtenir la mise à disposition d'un nouveau numéro de téléphone, qui ne sera pas communiqué par le numéro des renseignements. Il n'est plus obligatoire de figurer dans l'annuaire et l'abonné peut choisir de figurer dans l'une des listes suivantes:

- blanche: le numéro figure dans l'annuaire, sur internet (également auprès d'éditeurs qui acquièrent ces données), sur le DVD et dans la base de données des renseignements;
- verte: le numéro est donné par le numéro des renseignements et sur internet;
- rouge: l'adresse est communiquée, mais pas le numéro de téléphone;
- noire: aucune information n'est divulguée.

Choisir de figurer dans la liste noire pour échapper à des appels anonymes peut toutefois ne pas être judicieux. En effet, l'abonné peut avoir communiqué son numéro à des tiers qui eux-mêmes l'auront donné, etc., ce qui rend le secret tout relatif. Surtout, il risque de ne pas pouvoir être atteint en cas d'urgence. Il est cependant possible de faire installer une seconde ligne qui, elle, sera sur liste noire. Il est aussi possible d'avoir son numéro de téléphone sous un autre nom, par exemple celui d'un membre de sa famille ou d'une société.

Les questions relatives à la présence dans l'annuaire sont traitées sur le site du Préposé fédéral à la protection des données et à la transparence (PFPDT – dans les sites utiles)

Arnaques sur internet

Certains sites proposent des offres en apparence gratuites, mais qui se révèlent payantes, soit par l'envoi d'une facture suite à un téléchargement, soit par l'envoi de SMS surtaxés.

L'une des caractéristiques de ces arnaques, qui portent sur des sujets divers (concours, sonneries « gratuites », vidéos pour adultes, programmes « gratuits »...), c'est qu'il faut s'inscrire en indiquant ses coordonnées complètes, alors que l'offre est présentée comme gratuite. Avec son clic d'acceptation, le consommateur accepte aussi les conditions générales, dans lesquels les termes réels du contrat sont indiqués.

Mesures contres les arnaques sur internet

Le paragraphe qui suit se base sur les informations du SECO « Attention aux arnaques sur internet » (lien dans les sources). Le dicton « mieux vaut prévenir que guérir » est ici à sa place. Mieux vaut ne pas remplir de formulaire et ne pas cliquer sur J'accepte, alors qu'en règle générale, aucune demande d'identification n'est requise pour accéder à des offres réellement gratuites.

S'il est trop tard pour la prévention et que la victime de l'arnaque reçoit une facture, le SECO préconise de refuser de la payer et de le faire savoir à son expéditeur, par courrier recommandé, en ces termes « j'ai été induit en erreur par votre site internet. Par conséquent, je conteste la validité de tout contrat éventuellement conclu aux motifs d'une erreur essentiel et de dol. Le contrat est donc frappé de nullité. » Tout courrier de relance peut ensuite être ignoré. Attention : le délai pour contester le contrat est d'une année à partir de la découverte de l'erreur ou de la tromperie.

Dans le cas de la conclusion d'un abonnement SMS onéreux (dont la facture arrivera par le biais de l'opérateur téléphonique), le SECO conseille de faire cesser de suite le service en question en envoyant un SMS avec le mot STOP au numéro court. Ensuite, il faut contester le contrat (voir le paragraphe précédent) et envoyer copie de la contestation à son opérateur téléphonique avant la date d'échéance de la facture. À l'opérateur, il faut expliquer que l'on conteste devoir cette somme et que l'on ne réglera que la partie de la facture de téléphone qui est non-contestée. Selon le SECO, l'opérateur n'a pas le droit de bloquer un numéro de téléphone dans un tel cas (il peut en revanche bloquer les services à valeur

ajoutée).

Si aucun accord n'est trouvé avec l'opérateur, le consommateur peut s'adresser l'organe de conciliation des télécommunications (l'Ombudscom), dont le site est référencé à la fin de la fiche.

Les associations de consommateurs peuvent également fournir une aide utile (voir dans les sites utiles).

Pour en savoir plus, voir la fiche Droit de la consommation.

Pourriels (Spams)

L'envoi en masse par voie de télécommunication (fax, courriels, sms) de messages publicitaires sans l'autorisation des destinataires est interdit (art. 3 let. o de la Loi fédérale sur la concurrence déloyale, LCD). Les fournisseurs de services de télécommunication doivent disposer d'un service pour recevoir les annonces de spam et doivent prendre des mesures contre l'envoi de publicité en masse. En pratique, il s'agit surtout de suivre les règles de prudence lorsque l'on donne ses coordonnées, protéger les données de ses correspondants, filtrer ses messages et protéger son ordinateur.

En cas d'appel préenregistré ou de sms demandant de composer un certain numéro, il est recommandé de ne rappeler que si le numéro ou son titulaire paraît digne de confiance. Il est recommandé de ne pas répondre à des appels ou des sms de caractère publicitaire pour exprimer son mécontentement, mais de noter les informations importantes et de les signaler à l'opérateur téléphonique.

Concernant les courriels, il est recommandé de supprimer les spams sans les ouvrir, de n'ouvrir en aucun cas les pièces jointes, et de n'accepter aucune offre commerciale. Il est également conseillé de ne jamais répondre au spam, afin d'éviter de confirmer au spammeur que votre adresse est valide. Celle-ci sera à nouveau utilisée pour vous envoyer davantage de courriels non sollicités et elle pourrait même être revendue. De plus, il est fortement déconseillé de cliquer sur les liens hypertextes des spams!

Vous pouvez informer votre fournisseur de services des télécommunications (p.ex. votre fournisseur d'accès à Internet) des spams reçus et demandez-lui de vous indiquer leur provenance. Selon le préposé fédéral à la protection des données et à la transparence (PFPDT) : « vous devez rendre vraisemblable, par écrit, que vous avez reçu de la publicité de masse déloyale (p.ex. envoyez une copie des spams que vous avez reçus). Pour autant que ces données soient encore disponibles, votre fournisseur devra vous indiquer la date, le moment et la durée de la communication ou du message, l'élément d'adressage ainsi que les noms et l'adresse de l'expéditeur. Selon que le message a été envoyé depuis la Suisse ou depuis l'étranger, vous disposez de plusieurs moyens ».

Pour plus d'informations :
SECO "Réclamation pour toute autre pratique commerciale déloyale"

Abus de réseaux sociaux

Les réseaux sociaux peuvent également être utilisés à des fins malveillantes, par exemple dans une volonté de harcèlement (voir ci-dessous) ou afin de soutirer des informations qui se retourneront contre la personne qui les a divulguées. Par exemple, un voleur a tout intérêt de savoir à quel moment ses futures victimes partent en vacances. Ici aussi, la prudence dans le partage des informations et l'acceptation de nouveaux « amis » est de mise !

Par ailleurs, les textes et les photos personnels, une fois envoyés sur la toile, peuvent être partagés et ne sont plus sous contrôle de l'auteur de la communication. Ainsi, un message rédigé dans un moment festif peut s'avérer embrassant lors d'un entretien d'embauche, des années plus tard. Dans ces situations, il ne s'agit plus d'abus, mais d'un usage des réseaux sociaux qui se retourne contre son auteur.

Enfin, les propriétaires des réseaux sociaux reçoivent des données nombreuses et précises de la part de leurs membres. Le préposé fédéral à la protection des données et à la transparence (PFPDT) souligne que les données des utilisatrices et utilisateurs sont susceptibles de livrer des profils de la personnalité détaillés qui peuvent être utilisés avec profit, notamment en matière de publicité.

Mise en garde du préposé fédéral à la protection des données (PFPDT)

Le PFPDT relève deux aspects nouveaux des réseaux sociaux, s'agissant de la protection des données :

- Ce sont les utilisateurs eux-mêmes qui enregistrent les informations personnelles en question dans les profils Internet et qui donnent donc ainsi leur propre consentement.
- Les particuliers sont ainsi en mesure d'accéder aisément aux données personnelles d'autres particuliers, ce qui peut engendrer des risques. »

Le PFPDT recommande notamment :

- Prenez des précautions avant de publier sur un réseau social vos coordonnées (nom, adresse, numéro de téléphone) ainsi que toute autre donnée ou information personnelle (p.ex. convictions politiques). Utilisez des pseudonymes.
- Avant de publier des données, demandez-vous toujours si, lors d'un entretien d'embauche, vous souhaiteriez être confronté aux données/images en question, et cela, même dans dix ans.
- Respectez la sphère privée de tierces personnes, ne publiez pas leurs données personnelles et ne mettez pas leur nom sur des photos.

- Informez-vous au sujet des fournisseurs du portail et de la manière dont ils assurent la protection de la sphère privée des utilisateurs. Le service en question dispose-t-il d'un label de qualité en matière de protection des données ou de sécurité? Soyez critique à l'égard du comportement du fournisseur.
- Choisissez dans la configuration de votre profil les options permettant de préserver votre vie privée. Limitez l'accès à vos informations et photos à un cercle de personnes déterminé. Ne mettez jamais de contenus délicats sur Internet.
- N'employez pas le même nom d'utilisateur ni le même mot de passe pour tous les services.

Le site du préposé fédéral à la protection des données et à la transparence (PFPDT – dans les sites utiles) contient des informations supplémentaires.

Abus des réseaux sociaux - cadre légal

Que ce soit en ligne ou « en direct », une infraction reste une infraction. Peu importe par exemple qu'une escroquerie utilise ou non internet pour se produire. De la même façon, les atteintes à la personnalité sont interdites et réprimées par le droit civil et pénal. Par contre, la poursuite des auteurs, parfois domiciliés à l'étranger et/ou agissant de manière anonyme, peut se révéler difficile. Pour le cadre légal, se référer à la fiche Protection de la personnalité et lutte contre les discriminations.

Hameçonnage (phishing), envoi de courriels frauduleux

Le phishing ou hameçonnage consiste à conduire une personne à révéler des données personnelles, par exemple bancaires ou à faire des actes qui lui sont dommageables (envoyer une somme d'argent pour se voir attribuer un appartement par exemple). En matière d'escroquerie, la seule limite est l'imagination et l'astuce de son auteur. Le Centre national pour la cybersécurité NCSC a publié une liste des différentes formes d'escroquerie.

Des criminels peuvent travestir leur identité afin de récolter des données telles que mots de passe, données bancaires, nom et adresses exactes etc. Ces informations leurs permettent ensuite de réaliser des affaires au nom de leurs victimes et ainsi de s'enrichir à leurs dépens. Les moyens utilisés pour y parvenir vont du plus rudimentaire (fausse adresse mail, message bourré de fautes d'orthographe) au plus raffiné (courriel au premier abord digne de confiance et création d'unfaux site d'une banque). Le courriel fait valoir des motifs de sécurité ou le remboursement d'une somme payée en trop et demande au destinataire de remplir un formulaire avec ses données personnelles, notamment des mots de passe ou des données bancaires.

Les données ainsi subtilisées peuvent être soit directement utilisées, soit revendues à des tiers.

Si le fait d'envoyer des courriels de hameçonnage n'est en lui-même pas punissable, l'utilisation des données récoltées peut être constitutive d'une utilisation frauduleuse d'un ordinateur (art. 147 CP) ou d'escroquerie (art. 146 CP).

Quelques règles de base

Ces conseils viennent du site de l'office fédéral de la police (fedpol – dans les sites utiles).

- Rester vigilant-es : ne pas croire à tout ce que l'on lit sur internet ou dans les courriels, même si l'auteur ou l'expéditeur paraissent à première vue dignes de confiance ou connus. Les entreprises sérieuses n'exigent jamais de données confidentielles par courriel. Rester prudent-es également lorsqu'une offre défie toute concurrence ! Mieux vaut renoncer en cas de doute.
- Ne jamais cliquer sur un lien et ne jamais ouvrir de pièces jointes à un courriel dont l'expéditeur est inconnu.
- Protéger son ordinateur en actualisant tous les programmes, en particulier la protection antivirus, et effectuer les mises à jour du système d'exploitation.

Chantage par webcam (sextorsion)

Informations tirées de l'aide-mémoire de fedpol (voir dans les sources).

La sextorsion est une forme de chantage qui utilise une vidéo reproduisant des actes sexuels de la victime, et la menace de publier la scène sur des réseaux sociaux ou sur un site de vidéo en ligne (Youtube p.ex.). Souvent, les victimes sont des hommes, qui sont contactés sur un réseau social par des femmes inconnues. Les auteur-es ont un contact avec leurs victimes par webcam et les incitent à des actes de sexe en ligne, qu'ils/elles enregistrent. Ils demandent ensuite de l'argent pour ne pas publier la vidéo en question. Selon l'office fédéral de la police, les auteurs opèrent souvent depuis des cybers-cafés en Afrique de l'Ouest. Malgré le versement de la somme exigée, il arrive que la vidéo soit publiée (avec le nom de la personne suivi p.ex. de la mention « pédophile ») ou que les extorqueurs continuent d'exiger de l'argent.

Une variante de ce mode opératoire est l'envoi d'un courriel dans lequel des escrocs prétendent avoir pris le contrôle de l'ordinateur (et de la webcam) et menacent de publier des images ou vidéos de la victime en train de consommer de la pornographie. Ils demandent ensuite un paiement en bitcoin pour ne pas mettre leur menace à exécution. La fréquence de ces tentatives d'extorsion en 2018 a amené les autorités à créer le site stop-sextorsion.ch (dans les sites utiles).

Les dispositions pénales qui répriment la sextorsion sont les suivantes : l'art. 156 CP (extorsion et chantage), l'art. 179^{quater} CP (violation du domaine secret ou du domaine privé au moyen d'un appareil de prises de vue), l'art. 174 CP (calomnie, si la vidéo est publiée avec un message calomnieux), l'art. 197 CP (pornographie). Même s'il est peu probable que les coupables puissent être traduits en justice (et l'argent versé

récupéré), il est important de porter plainte. Cela permet à la police de mesurer l'étendue de ces pratiques, d'opérer des recoupements et de lancer des campagnes de prévention.

Quelques conseils

- La prudence est de mise en cas de propositions d'amitié ou de rencontre en ligne de personnes inconnues, qui semblent nous contacter par hasard (et dont le profil est plus qu'avantageux).
- Toujours avoir à l'esprit que toute conversation par webcam peut être enregistrée. La webcam doit être désactivée lorsque l'on ne se trouve pas en discussion vidéo et un papier doit être collé sur l'objectif.
- Ne pas céder pas au chantage.
- Rompre tout contact avec le maître chanteur.
- Changer d'adresse e-mail.
- Modifier vos paramètres de sécurité sur vos comptes de réseaux sociaux (Facebook, Google+, Skype, etc…).
- Contacter immédiatement YouTube ou Facebook afin qu'ils puissent supprimer la vidéo/l'image. Activer une alerte google personnalisée qui permet d'être averti dès qu'une photo ou une vidéo à son nom est publiée sur internet.
- En particulier si un versement a déjà été effectué, signaler l'incident à votre poste de Police cantonale, en prenant soin de conserver toutes les preuves.
- Contacter le Centre LAVI de votre région. Le Centre LAVI (Loi sur l'aide aux victimes d'infractions) vient en aide aux victimes d'infractions, par le biais de l'écoute, de conseils, d'une assistance financière limitée et d'une orientation vers les professionnels qualifiés (voir fiche « Aide aux victimes d'infractions »).
- Informer votre entourage sur cette méthode de chantage.

Romance Scam (arnaque aux sentiments)

« Dans ce type d'arnaque, la victime croit rencontrer l'âme sœur, par exemple sur un site de dialogue en direct ou un site de rencontres. Une complicité se noue au fil des discussions. En réalité, la victime est en train de dialoguer avec un escroc, qui utilisera cette relation pour lui demander de l'argent. Les justifications à cette demande peuvent être diverses, mais la plupart du temps les escrocs expliquent connaître des difficultés financières passagères. Ces derniers utilisent bien souvent de fausses photos et font diverses promesses (mariage, rencontre future, etc.) pour mieux manipuler leur victime. » (Service national de coordination de la lutte contre la criminalité sur Internet).

Souvent, le faux profil est attractif. L'escroc prend le temps de connaître sa victime et l'amène à se dévoiler, également dans le but de créer un état de dépendance affective chez elle. Il va rapidement proposer une rencontre dans la vie réelle, qui sera toujours contrariée par mille péripéties, qui formeront autant d'appel à l'aide financière à l'attention de la victime. Tout cela ne s'arrêtera qu'au moment où cette dernière n'aura plus d'argent – ou au moment où elle prend conscience de l'escroquerie.

Conseils : Il est recommandé de se méfier de son interlocuteur si celui-ci vous promet le grand amour après quelques discussions seulement. De même si ce dernier parle de problèmes financiers et vous demande de l'aide. Il faut également être prudent sur l'identité de l'interlocuteur car il peut facilement tromper la victime sur son identité (nom, photo, etc…). Pour cette raison, il convient de rester soi-même le plus anonyme possible et de ne pas envoyer de photos ou de vidéo sexy de soi-même que l'on n'aimerait pas voir diffusée en public.

En tous les cas, il ne faut jamais verser d'argent à une personne inconnue, jamais rencontrée physiquement.

Harcèlement obsessionnel (Stalking)

Le stalking (de l'anglais « to stalk » = traquer) est une forme particulière de harcèlement où une personne porte une attention obsessionnelle envers une autre et peut inclure le fait de suivre ou de surveiller la victime. Le harceleur ou la harceleuse va persécuter, harceler ou menacer sa victime intentionnellement et de façon réitérée, suscitant la peur et portant atteinte à son intégrité physique ou psychique.

Ce harcèlement peut être de gravité variable. Il peut se dérouler en ligne, par téléphone, par les réseaux sociaux ou physiquement. Il peut consister en des actes de surveillance, des menaces, des violations de domicile, des injures, des dommages à la propriété (casser des objets appartenant à la victime, par exemple). Les victimes sont en majorité des femmes, qui sont principalement harcelées par des hommes. Les victimes hommes sont harcelées dans une proportion égale par des hommes ou des femmes. Des actes de violence et des menaces se produisent dans environ un tiers des cas, selon le bureau fédéral de l'égalité (référence dans les sources). Ce risque existe particulièrement lorsque le harcèlement est le fait d'un-e ex-partenaire, que la violence avait déjà existé pendant la relation et que la famille a des enfants communs (voir la fiche : violence domestique).

Le harcèlement obsessionnel n'est pas une infraction pénale. Par contre, les actes individuels de harcèlement peuvent constituer une infraction

et être dénoncés. Parmi eux : la menace (art. 180 CP), la contrainte (art. 181 CP), l'utilisation abusive d'une installation de télécommunication (art. 179septies CP), la violation de domicile (art. 186 CP), les dommages à la propriété (art. 144 CP) etc.

Le 1er juillet 2020, des modifications du Code pénal sont entrées en vigueur ; elles ont pour objectif de mieux protéger les victimes de violence domestique et de harcèlement obsessionnel. En particulier, la victime ne devra plus assumer de frais de procédure et les décisions de justice feront l'objet d'une communication aux services cantonaux chargés d'intervenir en cas de crises, aux autorités de protection de l'enfant et de l'adulte, notamment.

En droit civil, l'article 28b CC prévoit qu'une personne peut demander à un tribunal, en cas de violence, de menaces ou de harcèlement, d'interdire à l'auteur de ces actes :

- De l'approcher ou d'accéder à un périmètre déterminé autour de son logement ;
- De fréquenter certains lieux ;
- De prendre contact avec elle, notamment par téléphone, par écrit ou par voie électronique, ou de lui causer d'autres désagréments.

Plus d'informations dans la fiche : violence domestique.

Quelques conseils

Tirés de la brochure de la Prévention Suisse de la Criminalité (voir dans les sources)

- Couper radicalement contact avec la personne qui vous harcèle et rester ferme
- Refuser les cadeaux et articles commandés à votre nom
- Informer l'entourage (pour avoir du soutien, être protéger et leur éviter de divulguer des informations)
- Documenter tous les faits et gestes de la personne qui vous harcèle (tenir un journal des événements, conserver les emails, sms, lettres etc, photographier les cadeaux avant de les rendre, etc...)
- Contacter le Centre LAVI de votre région
- Contacter la police pour évaluer ensemble les mesures à prendre.

Procédure

Démarchage téléphonique et pourriels

Comme évoqué plus haut, toute personne peut s'adresser à son opérateur pour enquêter sur la provenance des appels ou messages. Lorsque l'auteur d'appels abusifs est identifié, l'opérateur, ou la personne importunée peut adresser à l'auteur une lettre d'avertissement signalant la possibilité de porter plainte en vertu de l'article 179septies précité. Il est aussi possible de dénoncer les pratiques déloyales auprès du SECO et auprès d'une association de défense des consommateurs (voir les paragraphes correspondants).

Plainte pénale

Selon l'article 179septies CP, "Quiconque utilise abusivement une installation de télécommunication pour inquiéter un tiers ou pour l'importuner est, sur plainte, puni d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire". Il est donc possible de porter plainte contre la personne qui abuse du téléphone (pour la procédure de plainte et ses suites, voir la fiche Plainte pénale).

En cas de harcèlement obsessionnel, de cyber-harcèlement et de hameçonnage (phishing), une plainte pénale est également possible. Les victimes peuvent trouver du soutien et des conseils dans le centre LAVI de leur canton (voir la fiche Aide aux victimes d'infractions).

Pour les cas de Romance scam (ou Love scam) : « si vous avez déjà procédé à des versements, il est recommandé de s'adresser à la police cantonale et éventuellement de déposer plainte pour escroquerie. » (Service national de coordination de la lutte contre la criminalité sur Internet). Il n'y a toutefois pas d'escroquerie au sens du droit pénal si la victime aurait pu se protéger avec un minimum d'attention.

Pour plus d'informations :
Prévention Suisse de la criminalité – rubrique "Escroquerie"

Mesures de protection de la personnalité

En cas de violence, de menaces ou de harcèlement, on peut demander au juge d'interdire à l'auteur de l'atteinte, en particulier, de s'approcher ou d'accéder à un périmètre déterminé autour de son logement (art. 28b al. 1 ch. 1 CC), de fréquenter certains lieux, notamment des rues, places ou quartiers (ch. 2), de prendre contact avec soi, notamment par téléphone, par écrit ou par voie électronique, ou de causer d'autres dérangements (ch. 3) (voir la fiche Protection de la personnalité et lutte contre les discriminations).

Recours

Se référer aux fiches Procédure civile suisse, Procédure pénale suisse, ainsi qu'aux fiches cantonales correspondantes.

Sources

Responsable rédaction: ARTIAS

Sources:

Démarchage téléphonique et pourriels:

SECO: Se préserver des appels publicitaires non sollicités, 2021

SECO: Attention aux arnaques sur Internet, 2010

Hameçonnage (phishing):

FEDPOL : Hameçonnage (phishing), vishing et smishing

Chantage par webcam (sextorsion):

FEDPOL : Sextortion

Arnaque aux sentiments (romance scam):

Prévention suisse de la criminalité : grand amour ou grosse arnaque ? Brochure d'information.

Harcèlement obsessionnel (stalking):

Prévention Suisse de la Criminalité > Stalking
Bureau fédéral de l'égalité entre femmes et hommes > Stalking

---

Adresses

Préposé fédéral à la protection des données et à la transparence (PFPDT) (Berne)
Office fédéral de la police (fedpol) (Berne)

Lois et Règlements

Code pénal suisse du 21 septembre 1937 (CP) (RS 311)
Loi fédérale du 19 décembre 1986 sur la concurrence déloyale (LCD) (RS 241)
Loi fédérale du 19 juin 1992 sur la protection des données (LPD) (RS 235.1)
Loi fédérale du 30 avril 1997 sur les télécommunications (LTC) (RS 784.10)

Sites utiles

Secrétariat d'Etat à l'économie (SECO)
Prévention Suisse de la Criminalité
Préposé fédéral à la protection des données et à la transparence
Aide aux victimes en Suisse
Jeunes et médias - portails d'information
Fédération romande des consommateurs
Ciao.ch
Stop sextortion!
Organe de conciliation des télécommunications
Le Centre national pour la cybersécurité (NCSC)