Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

JEUNES ET MÉDIAS
PLATEFORME NATIONALE DE PROMOTION DES COMPÉTENCES MÉDIATIQUES

Protection des données

Dossier d'information

En coopération avec le Préposé fédéral à la protection des données PFPDT et la plateforme nationale de promotion des compétences « Jeunes et Médias » de l'Office fédéral des assurances sociales OFAS

Table des matières

1. Qu'est-ce que la protection des données?

Que nous discutions de nos devoirs dans le chat de la classe, sur WhatsApp, ou que nous publiions une nouvelle photo de nous, malade, pour l'envoyer à notre professeur par e-mail ou SMS; que nous commandions une nouvelle paire de chaussures de sport sur une boutique en ligne ou que nous participions à une enquête dans la rue, pour laquelle nous communiquons notre âge et notre adresse – nombreuses sont les informations personnelles échangées au quotidien, et pas seulement avec la famille ou les amis. Nous devrions toujours garder à l'esprit que ces données peuvent tomber entre les mains de personnes qui n'étaient pas leurs destinataires initiaux, et qu'elles peuvent ne pas être utilisées comme nous le souhaiterions.

1.1. Définition

La notion de «protection des données» est apparue dans la seconde moitié du 20^{e} siècle et est définie comme la protection de la vie privée lors du traitement des données, et comme protection du droit d'autodétermination informationnelle. Cela signifie que toute personne peut librement décider des données personnelles la concernant pouvant être communiquées, à qui elles sont communiquées et dans quel but.

Les données personnelles regroupent toutes les informations se rapportant à une personne identifiable, telles que:

- les données d'adresses
- l'âge
- les intérêts et penchants personnels
- les données de positionnement, qu'un téléphone mobile enregistre par GPS
- sa propre image (p.es. photo du profil)
- etc.

La protection des données signifie que la vie privée des personnes dont les données sont traitées par les administrations, les entreprises ou les personnes privées, est protégée.

La protection des données gagne en importance dans la société de l'information numérique et interconnectée. Elle vise à éviter la collecte incontrôlée et l'utilisation abusive de données et la tendance à la «transparence totale de la personne», la création de monopoles des données par des entreprises privées et le recours à des mesures de surveillance étatiques.

(Source: Wikipédia, traduction du site allemand)

Protection de la personne
Si la notion de protection des données peut sembler sèche et impersonnelle, elle est pourtant principalement axée sur notre personne, c'est-à-dire sur la protection de notre personnalité et de nos droits fondamentaux. En effet: vous ne souhaitez pas révéler à tout un chacun toutes des informations vous concernant ou concernant votre vie.

Toutes les données ayant trait à notre personne sont des «données à caractère personnel» ou des «données personnelles». Ces données révèlent de nombreuses informations sur notre personne et sont donc précieuses. Pour les entreprises, elles représentent beaucoup d'argent et

peuvent être utilisées de manière abusive. C'est pourquoi nous devons être particulièrement vigilants – c'est-à-dire économes et réfléchis – lors de l'utilisation de nos données personnelles. Nous devons être conscients de la valeur de nos données. Protéger nos données revient à protéger notre **vie privée, notre anonymat et à accroître notre sécurité**.

Données sensibles

Certaines données personnelles sont considérées comme particulièrement sensibles, parce qu'elles peuvent avoir des conséquences très négatives pour la personne concernée si elles tombent entre de mauvaises mains. Sont notamment considérées comme données sensibles les données relatives aux convictions religieuses, philosophiques ou politiques d'une personne; ainsi que toutes informations touchant à la santé, la sphère intime (sexualité, par exemple) ou des poursuites ou sanctions pénales.

La liste intégrale est énumérée au chapitre «*1.1.1 Bases légales*».

Réflexions approfondies

La technique actuelle permet une saisie, un regroupement et une disposition presque illimités des informations. Le potentiel d'atteinte à la personnalité a donc lui aussi augmenté. En tant qu'individus, nous ne sommes pour ainsi dire plus capables de contrôler les données nous concernant qu'un tiers est autorisé à traiter. Tous les jours, nous transmettons des données nous concernant, volontairement ou non, à des tiers, souvent sans vraiment savoir à quoi elles serviront ni où et combien de temps elles resteront enregistrées. De cette manière, les entreprises peuvent par exemple savoir aujourd'hui si un client est un bon ou un mauvais payeur, connaître les livres qu'il lit ou la musique qu'il écoute, sans que la personne concernée en soit consciente.

Toute collecte et tout traitement d'informations sur des personnes touchent à leur personnalité. Le degré d'atteinte à la personnalité peut varier, et entraîner des réactions positives ou négatives. Une personne peut être victime de l'opprobre toute sa vie si des données négatives à son sujet sont conservées pour une durée illimitée et régulièrement réutilisées. C'est pourquoi les données personnelles sont un bien qu'il s'agit de protéger. Pour les personnes concernées, mais aussi pour les tiers touchés.

L'objectif de la protection des données est de protéger ce bien précieux: elle met en place des garde-fous pour le traitement des données à caractère personnel, de manière à garantir que l'épanouissement de la personnalité ne soit pas menacé par un traitement indésirable des données. Sauf disposition contraire de la loi, tout individu doit pouvoir décider lui-même de la communication et de l'emploi des informations le concernant. *(Voir Message relatif à la révision de la loi fédérale sur la protection des données), LPD, 23 mars 1988, ch. 113: Objectifs principaux de la loi sur la protection des données)*

L'individu a par ailleurs le droit de savoir qui détient quelles données à son sujet et dans quel but elles sont traitées. Nous pouvons exiger du maître d'un fichier de nous communiquer, de corriger ou de supprimer les données personnelles nous concernant.

Pourquoi la protection des données est-elle si importante?

La **technologie de l'information** permet de **saisir** d'énormes **quantités de données personnelles et de les connecter entre elles** (mots-clés: big data, intelligence artificielle, Internet des objets). Les personnes chargées du traitement de ces données ne sont malheureusement pas toujours conscientes des derniers progrès de la technique. La plupart des personnes – que ce soient celles qui traitent les données ou celles que ces données concernent – ne sont en outre pas encore suffisamment sensibilisées aux questions liées à la protection de la personnalité.

Nous n'avons que trop tendance à traiter nos données personnelles avec désinvolture, que ce soit sur Internet ou **en complétant des questionnaires ou des formulaires de concours,** ou lors de l'utilisation de **diverses applications sur notre smartphone** (activation de la fonction de localisation, la communication d'informations personnelles sur des réseaux sociaux, etc.), pour ne citer que quelques exemples.

L'évolution incessante des possibilités techniques et les risques qu'elle entraîne (perte de données, vol d'identité, etc.) ne sont pas la seule raison de la mise en place de garde-fous visant la protection de la vie privée. L'exercice de libertés civiles, telles que la liberté d'expression, de croyance et d'association requiert lui aussi la protection des données.

En effet: comment pourriez-vous exprimer librement votre opinion si vous deviez craindre d'être sur écoute? Comment voteriez-vous, si vous deviez le faire publiquement en mentionnant votre nom?

Le **préposé fédéral à la protection des données et à la transparence (PFPDT)** veille au respect des garde-fous mis en place dans la loi sur la protection des données. Il conseille également les personnes privées et les organes fédéraux en matière de respect des dispositions de protection des données. Le PFPDT doit donc informer et sensibiliser, mais aussi intervenir si les maîtres de fichiers ne respectent pas les principes de la protection des données.

(Voir également https://www.edoeb.admin.ch/edoeb/fr/home/le-pfpdt/mandat.html)

1.1.1. Bases légales

Convention européenne des droits de l'homme (CEDH)

Art. 8 Droit au respect de la vie privée et familiale

[1] Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

[2] Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

La protection des données dans la Constitution fédérale:

Art. 13 Protection de la sphère privée

[1] Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications.

[2] Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent.

La protection des données sert donc à protéger les informations relatives à des individus. Toute personne a le droit de déterminer elle-même les informations la concernant pouvant être communiquées, ainsi que quand, où et à qui ces données sont communiquées. La protection des données veille à ce que la collecte et le traitement des données impliquent le moins de données personnelles possible, et jamais plus que le strict nécessaire. Toute personne a par ailleurs le droit d'accès aux données la concernant!

Code civil suisse (CC)

Art. 281B. Protection de la personnalité / II. Contre des atteintes / 1. Principe

II. Contre des atteintes

1. Principe

[1] Celui qui subit une atteinte illicite à sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe.

[2] Une atteinte est illicite, à moins qu'elle ne soit justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi.

Voir également: art. 28a ss. CC (Protection de la personnalité).
https://www.admin.ch/opc/fr/classified-compilation/19070042/index.html#a28

Loi fédérale sur la protection des données (LPD):

Art. 1 But

La présente loi vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données.

(…)

Art. 4 Principes

[1] Tout traitement de données doit être **licite**.

[2] Leur traitement doit être effectué **conformément aux principes de la bonne foi** et de la proportionnalité.

[3] Les données personnelles ne doivent être traitées que dans le **but** qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances.

[4] La collecte de données personnelles, et en particulier les finalités du traitement, doivent être **reconnaissables** pour la personne concernée.

[5] Lorsque son consentement est requis pour justifier le traitement de données personnelles la concernant, la personne concernée ne consent valablement que si elle exprime sa **volonté librement et après avoir été dûment informée**. Lorsqu'il s'agit de données sensibles et de profils de la personnalité, son consentement doit être au surplus explicite.

Les données sensibles dans la loi fédérale sur la protection des données

Art. 3 Définitions

c. données sensibles,
les données personnelles sur:
les opinions ou activités religieuses, philosophiques, politiques ou syndicales
la santé, la sphère intime ou l'appartenance à une race,
3. des mesures d'aide sociale,
4. des poursuites ou sanctions pénales ou administratives.

Adaptation dans la nouvelle loi sur la protection des données

Outre les données actuelles, la nouvelle loi sur la protection des données (LPD) définit également les données biométriques et génétiques comme données sensibles.

1.1.2. Conclusion

Compte tenu des avancées technologiques mentionnées et des possibilités qu'elles offrent d'enregistrer et de connecter entre elles plus rapidement de plus grande quantité de données, il est essentiel de se pencher sur la question de la protection des données.

Par ses possibilités, Internet rend les données qui y sont téléchargées rapidement accessibles à des tiers, or, ce qui est mis en ligne une fois, ne peut être entièrement supprimé ou corrigé que très difficilement, voire pas du tout. Internet n'oublie jamais.

En tant que personne privée, il est particulièrement important de connaître ses droits et de savoir comment réagir, en cas d'enregistrement, de traitement ou de transmission illicites de données personnelles nous concernant. Le présent dossier d'information, les feuilles de travail et mandats correspondants doivent y contribuer.

Par ailleurs, il est indispensable de respecter soi-même les directives de protection des données, de traiter consciemment ses propres données et les données de tiers. Vous trouverez des recommandations et des conseils au chapitre 3 «Conseils pour bien gérer ses données».

1.2. Qui s'intéresse aux données personnelles? Qui les collecte et pourquoi?

Les raisons pour lesquelles une personne s'intéresse à nos données sont diverses.

1.2.1. Fichier national

Dans les Etats autoritaires et totalitaires, les autorités nationales ont tout intérêt à connaître le comportement de leurs citoyens. Dans ce cas, le but est de contrôler les citoyennes et citoyens (mot-clé: «citoyen de verre»).
Le **contrôle** de la société dans l'Allemagne nazie entre 1933 et 1945 en est un exemple particulièrement grave. Des listes des ennemis politiques en général, et des juifs en particulier ont été dressées. Outre la garantie du pouvoir des national-socialistes, l'objectif était en outre l'élimination physique totale des juifs. L'étoile jaune – les juifs devaient afficher leur appartenance au peuple juif en arborant à tout moment une étoile cousue – était une violation particulièrement «visible» de la notion actuelle de la protection des données.

Des démocraties telles que la Suisse connaissent également la collecte de données et l'observation et le contrôle de personnes. A la fin des années 80, il a été établi que les autorités fédérales suisses et les autorités de police cantonales avaient créé environ 700'000 fiches et détenaient ainsi des sonnées sensibles et des informations d'ordre philosophique sur plus de 10% des citoyens et citoyennes suisses. L'objectif officiel était de protéger le pays de la «menace communiste». Suite à ce que l'on a appelé le **Scandale des fiches**, la confiance des citoyennes et citoyens en l'Etat suisse fut ébranlée pour longtemps.
Aujourd'hui encore, les autorités collectent des données, mais de manière officielle et légale. Les membres suisses de groupements extrémistes et criminels ou les personnes liées au terrorisme international, par exemple, sont surveillés. Cette tâche incombe au service de renseignement de

la Confédération (SRC), subordonné au Département fédéral de la défense, de la protection de la population et des sports (DDPS).
Bien entendu, un Etat de droit ne peut admettre la surveillance d'une personne sans raison. Des fondements législatifs précis régissent les atteintes de ce type dans les droits individuels. L'activité étatique doit donc être **prévue par une loi** (droit de la procédure pénale, loi sur les services de renseignement, par exemple). On parle alors de «principe de **la légalité»**).
Les enquêtes, investigations et le contrôle de personnes sont par ailleurs régie par le principe de **proportionnalité**. Il convient en tout cas de voir si l'atteinte aux intérêts privés et aux droits fondamentaux est justifiée par l'intérêt public général.

Légalité et proportionnalité dans la Constitution fédérale

Art. 5 Principes de l'activité de l'Etat régi par le droit

[1] Le droit est la base et la limite de l'activité de l'Etat.

[2] L'activité de l'Etat doit répondre à un intérêt public et être proportionnée au but visé.

1.2.2. Collecte de données par des personnes privées et des sociétés

Fournisseurs d'accès à Internet et de services en ligne

Tout utilisateur d'Internet, que ce soit avec un ordinateur, une tablette ou un téléphone mobile, génère automatiquement des données. Ces données peuvent être enregistrées par le fournisseur d'accès à Internet. Cela permet de déterminer qui visite quels sites Internet et combien de temps, ou qui utilise quelles applications. Ces données intéressent les entreprises, car elles leur révèlent notamment le comportement des consommateurs et les préférences des internautes. Il est alors possible de faire parvenir à l'utilisateur des publicités personnalisées, ciblant ses intérêts. Un utilisateur utilisant régulièrement des portails de shopping en ligne et des applications de shopping trouvera dans son navigateur ou directement dans l'application des propositions d'articles pouvant également l'intéresser.

Assurances

Les statistiques généralement réalisées sur la base de données anonymisées permettent de définir des groupes de risques et d'exiger en conséquence des primes d'assurance plus élevées pour certains groupes. C'est notamment le cas des statistiques sur les accidents de la route: selon l'âge ou le sexe de la personne, certaines catégories d'assurés paient une prime plus élevée que d'autres assurés parce que leur «groupe» cause statistiquement parlant plus d'accidents, mais paient moins à la caisse-maladie parce qu'ils sont généralement moins malades.

Pour définir des modèles d'assurance sur mesure ou pour participer à des programmes de bonification, les assurances collectent cependant de plus en plus souvent des informations personnelles, dont des données sensibles relatives à la santé ou au profil de déplacement.

Commerces de détail

Les profils clients aident les commerces de détail à analyser les habitudes d'achat de leurs clients, ce qui leur permet de concevoir leur offre de marchandises et leur publicité de manière ciblée, et de générer plus de chiffre d'affaires et de bénéfices. L'acheteur risque indirectement d'être manipulé.

Questionnaires ou des formulaires de concours

Généralement, les sociétés utilisent ces formulaires pour personnaliser leurs publicités et les adresser à des clients potentiels.

Les adresses et autres données personnelles de clients potentiels ont une influence décisive sur l'efficacité du marketing direct. En effet, des données aussi exactes que possible sur l'âge, la profession, le comportement de consommation, etc. contribuent à réduire le risque de publicité inutile. Parmi la population, on constate une grande prédisposition à communiquer des données, même très personnelles, lorsque la personne interrogée croit participer à un projet scientifique. Un procédé particulièrement fructueux consiste à lier de tels sondages à la participation à un concours ou un jeu, sans préciser le but de la collecte de données personnelles. L'information relative à l'utilisation des données à d'autres fins n'est souvent indiquée qu'en petits caractères et passe souvent inaperçue. Les clients potentiels sont ainsi amenés à remettre de plein gré des données les concernant. Cette collecte commerciale camouflée n'est pas autorisée.

Sociétés de renseignements commerciaux, de renseignements économiques et d'informations sur la solvabilité

Les sociétés de renseignements collectent des informations sur les personnes ne réglant pas une facture à temps, ayant reçu un commandement de payer ou ayant fait l'objet d'une poursuite, et les classent comme insolvables – même s'il y a eu un malentendu. Il peut dès lors vous arriver que l'on vous refuse un contrat de téléphonie mobile ou qu'une société de vente par correspondance vous demande de payer à la livraison.

Un autre type de bureau est susceptible de disposer d'informations sur vos habitudes de paiement, il s'agit des bureaux de recouvrement. Il s'agit d'entreprises privées qui veillent à l'encaissement des factures impayées. Il est à noter que de nombreuses entreprises font office à la fois de sociétés de renseignements et de bureaux de recouvrement.

Les fichiers de ce type comprennent des indications sur le débiteur, mais aussi des données sur le genre de dette, la date à laquelle la dette remonte et le montant. Les indications émanent de sources diverses, notamment de créanciers tels que les banques ou les entreprises de cartes de crédit. Avant de conclure un contrat, les intéressés peuvent s'enquérir auprès de la société de renseignements pour savoir si un futur partenaire est solvable et s'il s'acquitte de ses obligations financières.

Si vous êtes en mesure de prouver que les données vous concernant sont fausses, vous pouvez exiger leur destruction.

2. Les technologies de l'information modernes et leurs risques

2.1. Internet et ordinateur

2.1.1. Web 2.0, une fausse bonne idée

Depuis quelques années, les internautes ne sont plus de simples «consommateurs», mais utilisent l'Internet pour diffuser des informations, des photos, des vidéos, etc. Les sites Internet se font plus dynamiques et interactifs. En jargon informatique, cette évolution répond au doux nom de **Web 2.0**.

Les sites de réseautage social (ou «Social Networking Sites», «SNS» en anglais) gagnent en importances.

Les utilisateurs de ces plateformes créent en général un profil contenant des informations telles que leur adresse, leurs centres d'intérêt ou des photos, ainsi que d'autres informations. Selon les paramétrages choisis, ce profil peut être accessible à tous les internautes. En règle générale, les paramètres par défaut sont tels que les utilisateurs divulguent automatiquement nettement trop de données s'ils ne modifient pas activement ces paramètres. C'est pourquoi il importe de contrôler les paramètres de confidentialité de chaque fournisseur de services et de les adapter individuellement. Il faut parfois octroyer des droits afin de permettre à un certain groupe de personnes d'accéder au profil. Cependant, l'utilisateur divulgue de nombreuses informations personnelles dans les paramètres par défaut, sans en être conscient.

La divulgation active et volontaire par les internautes de nombreuses informations les concernant pose de nouveaux défis à la protection des données. Toute publication sur Internet d'informations sur d'autres personnes sans leur consentement constitue une violation de la vie privée et une infraction à la loi sur la protection des données.

Du point de vue de la protection des données, les points suivants doivent être pris en compte:

- Une grande quantité d'informations, considérées jusqu'ici comme personnelles ou privées, sont divulguées volontairement à un large public par les membres des sites de réseautage.
- Par conséquent, particuliers, entreprises, services de l'administration, etc. peuvent aisément accéder à des données personnelles et dans l'anonymat le plus parfait.
- Les membres des sites de réseautage peuvent également télécharger les données de personnes non membres, les rendant accessibles à un large public qui peut à son tour les utiliser.

Ces sites de réseautage n'ont donc **rien d'anodin**.

- **Internet n'oublie jamais.** les profils utilisateurs peuvent être téléchargés et enregistrés par d'autres utilisateurs. Il est donc pratiquement inutile d'effacer son profil, car les données sont toujours conservées quelque part. Il en résulte un nombre incalculable de collections privées contenant des données dont on ne sait pas ce qu'il advient: le risque est grand qu'elles soient utilisées à d'autres fins que celles prévues initialement
- Les opérateurs des sites de réseautage ont accès non seulement aux données personnelles, mais aussi à d'autres informations: heure et durée de connexion, provenance géographique de l'adresse IP, temps passé sur un même site, navigation à l'intérieur du site, etc.

- Pour beaucoup de ces opérateurs, on ne sait pas vraiment ce qu'ils font de ces données, mais une chose est claire: les données personnelles et autres informations permettent de générer des profils de la personnalité dont la vente est une source potentielle de profits juteux et dont l'utilisation peut être préjudiciable à la personne concernée.
- Reconnaissance automatique des visages: Facebook, Instagram, Google+ et autres permettent à leurs membres de marquer (par des «tags») des amis et des connaissances sur les photos. Lors de la reconnaissance automatique des visages, le système balaye chaque nouvelle photo d'amis d'un utilisateur déjà connus et déjà marqués d'un tag pour proposer un nom. Dans ce cas, un seul clic suffit pour que le nom de l'ami soit désormais visible sur toutes les photos sur lesquels il apparaît. Cette fonctionnalité peut être enclenchée par défaut sur certaines plateformes. Qui ne souhaite pas être marqué d'un tag, doit modifier activement les paramètres de confidentialité.
- Dans la même logique, il est possible d'identifier, par des procédés de **reconnaissance** automatique, les caractéristiques d'arrière-plan d'une photo, comme un tableau ou une maison, et donc de localiser géographiquement le contexte d'une photographie. Il est encore plus simple d'attribuer une photo à un lieu et une date à l'aide des métadonnées. Les métadonnées sont des informations supplémentaires, enregistrées dans le fichier image, telles que des informations géographiques, la date et l'heure auxquelles la photo a été prise.
- Certaines plateformes autorisent également le téléchargement de données de tiers qui ne sont même pas membres du réseau – sans leur demander l'autorisation, s'entend. Cela peut compromettre la sphère privée des personnes concernées, ou leur porter préjudice.
- Les comptes d'utilisateurs ne peuvent pratiquement pas être effacés de manière définitive. D'une part, dans certains cas, on ne peut que les «désactiver» au lieu de les supprimer complètement. D'autre part, les utilisateurs actifs laissent un grand nombre d'informations supplémentaires sur d'autres pages du réseau. Et il est pratiquement impossible d'effacer absolument tout. C'est ainsi que les utilisateurs perdent le contrôle de leurs données.
- On entre comme dans un moulin sur la plupart des sites de réseautage: il suffit de quelques indications personnelles, qui ne sont pas vérifiées et qui peuvent donc être inventées de toutes pièces. Si cela est positif du point de vue de la protection des données, parce que la personne peut ainsi rester anonyme, la situation peut aussi présenter des dangers pour ceux qui entrent en contact avec ce type de personnages «fictifs». Une fois qu'on est sur le site, il est parfois très simple de nouer des contacts et d'être intégré aux cercles d'amis d'autres personnes. Si des personnes mal intentionnées se faisant passer pour des amis et obtiennent malhonnêtement des informations, la situation peut devenir difficile.

L'utilisateur typique d'Android (en anglais uniquement):
http://allthingsd.com/20111229/if-android-were-a-single-person-heres-what-he-would-look-like/

2.1.2. Fichiers de données numériques

Les formulaires d'enquêtes et de concours numériques, notamment réalisés dans le cadre du «Web 2.0» sur de nombreuses plateformes et réseaux de communication, génèrent une quantité de données en circulation considérable. Grâce aux technologies de l'information actuelles, il n'est pas bien difficile de collecter des données personnelles, de les enregistrer, de les analyser, de les systématiser et de les exploiter. Dans la «communauté de l'Internet» (ou «Web community» en anglais), il est presque impossible de ne pas laisser de trace avec ses données, utilisées ensuite à d'autres fins.

Ici aussi, les sociétés cherchent avant tout à générer des recettes publicitaires par des offres adaptées à l'utilisateur. Les risques liés aux technologies numériques modernes font l'objet des chapitres suivants.

2.1.3. Transmission de données par des périphériques de stockage numériques

Les périphériques de stockage mobile, les clés USB notamment, présentent leur lot de risques – souvent sous-estimés. Ils peuvent transmettre des virus et compromettre la sécurité de données personnelles en cas de perte. Ce risque peut cependant être réduit en suivant certaines règles.

Les médias ont rapporté que de nombreuses organisations ont été infectées ces derniers mois par des logiciels malveillants transmis par des périphériques de stockage. Une enquête américaine révèle que la part des transmissions de virus par clés USB a fortement augmenté ces dernières années. Pour que le virus soit transmis, il suffit que le support amovible soit raccordé à l'ordinateur et déjà le logiciel malveillant peut s'incruster sur le disque dur.

LanLine (en allemand uniquement): Points faibles sous-estimés des clés USB
http://www.lanline.de/unterschaetzte-schwachstelle-usb-stick/

Il est pourtant relativement simple de protéger ses données contre les attaques provenant de clés USB

- La fonction «autorun» de clés USB sur l'ordinateur doit être désactivée pour éviter la transmission automatique des données. Ce réglage peut être paramétré en quelques clics dans le panneau de configuration. L'utilisateur peut cliquer «Non» sous «Lecture automatique», afin d'éviter le lancement non sollicité d'une clé USB.
- Nous recommandons par ailleurs un contrôle antivirus régulier de la clé, tout comme du disque dur, ainsi que l'utilisation d'un programme de nettoyage afin d'analyser les données de la clé et de les nettoyer le cas échéant.
- Enfin, pour éviter que des données personnelles ne tombent en de mauvaises mains en cas de perte du périphérique de stockage, il suffit de crypter les données.

Chip.de (en allemand uniquement): UsbFix2017 (Scanner antivirus pour clés USB et disques durs)
http://www.chip.de/downloads/UsbFix-2017_74217923.html

Selbstdatenschutz.info: Crypter les disques durs externes ou les clés USB avec Windows (en allemand uniquement)
https://www.selbstdatenschutz.info/windows/externe_datentraeger_verschluesseln/

2.1.4. Les dangers du flot de données numériques

Au cours des deux dernières décennies, notre vie a été considérablement transformée et – dans le meilleur des cas – simplifiée par l'arrivée du «World Wide Web» et des services liés. Nous communiquons sans problème et en temps réel partout dans le monde. La quantité de données générées et l'échange de données ne sont cependant pas sans danger pour les utilisateurs. Dès leur publication, tous textes, films, photos et informations personnelles transmis sur la Toile perdent leur caractère privé. Une fois sur Internet, les données développent leur propre vie. Elles se répandent, sont reprises par les moteurs de recherche et des archives en ligne (telles que thearchive.org), sont copiées et transmises par d'autres utilisateurs. Il est quasiment impossible de défaire et de supprimer tout ce qui a été fait.

Le World Wide Web n'oublie (presque) rien!

De nombreuses données sont transmises automatiquement, sans que l'on ne s'en rende compte.

Dès que nous nous connections à Internet (de notre domicile avec un ordinateur, ou avec un smartphone), cette connexion est enregistrée par une adresse dite IP (une sorte de «numéro de téléphone» sur Internet). Il est ainsi possible de déterminer exactement qui visite quels sites Internet et combien de temps sous ce numéro. Si l'adresse IP est attribuée à chaque connexion à Internet, le fournisseur d'accès à Internet enregistre toutes les connexions à Internet avec les adresses IP. Il est donc possible à tout moment de connaître les sites consultés, le temps et la fréquence de la visite pour chaque numéro.

L'adresse IP permet à la police d'identifier le malfaiteur en cas d'infraction (téléchargement illégal de musiques, par exemple). Les entreprises enregistrent elles aussi les adresses IP afin de déterminer le cas échéant si un ordinateur a déjà accédé au site Web ou non. En navigant sur Internet, nous laissons donc toujours une **empreinte numérique**, donnant des informations sur nos habitudes de navigation. Par ailleurs, toute navigation sur Internet laisse également des traces sur notre ordinateur ou sur notre smartphone.

2.2. Webtracking

2.2.1. Cookies

Les «**cookies**» («biscuits» en anglais) permettent de créer des profils de données. Les profils contiennent par exemple des informations relatives à nos préférences de navigation, les bannières publicitaires sur lesquelles nous cliquons, ou sur la durée de notre consultation de chaque site ouvert. Le cookie lui-même est un petit fichier qui s'enregistre sur le disque dur lors de la consultation de certains sites Internet. Parfois pratiques, car ils nous permettent de ne pas devoir paramétrer nos préférences spécifiques (la langue du site, par exemple) à chaque nouvelle visite de sites et de ressources, ils sont également utilisés à d'autres fins. Ils peuvent cependant avoir des effets indésirables. Les cookies étant enregistrés de manière invisible, l'utilisateur ne peut généralement pas savoir ce qu'ils contiennent ni ce qu'ils déclenchent: dans de nombreux cas, cela entraîne un flux publicitaire indésirable, axé sur le comportement et le groupe cible.

2.2.2. Intégration de plugins sociaux

Grâce aux plugins sociaux, les exploitants de sites web peuvent utiliser certains services de réseaux sociaux sur leurs propres sites web. Au moyen du bouton «J'aime» de Facebook, par exemple, les internautes peuvent, d'un simple clic, partager un site web sur leur profil Facebook. Les exploitants du site concerné espèrent que celui-ci sera ainsi rapidement connu. Les plugins sociaux permettent aussi d'obtenir des informations statistiques précises sur les utilisateurs du site. Les plugins sociaux déclenchent automatiquement une transmission de données vers le fournisseur concerné. Sur Facebook, par exemple, des données telles que l'adresse IP de l'internaute et l'adresse du site web visité sont transmises dès que l'internaute se rend sur le site,

qu'il ait ou non appuyé sur le bouton «J'aime», qu'il se soit connecté ou non à Facebook ou qu'il dispose ou non d'un profil Facebook. Un cookie installé antérieurement est également transmis, pour autant qu'il existe.

Si l'internaute est connecté au réseau social pendant qu'il surfe, les données de tracking peuvent être directement mises en relation avec lui. S'il clique sur le bouton «J'aime», les informations transmises incluront aussi les contenus qu'il apprécie. Il est ainsi possible d'établir des profils d'utilisateurs détaillés, au moyen desquels de la publicité personnalisée peut être envoyée à l'utilisateur et à son cercle d'amis dans le réseau social.

2.2.3. Ce que les utilisateurs peuvent faire contre le webtracking

Il est recommandé de supprimer après chaque session les **cookies enregistrés et l'historique de navigation**, ou de configurer le navigateur de telle manière qu'il procède automatiquement à cette opération après avoir été fermé.
L'utilisateur a de plus la possibilité d'empêcher l'enregistrement de cookies tiers partie dans son navigateur. Cette stratégie n'est cependant d'aucune utilité face aux «flash cookies», qui sont enregistrés sur l'ordinateur même et non dans le navigateur. Ces cookies doivent être désactivés dans l'**outil de gestion des réglages de Flash Player**, qui se trouve dans le panneau de configuration, dans la mesure où le Flash Player est installé.
L'installation de petits **paquets de logiciels («add-ons»)** dans le navigateur permet à l'utilisateur d'observer quels services de webtracking suivent ses mouvements sur la Toile – et selon le produit choisi, ces services peuvent être bloqués de manière spécifique. Cependant, il convient de rester prudent avec ces petits programmes: des applications prétendument utiles peuvent contenir des chevaux de Troie qui prélèvent des fichiers. Conseil: ne télécharger que des applications provenant de sources dignes de confiance, procéder régulièrement à des mises à jour et supprimer les applications que l'on utilise plus.
De nombreux navigateurs sont aujourd'hui munis d'une fonction «**Do not track**», qui peut être réglée dans le navigateur et permet de signaler que l'on ne souhaite pas être soumis à un webtracking.
L'utilisateur n'est cependant pas en mesure de voir directement si l'autre partie s'y tient. Du point de vue de la protection des données, le non-respect d'une telle déclaration d'opposition constitue une atteinte illicite à la personnalité.

Voir PFPDT, Explications concernant le webtracking
https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/webtracking/explications-concernant-le-webtracking.html

2.3. Réseaux sociaux et chats

Exemples: Facebook, Instagram, Snapchat, Twitter, Pinterest, etc.

Qui souhaite utiliser autant de fonctions que possible sur les réseaux sociaux est rapidement tenté de divulguer autant d'informations personnelles que possible. La personne peut alors de devenir identifiable et risque notamment d'être contactée de manière non sollicitée. Voici donc toute la distance entre le réseau social et la vie privée: «Je dois me montrer pour être de la partie» – une nouvelle forme de pression sociale.

Désormais, tous les réseaux sociaux proposent des paramètres de visibilité des informations privées, permettant à l'utilisateur de décider du DEGRÉ de visibilité des informations, ainsi que des INFORMATIONS consultables et par QUI.

Le graphique ci-dessous montre l'importance actuelle des réseaux sociaux dans paysage numérique.

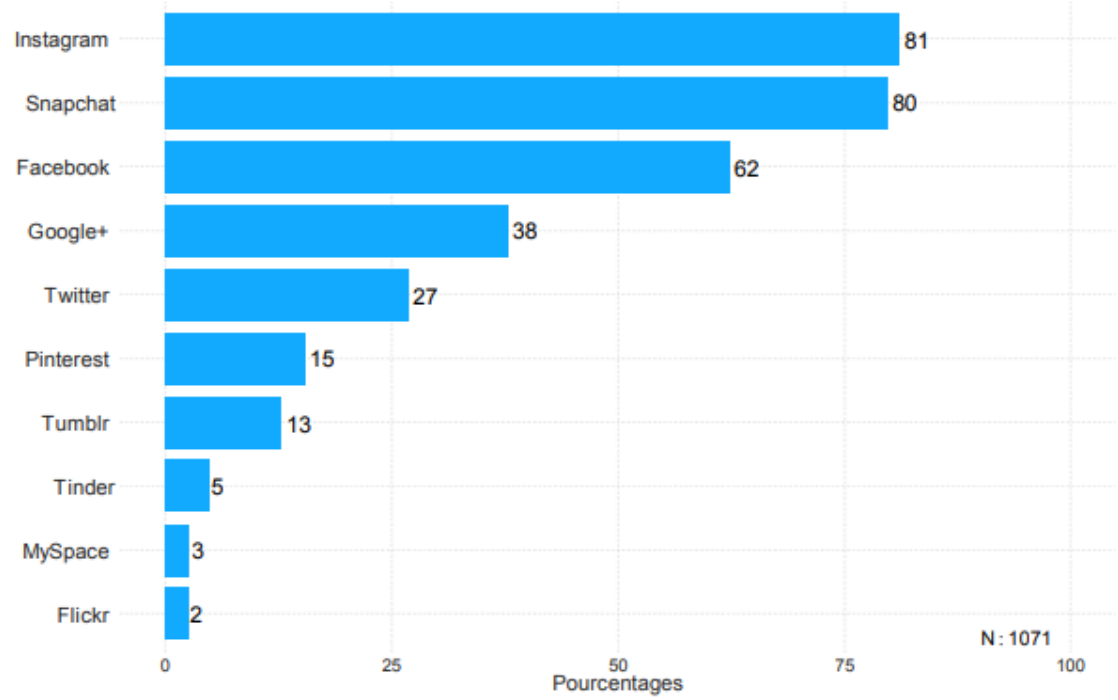

Figure 42: Comptes sur les réseaux sociaux

(Source :https://www.zhaw.ch/storage/psychologie/upload/forschung/medienpsychologie/james/2016/Rapport_JAMES_2016.pdf)

Là où le bât blesse, c'est qu'il existe toujours des réseaux sur lesquels l'utilisateur doit activement modifier les paramètres de sécurité relatifs à la protection de la vie privée après son inscription sur le réseau. Il serait cependant souhaitable que les paramètres soient par défaut ceux du plus haut niveau de sécurité lors de l'inscription, pouvant être assouplis par la suite au souhait de l'utilisateur («Privacy by default»).

Que faire cependant si une panne technique révèle des photos ou des commentaires, destinés à quelques amis seulement? C'est ce qu'à appris à ses dépens le visionnaire et fondateur de Facebook, Mark Zuckerberg, en 2011: certaines de ses photos privées ont été brièvement visibles pour le monde entier – et se retrouvent désormais ailleurs sur la Toile.

Zuckerberg victime d'un bug de Facebook
http://geeko.lesoir.be/2011/12/07/12688/

2.3.1. Quelles sont les données collectées par Google?

Fin des années 90, deux étudiants en informatique créaient l'entreprise «Google», principalement connue pour son moteur de recherche. Désormais, Google propose cependant un grand nombre d'autres services en ligne populaires. Voici quelques exemples de données que nous mettons à la disposition de Google, volontairement ou non:

Recherche Google:
Code pays
Recherches
Adresse IP
Langue
Nombre de résultats
Safe search enclenché ou non
Clis sur des liens obtenus
après recherche
Cookies / type de navigateur

Youtube:
Toutes les vidéos envoyées
Tous les commentaires
Vidéos renseignées
Chaîne
Vidéos visionnées
Transfert des données
Déplacement
Pays
Cookies / type de navigateur

Blogger:
Photos utilisateur
Date de naissance
Pays
Transfert des données
Taille des données
Clics
Publications

Compte Google:
Date d'enregistrement
Nom d'utilisateur
Mot de passe
Adresse e-mail alternative
Pays
Nombre de connexions
Services Google utilisés
Cookies / type de navigateur

Pour les utilisateurs inscrits:
Adresse e-mail
Mot de passe
Nom d'utilisateur
Préférences
Groupes
Contacts

Documents Google:
Adresse e-mail
Nombre de connexions
Nombre d'actions
Taille des données
Clics
Tous les textes
Toutes les images
Toutes les modifications
Données d'inscription

Barre d'outils Google
Sites Web consultés (tous)
Toutes les pages 404
Fonction de synchronisation
Avec le compte Google

Traducteur Google
Tous les textes traduits
Cookies / type de navigateur

GMail
Tous les e-mails
Toutes les activités du compte
Espace de stockage
Nombre de connexions
Liens suivis
Listes de contacts
Flux de données
Taille des données

Conclusion:
Il s'agit là de quelques services proposés gratuitement. Nous devons toujours garder à l'esprit que ces services ne sont jamais vraiment «gratuits» – nous les payons avec nos données. Le fait est que Google & Cie collecte de nombreuses données. Si cela est parfois nécessaire au bon fonctionnement de certains services, cette façon de faire permet également de trier et de catégoriser les utilisateurs recourant à de nombreux services. Des profils de la personnalité très

détaillés peuvent alors être créés. En premier lieu, ces données sont utilisées à des fins de personnalisation de la publicité qui vous est envoyée. La recherche Google optimise les résultats de la recherche à l'aide du profil. La personne réalisant la recherche obtient ainsi plus rapidement un résultat, car elle est catégorisée par son profil. La question qui se pose ici est celle de la volonté de l'utilisateur d'être catégorisé de la sorte et de se voir proposer une sélection de résultats générée par ordinateur.

2.3.2. Pourquoi Facebook collecte-t-il des données utilisateurs?

La plateforme de communication Facebook permet à des personnes du monde entier d'échanger des idées, sans se limiter à leurs loisirs et à leurs opinions sur l'évolution du monde. Au contraire: de nombreux utilisateurs de Facebook y recourent comme mémoire personnelle ou comme archive photo accessible du monde entier. Enfin, pour les personnes «mobiles», la plateforme offre une possibilité apparemment avantageuse de rester en contact: un accès à Internet suffit. Pour comprendre pourquoi Facebook collecte des données – même supprimées – des utilisateurs, il convient de se pencher sur l'historique de l'entreprise et de comprendre son modèle commercial.

Facebook comme plateforme publicitaire

La plupart des offres publicitaires sur Internet ont le défaut d'être proposées de manière généralisée à toute personne se trouvant sur un certain site Web. La plupart des publicités publiées sur Internet, que ce soit sous la forme d'une bannière ou d'un lien, restaient donc non lues, car elles étaient trop peu spécifiques à l'utilisateur. L'idée qui se cache derrière le réseau social Facebook est de personnaliser la publicité. Dès que l'utilisateur donne des informations sur sa profession et ses loisirs, il reçoit de la publicité correspondante, soit directement sur la page du profil d l'utilisateur, soit – s'il a accepté de recevoir des offres par d'autres canaux – par e-mail ou d'autres plateformes de communication. De cette façon, l'annonceur évite de payer des clics superflus. Etant donné que chacun se connecte à Facebook avec un nom qu'il a lui-même choisi, la société sait à tout moment qui se trouve à l'ordinateur. D'autres indications, telles que le domicile, la profession et l'âge permettent également d'estimer le revenu. Les annonceurs apprennent ainsi les indications d'âge, le groupe de revenu et, selon les informations fournies par l'utilisateur, les intérêts de chacun.

Chaque clic permet à Facebook de mieux connaître l'utilisateur

Les fameux boutons «J'aime» permettent à Facebook d'en savoir chaque fois un peu plus sur l'utilisateur – donc sur nous et nos intérêts. Si nous nous passionnons pour les croisières, une croisière de luxe ou une croisière club peuvent être proposées. Partant, toutes les données historiques valent argent comptant. Chaque clic rend le profil de l'utilisateur plus transparent et plus intéressant pour l'industrie publicitaire. C'est ce qui fait la véritable valeur de Facebook. A propos: ne serait-ce qu'en ouvrant une page Internet avec le bouton «J'aime», des données sont envoyées à l'entreprise et reliées au profil connecté.

Des opérations de suppression trop fréquentes font perdre à Facebook sa valeur

Une enquête sur la protection des données chez Facebook déclenchée par un étudiant viennois s'attaque presque à la nature même de l'entreprise. Si les informations collectées jusqu'ici peuvent être simplement supprimées, l'utilisateur reprend en partie le contrôle sur son profil.

Pour l'industrie publicitaire, Facebook n'a d'intérêt que si la plateforme dispose d'informations complètes. Entre temps, la société a révélé qu'il n'est pas donné suite à la demande de l'utilisateur de supprimer ses données. Celles-ci ne sont pas vraiment supprimées du centre de calcul, mais désactivées, c'est-à-dire rendues «invisibles».

Que peuvent faire les utilisateurs de Facebook pour y remédier?
Il incombe à chacun d'analyser personnellement la situation. Chacun doit décider pour lui-même de la quantité d'informations qu'il communique et dans quel but. Pour mener une vie indépendante, il vaut mieux faire preuve de parcimonie en ce qui concerne les adresses, photos, intérêts, ainsi que l'expression d'opinions. Il convient en tout cas de ne pas envoyer de données personnelles et de ne pas réaliser d'opération commerciale si vous êtes inexpérimenté. Quoi qu'il en soit, lire les CGV – et particulièrement les dispositions de protection des données d'un service en ligne – est indispensable.

Attention:
Chacun d'entre nous prend une décision personnelle: Quelle importance est-ce que j'accorde à la liberté et à l'avantage d'une utilisation confortable (presque) gratuite? Il faut également réfléchir aux informations avec lesquelles nous souhaitons toujours être confrontés dans cinq ans.
En effet, Internet n'oublie jamais. Il incombe à chacun de décider.

2.3.3. Recherches et falsification de profils

Des personnes entrant en contact avec d'autres, quel qu'en soit le motif, notamment un employeur actuel ou futur, peuvent rechercher la personne sur Google et étudier ses profils de réseaux sociaux.
Toutes les informations relatives à d'autres personnes et disponibles sur Internet ne sont pas à leur avantage.
Cependant, des profils peuvent être falsifiés, ce qui peut s'avérer très désagréable pour la personne concernée. Contrôler son propre nom sur des moteurs de recherche spécialisés sur les réseaux sociaux, tels que www.yasni.ch peut contrer ce type d'abus. Il convient de demander à l'exploitant des sites Web publiant de fausses informations de supprimer les pages correspondantes ou de corriger les indications.

2.3.4. Intentions criminelles

Les données du titulaire du profil peuvent tomber entre les mains de personnes déloyales ou criminelles. Le manque de protection des données ou la manipulation négligente des informations peuvent avoir des conséquences indésirables.

2.3.5. Hameçonnage («phishing»)

On appelle «phishing» les tentatives de malfaiteurs d'obtenir les données d'un internaute (données de profils, par exemple), afin de voler son identité et de lui nuire sur des adresses Internet, e-mail ou de messagerie instantanée falsifiées (pillage d'un compte, par exemple).

Le vol de données sur Internet pour s'approprier une identité tierce peut avoir des conséquences graves pour la victime – de nature financière ou de réputation. La prudence est donc de mise, particulièrement dans le domaine de la banque et du commerce en ligne, mais aussi des sites de rencontre.

2.3.6. Achats en ligne

Le domaine des achats en ligne, où le phishing peut devenir un véritable problème, présente plus d'un danger. Aujourd'hui, presque tout peut s'acheter sur Internet, et les offres alléchantes attirent le chaland numérique. Pour que cette expérience ne tourne pas à la frustration, il convient de vérifier le sérieux des boutiques en ligne pour chaque achat. Il convient d'être particulièrement vigilant lors d'achats à l'étranger. Si l'on ne risque pas grand-chose sur les sites connus, l'internaute serait bien avisé de lire attentivement les conditions générales de vente de sites relativement méconnus. Le mode de paiement permet également de se faire une idée du sérieux du prestataire.

Conseils pour se protéger contre la fraude et l'escroquerie sur les sites marchands – ouvrezloeil.ch
https://www.ouvrezloeil.ch/fr/fraude_et_vol_de_donnees#!escroquerie_sur_les_sites_d_achats_en_ligne_et_de_ventes_aux_encheres

Prévention de l'escroquerie sur Internet – skppsc.ch
https://www.skppsc.ch/fr/sujets/internet/fraude-en-ligne/?noredirect=fr_FR

Achats en ligne – les risques associés aux achats et aux enchères en ligne
https://www.pensezcybersecurite.gc.ca/cnt/rsks/nln-ctvts/shppng-nln-fr.aspx

Phishing – (hameçonnage ou filoutage)
https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage-ou-filoutage

Petites histoires d'Internet – Office fédéral de la communication (OFCOM)
http://www.thewebsters.ch/fr/

Attention aux arnaques sur Internet! (brochure) – Secrétariat d'Etat à l'économie (SECO)
https://www.seco.admin.ch/seco/fr/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Werbe_und_Geschaeftsmethoden/Unlauterer_Wettweberb/vorsicht-vor-internetfallen-.html

2.4. Dangers concrets et conséquences juridiques

2.4.1. Cyberharcèlement («cyberstalking»)

On parle de cyberharcèlement lorsque les possibilités de nouer des relations sur les sites de réseautage sont utilisées par des personnes mal intentionnées pour harceler quelqu'un. En outre, vu la quantité de données personnelles dévoilées par les utilisateurs, le harceleur a toutes les chances de trouver l'adresse de sa victime, de connaître son emploi du temps et de la persécuter physiquement.

Police municipale de Zurich, Schaugenau.ch – Cyberharcèlement (conseils et mesures possibles)
https://www.ouvrezloeil.ch/fr/harcelement

2.4.2. Cybermobbing

On parle de cybermobbing lorsqu'un internaute est harcelé, brimé, voire terrorisé sur une longue durée par d'autres internautes – généralement des enfants ou des adolescents La victime est confrontée à des photos ou des vidéos truquées, humiliantes ou très personnelles, à des vexations publiées sur l'Internet. Là encore, les fauteurs de trouble peuvent s'inscrire sur les communautés en ligne (telles qu'Instagram ou Facebook) pour causer du tort à leurs victimes, avec des conséquences souvent redoutables.

Le cybermobbing et le droit

- Toute publication de vidéos ou de photos sans autorisation viole le droit à l'image.
- Toute personne harcelant ou insultant régulièrement une autre personne, que ce soit par e-mail, messagerie instantanée, SMS ou par tout autre canal, peut se rendre punissable.
- Si des forums, des réseaux sociaux ou des blogs sont utilisés à des fins de déclarations mensongères ou d'insultes, les victimes peuvent faire valoir des prétentions civiles en prévention ou déposer plainte pour calomnie/diffamation. Quel que soit le moyen utilisé, le harcèlement, la menace, le chantage la diffamation, la coercition et la contrainte, exercés en privé ou en public, constituent des délits. **Il convient de signaler ces cas à la police.**

2.4.3. Cyberintimidation

Ce phénomène consiste à tyranniser quelqu'un de manière répétée en publiant sur la Toile des insultes ou des humiliations, voire des menaces. Le terme «bullying» peut aussi être rendu par brimades, brutalités ou mauvais traitements.

Qu´est-ce que le cyberintimidation ?
https://www.pensezcybersecurite.gc.ca/cnt/cbrbllng/prnts/cbrbllng-fr.aspx
L´enfer du harcèlement entre ados sur internet
https://www.24heures.ch/vaud-regions/enfer-harcelement-ados-internet/story/15226514

2.4.4. Sexting et sextortion

«Le sexting (appelé textopornographie selon FranceTerme ou sextage selon l'Office québécois de la langue française) est l'acte d'envoyer électroniquement des textes ou des photographies sexuellement explicites, en français des « sextos », surtout d'un téléphone portable à un autre. Le terme est apparu en 2005 en Australie dans un article du journal The Daily Telegraph (édition magazine du dimanche).»

Wikipédia https://fr.wikipedia.org/wiki/Sexting

Si la communication privée sur des thèmes sexuels ne constitue pas, en soi, un délit, il convient de tenir compte des dangers qu'elle entraîne:

- Toute personne diffusant des photos ou des films de soi se rend punissable si le matériel transmis comporte une représentation d'actes sexuels impliquant de la violence ou des animaux. Il s'agit de pornographie illégale.
- La représentation de sexe entre mineurs (personne de moins de 18 ans) ou des représentations aguichantes des mineurs sont considérées comme de la pédopornographie et entraînent des conséquences pénales. Les personnes de moins de 18 ans doivent impérativement en être informées.

- Sont considérées comme pédopornographiques toutes représentations d'actes sexuels avec des mineurs (personnes de moins de 18 ans). Toutes représentations à caractère sexuel de mineurs – même en l'absence d'actes sexuels – sont interdites, donc également les selfies de poses non équivoques. Il est interdit de créer des documents pédopornographiques, d'en regarder, d'en détenir ou d'en envoyer. Le sexting peut être de la pédopornographie!

(Source en allemand uniquement: https://www.lilli.ch/sexting_kinderpornografie/)

Site web Pornographie illégale – skppsc.ch
https://www.skppsc.ch/fr/sujets/abus-sexuel/pornographie-illegale/

Brochure Pornographie: Agir de bon droit – skppsc.ch
https://www.skppsc.ch/fr/wp-content/uploads/sites/5/2016/12/droitpornograhie.pdf

- Le risque principal du sexting réside dans la rapidité de diffusion des contenus et la difficulté à les supprimer. En un seul clic, une image ou une vidéo compromettante peut se retrouver sur Internet et y rester pour toujours. Même s'ils ont été envoyés consciemment – à une personne de confiance ou sous l'effet de la pression du groupe – ils peuvent devenir la source de beaucoup de souffrance s'ils atterrissent entre des mains malintentionnées et/ou sont largement diffusés.
- La «Sextortion» est une forme d'extorsion en lien avec le sexting. Sous une fausse identité, un adulte se procure des images osées d'adolescents via les réseaux sociaux ou Internet. Puis, il menace de rendre ces images publiques, afin d'obtenir davantage d'images (striptease devant la webcam par exemple), de l'argent ou une rencontre.

(Source: https://www.jeunesetmedias.ch/fr/opportunites-et-risques/risques/sexting.html)

Conclusion:
On ne le dira jamais assez souvent: Internet n'oublie jamais! Il convient donc de toujours bien réfléchir avant d'octroyer l'accès à des photos envoyées à tout un chacun, car on ne peut jamais exclure leur publication, qu'elle soit voulue ou non. Ce qui est téléchargé une fois sur Internet peut resurgir à tout moment. Vous trouverez aide et conseil auprès de Pro Juventute (tél. ou SMS au 147 ou sous 147.ch), d'un centre de consultation cantonal pour l'aide aux victimes, mais aussi auprès d'un assistant social, d'un enseignant et bien entendu de vos parents ou de toute autre qui vous est proche (famille ou amis proches). Il importe que les cas soient abordés et découverts, afin que des mesures puissent être prises et que le matériel publié puisse être retiré d'Internet, et afin d'éviter toute autre incursion.

Liste d'adresses pour l'aide aux victimes
http://www.sodk.ch/fr/domaines/famille-et-societe/aide-aux-victimes/wwwaide-aux-victimesch/liste-dadresses/

2.5. Smartphones

Aujourd'hui, un smartphone dispose de nombreux programmes supplémentaires. Certaines de ces applications peuvent être obtenues gratuitement dans un premier temps, avec une option payante proposant plus de possibilités ou l'absence de publicité. Certaines applications entraînent

des coûts d'abonnement régulier. Les applications collectent des données relatives à l'utilisateur, sans que celui-ci ne le sache ni ne puisse rien y faire. Les données collectées sont par exemple le lieu, l'heure et la fréquence d'utilisation de programmes, ainsi que les SMS et les données de contact enregistrées. C'est notamment le cas d'Instagram et de Facebook, qui ont un accès complet aux données de l'appareil, y compris aux données géographiques et de SMS.

2.5.1. Géolocalisation – malédiction ou bénédiction?

Lors de la géolocalisation, un numéro IP ou d'autres adresses d'identification sont attribués à la position géographique. Une autre possibilité de déterminer l'emplacement de l'utilisateur est l'accès par GPS ou réseau sans fil. Ce qui peut s'avérer judicieux sur des ordinateurs et rend le fonctionnement de certaines applications possible – application de navigation, par exemple – doit être considéré d'un œil critique sur les smartphones.

Si informer d'autres personnes de l'endroit où l'on se trouve est un phénomène en vogue, il n'est pas dénué de danger. Ce faisant, nous divulguons par exemple si nous sommes chez nous ou non, ce qui peut intéresser des cambrioleurs.

Il convient de toute façon de se demander si le monde entier doit savoir à tout moment où un utilisateur se trouve. Le danger majeur lié à l'utilisation de la fonction de localisation des services en ligne et des applications est dû au fait que la technique de localisation peut également être utilisée pour créer des profils de déplacement. Même si ces profils ne se rapportent pas toujours à une personne, les données de nombreux internautes et utilisateurs de smartphones représentent un moyen intéressant d'étude de marché et beaucoup d'argent pour l'industrie.

L'historique des positions Google: Google enregistre votre profil de déplacement. Voici comment le supprimer (en allemand uniquement):
http://www.journaldemontreal.com/2015/10/27/google-enregistre-tout-ce-que-vous-lui-dites-voici-comment-ecouter-et-effacer-vos-recherches

2.5.2. Droit pénal

Certains contenus sont généralement interdits et punissables: c**ontenus diffamatoires, incitant à la haine raciale et dangereux pour la jeunesse**. Le seul fait de cliquer sur des liens de ce type sur Internet peut être punissable. Il convient d'en tenir compte lors de la transmission de contenus «délicats», et pas seulement sur Internet, mais par exemple aussi d'un téléphone mobile à un autre. Important: La transmission de pornographie aux moins de 16 ans est interdite!

2.6. Appels vidéo

Exemples: Skype, FaceTime, Google Hangouts, Viber

Depuis quelques années, les appels vidéo a jouent un rôle de plus en plus important dans la communication. Que l'usage soit professionnel ou privé, de nombreuses personnes communiquent désormais non seulement verbalement et par écrit, mais aussi par transmission d'image et de son. Différents prestataires ont pris ce train en marche et ont élargi leur offre de communication à l'option d'appels vidéo.

Lors du choix du service de messagerie, il convient cependant de vérifier certains points:

- Les contenus sont-ils cryptés pour leur transmission?

- Ces contenus sont-ils à l'abri de l'indiscrétion du prestataire; les clés de décryptage sont-elles enregistrées sur les appareils, et non sur un serveur?
- D'anciens messages peuvent-ils être retrouvés en cas de seule protection par une clé éphémère (mots de passe à durée de validité limitée, par exemple)?

(Source en allemand uniquement: http://www.zeit.de/digital/datenschutz/2014-11/messenger-sicher-vergleich-eff)

Outre le prestataire, il convient également de bien choisir son interlocuteur. Les chats avec des inconnus sont critiques dans la mesure ou l'image et le son peuvent être enregistrés, sans que la personne concernée le remarque. Des données sensibles, des déclarations personnelles et du matériel visuel compromettant ne doivent donc pas être envoyés ni montrés par chat vidéo.

Skype: les chats anonymes compromettent la vie privée (en allemand uniquement)
http://www.onlinewarnungen.de/warnungsticker/skype-anonyme-chats-gefaehrden-die-privatsphaere/

2.7. Images et droits d'image

2.7.1. Publier encore rapidement quelque chose? (Le droit à l'image)

Si des photos ou des films sont réalisés avec un smartphone ou un téléphone mobile et que ce matériel est téléchargé sur Internet sans y réfléchir, l'utilisateur risque vite de **violer le droit à l'image** si des personnes y sont identifiables.

Indépendamment des considérations liées au droit d'auteur, la personne que l'on souhaite photographier possède un droit à l'image, qui lui permet en règle générale de s'opposer à la fixation et à la diffusion de son image ou de les soumettre à des conditions. Aussi n'est-il a priori licite de publier une photo qu'une fois que les personnes représentées ont donné leur consentement.

Un consentement n'est pas nécessaire

- si les personnes sont photographiées de manière «accessoire» dans le paysage ou dans l'espace public
- si les personnes participantes sont au premier plan
- si les photos montrent des personnalités de l'histoire contemporaine (et donc des personnes célèbres).

Autrement dit, il convient de faire attention lors de fêtes, de concerts et de soirées en discothèque: toutes les photos et tous les films ne peuvent pas être publiés sur la Toile sans autorisation!

Il est par ailleurs conseillé de faire preuve de sens critique lors de la publication de photos personnelles: «dans le feu de l'action», l'utilisateur risque d'autoriser trop rapidement que certaines photos peut-être délicates atterrissent sur un portail de commérage ou un réseau social. Les selfies doivent, eux aussi, faire l'objet de prudence.

A propos: seul le photographe a le droit de les publier. Publier une photo sans demander à l'auteur n'est pas autorisé – peu importe le nombre de fois que la photo est déjà disponible sur Internet.

2.7.2. Photos de groupe

Les photos de groupe sont elles aussi susceptibles de porter atteinte aux droits de la personnalité des personnes représentées, si elles sont reconnaissables. Cette atteinte sera moins grave si aucune personne en particulier ne se détache du groupe pour être perçue comme telle.

2.7.3. Prises de vue effectuées dans l'espace public

En ce qui concerne les photos prises dans l'espace public, si elles sont prises au su de toutes les personnes présentes et si les personnes représentées sur les photos n'en constituent pas le sujet principal (par ex., s'il s'agit de simples passants à proximité d'une curiosité locale), il est suffisant de supprimer la photo sur demande de la personne photographiée (immédiatement ou plus tard) ou de renoncer à sa publication. Il n'y a pas lieu cependant de les aborder exprès pour les informer de leurs droits.

2.7.4. Autorisation juridiquement valable

Dans tous les autres cas, on s'assurera du consentement des personnes concernées, qui pour être valable devra avoir été donné librement et en connaissance de cause. Si une personne s'oppose à cette publication, on se conformera à sa décision.

S'il s'agit de photographier une personne en particulier, la procédure sera différente, car l'autorisation générale décrite ci-dessus ne sera pas suffisante. La personne doit ici avoir la possibilité d'examiner les photos qu'il est prévu de publier, et elle devra être informée du contexte de la publication prévue. Il faut enfin ne pas perdre de vue que si la photo a pour sujet des mineurs, il faut également s'assurer du consentement des personnes qui ont l'autorité parentale.

2.7.5. Conséquences possibles d'une publication effectuée sans motif légitime

Toute personne dont la photo a été publiée sans motif légitime peut à tout moment s'y opposer et faire valoir ses droits, au besoin en intentant une action civile. Si le juge conclut à une atteinte illicite à la personnalité au motif que la ou les photos ont été publiées sans le consentement de la personne ou en l'absence d'intérêt public ou privé prépondérant, il peut ordonner, en plus de l'obligation de retirer ou de détruire les images, le versement d'un dédommagement ou même d'une indemnité pour tort moral.

(Source: https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/publication-de-photographies.html)

2.8. Autres technologies

2.8.1. Communication de données dans un nuage

Exemples: iCloud, One Drive, Dropbox

L'externalisation de données dans un nuage (ou «cloud») présente l'avantage pour l'utilisateur de ne pas utiliser l'espace de stockage local de son ordinateur de bureau ou portable, ni de son smartphone, mais d'enregistrer les données en ligne. De nombreuses applications utilisent automatiquement cette possibilité d'enregistrement et téléchargent certains contenus de l'utilisateur du téléphone mobile dans un nuage, parfois même à l'insu de l'utilisateur. Ainsi, certaines applications photo (Google Photos) enregistrent directement les photos sur le nuage après leur prise, dans la mesure où cette fonction n'a pas été désactivée par l'utilisateur.

Les risques de l'utilisation de nuages:

- **Perte de contrôle sur les données:** L'interconnexion mondiale et l'utilisation de la mémoire virtuelle font qu'il est souvent impossible de localiser les données, notamment lorsqu'on a recours à des nuages publics. L'utilisateur du nuage ne sait donc pas où les données qu'il a déposées dans le nuage sont enregistrées et traitées. Il ignore souvent si des sous-traitants interviennent et s'ils veillent à une protection adéquate des données.

- **Accès d'autorités étrangères aux données:** Dans de nombreux cas, les données destinées à être traitées dans le nuage sont communiquées à l'étranger. Elles sont alors souvent enregistrées ou traitées dans des pays qui ne leur assurent pas une protection suffisante. Les prestataires de services en nuage peuvent se voir ordonner par des autorités ou des tribunaux étrangers de donner accès aux données enregistrées dans le nuage, même si ces données ne sont pas traitées ou enregistrées dans le pays en question.

Les risques ci-dessous se posent toujours, que les données soient traitées dans un nuage ou non.

- **Perte de données:** Les données en nuage peuvent être volées, effacées, écrasées par erreur ou subir d'autres modifications entraînant leur perte.

- **Pannes de système et de réseau** et non-disponibilité des ressources et des services loués, qui peuvent entraîner des pertes de données ou impliquer l'accès de personnes non autorisées aux données (la confidentialité, la sécurité et l'intégrité des données ne sont alors plus garanties).

Conclusion:

L'utilisateur du nuage doit bien choisir les applications et les données qui peuvent être délocalisées dans un nuage et celles qui doivent rester sur ses propres serveurs.
(Source: https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/cloud-computing/explications-concernant-l-informatique-en-nuage--cloud-computing.html)

2.9. «Internet des objets»

L'Internet des objets désigne la connexion des objets à Internet, afin de leur permettre de communiquer de manière autonome par Internet et donc d'exécuter diverses tâches pour leur propriétaire. Le domaine d'utilisation s'étend de la fourniture d'informations aux fonctions d'alerte et d'urgence, en passant par les commandes automatiques.

(Source en allemand uniquement: http://wirtschaftslexikon.gabler.de/Archiv/1057741/internet-der-dinge-v4.html)

Exemples: bracelets de fitness, appareils électroménagers connectés (thermostat, compteur électrique, Smart TV, imprimante, jouets avec micro ou caméra, par exemple)

(Source: Pixabay / Pixabay)

De nombreux appareils et fonctions électroniques de l'Internet des objets par leur connectivité n'apportent pas d'aide réelle au quotidien. Même s'ils facilitent la vie à première vue et exécutent même certaines tâches de manière autonome, il convient, ici aussi, de rester sceptique.
Pour que notre vie dépende par de ces appareils, nous devons être certains qu'en plus de nous appartenir, ils nous obéissent. Ce n'est pas toujours chose aisée.
Si ces appareils sont connectés à Internet, ils ne sont généralement pas suffisamment protégés.
Certaines fonctions sont même voulues: les téléviseurs renseignent aux chaînes ce que nous regardons à quel moment ou nous écoutent, les haut-parleurs enregistrant les conversations tenues dans notre salon.
Si vous souhaitez acheter un de ces objets connectés, réfléchissez aux points suivants – bien avant de réfléchir aux fonctions du produit et au choix du fabricant:

1. Ai-je vraiment besoin de l'appareil ou ne l'ai-je pas déjà (ne puis-je l'emprunter) sous une autre forme, peut-être moins attrayante? Le but principal de l'appareil est-il peut-être de pavaner, d'avoir l'air cool ou de vouloir être de la partie?

2. Ai-je vraiment besoin des fonctions connectées? En ai-je également besoin s'il est entièrement pilotable à distance par un malfrat? Imaginez le pire et partez du principe que le malfaiteur a encore beaucoup plus d'imagination que vous. Les fonctions supplémentaires valent-elles le prix et le risque accru?
3. Si la fonction connectée devait être supprimée (le fabricant met fin à son service d'informatique en nuage) ou doit être désactivée (questions de sécurité): puis-je continuer à utiliser l'appareil?

(Source en allemand uniquement: http://www.pctipp.ch/tipps-tricks/kummerkasten/sicherheit/artikel/weg-vom-internet-der-unsicheren-dinge-87430/)

Internet des objets – le préposé à la protection des données déplore le manque de transparence, NZZ, 12.09.2016 (en allemand uniquement)
https://www.nzz.ch/schweiz/aktuelle-themen/internet-der-dinge-datenschuetzer-moniert-fehlende-transparenz-ld.116181

Conseils pour bien manipuler ses données

2.10. Principes

Un traitement minutieux des données et des informations:

- Divulguer le moins de données personnelles possibles, et jamais plus que le strict nécessaire
- Dans le cas de formulaires (concours, etc.) et de profils en ligne, faire preuve de parcimonie avec ses données personnelles – économiser les données!
- Dans la mesure du possible, ne pas renseigner d'adresse, de numéro de téléphone ni d'âge (surtout pour les enfants)

Respect: la règle d'or (un principe d'éthique pratique)

- «Traite les autres comme tu aimerais toi-même être traité(e).»
- «Ne fais pas à autrui ce que tu ne voudrais pas qu'on te fît.»

2.11. Conseils concrets

2.11.1. Conseils de sécurité généraux

- Garantir une utilisation de **mots de passe sécurisés** – 8 caractères minimum, combinant majuscules et minuscules, chiffres et lettres – ainsi que leur conservation en lieu sûr
- Utiliser pour chaque service un mot de passe différent (il existe des gestionnaires de mots de passe utiles, tels que KeePass, parce que l'on ne peut pas se souvenir d'un tel nombre de mots de passe)
- Veiller à une configuration sécurisée du navigateur Internet, c'est-à-dire utiliser des paramètres préservant la vie privée
- Supprimer régulièrement les cookies
- Supprimer l'historique du navigateur, notamment sur des ordinateurs publics
- Utiliser un logiciel antivirus et l'actualiser régulièrement
- Utiliser des logiciels/sources de fournisseurs dignes de confiance (notamment dans le cas de modules d'extension – ou «add-ons») – être vigilant avec les programmes gratuits.
- Utiliser la **version actuelle des logiciels** et procéder régulièrement à des mises à jour
- Recourir à des techniques de cryptage lors du transfert de données (veiller à la présence d'un cadenas vert dans la barre d'adresse; celui-ci indique une connexion cryptée)

2.11.2. Réseaux sociaux

Exemples: Facebook, Instagram, Google+, Youtube

- Chacun est responsable de la protection de sa vie privée!
- Il convient de faire attention à la manière de se présenter sur la Toile.
- Attention: tout ce que nous écrivons, publions, connectons, etc. donne des informations à notre sujet.

- Des photos humiliantes et des informations très personnelles n'ont pas leur place sur la Toile. Elles divulguent de nombreuses informations personnelles et peuvent vous coûter votre place de formation ou vous causer des ennuis.
- Réfléchir à l'image que donne de nous une adhésion à un groupe
- Etre vigilant avec les données de profil: mieux vaut éviter de donner son adresse, numéro de téléphone, adresse e-mail, etc.
- Paramétrer le profil pour qu'il soit privé. Seuls des amis doivent pouvoir voir les informations.
- Contrôler si les «amis en ligne» sont de vrais amis avant de leur donner libre accès à des photos et des données privées. On ne peut jamais savoir comment ils utiliseront ces informations!
- Ne publier des contributions qu'après avoir bien vérifié et réfléchi au contenu.
- Eviter les émotions et prises de position (trop) négatives. Nous regrettons souvent des réactions écrites sous le coup de l'émotion.
- Ne télécharger des photos, adresses et autres données (ainsi que des marquages sur des photos) d'amis, connaissances, etc. qu'avec leur consentement.
- En résumé: bien choisir les informations que l'on souhaite diffuser.
- Contrôler régulièrement ses paramètres de confidentialité et les adapter le cas échéant

2.11.3. Smartphone et réseau sans fil

- N'utiliser des réseaux sans fil que s'ils sont cryptés. Protéger l'accès par un mot de passe, et prudence en cas de communication de ce mot de passe. Mieux encore: créer des accès d'invité au réseau.
- Couper le réseau sans fil s'il n'est pas nécessaire. Cela accroît la sécurité parce que les attaques sur les interfaces sans fils sont empêchées – et cela économise la batterie.
- Faire preuve de prudence et de sens critique lors du recours à un réseau sans fil ou «hotspot» (éviter l'e-Banking et éviter de se connecter à des services Internet de type réseaux sociaux)
- Si possible, toujours utiliser et envoyer les données sensibles et importantes sous une forme cryptée
- N'activer la localisation GPS que de manière ciblée, c'est-à-dire en cas de besoin réel (toujours réfléchir si une localisation est nécessaire pour un service/une application avant de la valider)
- Télécharger des applications provenant de sources sûres uniquement («App Stores»)
- Avant de télécharger une application, s'informer de son utilité et de son contenu à l'aide de sa description et de ses évaluations, et toujours lire les CGV et les dispositions de protection des données.
- Utiliser les paramètres de sécurité du système d'exploitation: veiller à utiliser les logiciels d'exploitation actuels en installant les mises à jour.
- Limiter l'accès des applications aux informations nécessaires. Est-il nécessaire que l'application ait par exemple accès aux contacts, au calendrier, au GPS et aux messages?

Perte du smartphone –non seulement l'utilisateur perd un périphérique, mais ses données personnelles sont en danger!

- L'accès par des tiers peut être évité, voire empêché, par la saisie préventive d'un mot de passe lors de la mise en service et du déblocage.

- Certaines entreprises proposent un logiciel permettant de «supprimer à distance» les données à partir de l'ordinateur domestique.
- Créer et crypter des sauvegardes régulières (en local, et non dans un nuage)

2.11.4. Périphériques de stockage numériques

- Désactiver la fonction «autorun» de clés USB sur l'ordinateur
- Contrôler par défaut l'absence de virus sur le périphérique
- Utiliser exclusivement des périphériques de stockage provenant de sources et de personnes sûres, dignes de confiance

Perte de la clé USB ou du disque dur portable – les données sont en danger!

- Crypter les données personnelles sensibles ou délicates sur les périphériques de stockage numériques!

2.11.5. Chats

- Choisir des forums de chat surveillés (par un modérateur)
- Prendre un surnom (noms inventés, mots drôles, un nom qui ne prête pas à des associations délicates); ne pas utiliser son vrai nom, ne pas indiquer son âge, ne pas mentionner son lieu de résidence ni son école
- L'adresse, le numéro de téléphone et le nom de famille ne doivent jamais être divulgués
- Adopter un comportement respectueux d'autrui et le juste ton: respecter la «chatiquette» (voir ci-dessous).
- Etre vigilant lors de rencontre avec les personnes rencontrées lors de chat (informer ses parents)
- Une méfiance de bon aloi est préférable. Ne pas divulguer trop d'informations sur soi-même.
- Ne pas «murmurer» directement avec des inconnus.

En cas de situation équivoque:

- Réagir immédiatement et en parler! Les parents, une personne de confiance ou un enseignant peuvent aider.
- Mettre immédiatement fin à la conversation.

Chatiquette – le bon ton en ligne (en allemand uniquement): http://www.chatiquette.de/

2.11.6. Forums et blogs

Exemples: Twitter (microblog), Blogger (Google), forums Web (innombrables)

Nétiquette

La première et principale recommandation de la nétiquette de Usenet est la suivante:
«N'oublie jamais que tu as affaire à une autre personne!»
(Source en allemand uniquement: http://www.usenet-abc.de/wiki/Team/Netiquette)

Règles générales de la nétiquette:

- Eviter les insultes, la politesse a la priorité
- Eviter les longueurs.
- Eviter les remarques ironiques.

- Ecrire correctement (avec utilisation des majuscules et des minuscules)
- Citer correctement (avec les guillemets et la ponctuation finale, si nécessaire, si possible avec indication de la source)
- Ne publier des contributions qu'après avoir bien vérifié leur contenu.

2.11.7. Formulaire en ligne de sociétés, prestataires de services et administrations

- Principe: ne transmettre des données personnelles qu'à des contacts de confiance et uniquement si l'on en tire un avantage.
- Lire minutieusement les CGV (conditions générales de vente) – et particulièrement le paragraphe «Protection des données», qui nous indique quelles données personnelles sont enregistrées, communiquées ou utilisées à des fins publicitaires. Ensuite, voir si l'on souhaite vraiment utiliser l'application dans les conditions indiquées.
- En cas de services de paiement (cartes de crédit, Paypal, etc.), la prudence est de mise: faire preuve de sens critique!
- Ne jamais donner de renseignements sur les données d'utilisateur, de numéro de carte de crédit ou de mots de passe. Les banques ne contactent pas leurs clients par e-mail et ne demandent certainement jamais de mot de passe ou de nom d'utilisateur.
- Ne pas ouvrir de fichier joint ni de lien dans des e-mails douteux.
- Obtenir des informations sur le prestataire et contrôler son sérieux.
- Voir ce qu'il est possible de faire en cas d'attaques de phishing.

Comment réagir face au phishing (hameçonnage)?
https://www.skppsc.ch/fr/sujets/internet/phishing/?noredirect=fr_FR
https://www.melani.admin.ch/melani/fr/home/themen/phishing.html
http://www.service-client.fr/droits-du-consommateur/Phishing-comment-reagir

2.11.8. Messagerie instantanée et téléphonie par Internet

Exemples: Skype, WhatsApp, Snapchat, etc.

Conseils de sécurité généraux:

- Choisir un service de messagerie permettant la configuration de paramètres de sécurité
- Paramétrer le service de messagerie de telle sorte que les nouveaux contacts doivent être acceptés avant d'être repris dans la liste de contacts
- Ne pas transmettre à la légère ses propres identifiants (son nom d'utilisateur) à des inconnus
- N'accepter que de bons amis dans la liste de contacts et ne permettre qu'à ces personnes de vous ajouter sur leur liste (certains services de messagerie ne permettent pas d'annuler la manœuvre ultérieurement)
- Supprimer les contacts désagréables, indécents et envahissants, ou les bloquer avec la fonction «Ignorer»
- N'accepter les messages/appels que de personnes de votre liste de contacts
- Couper l'indicateur de statut général
- Enregistrer automatiquement l'historique des messages
- Bloquer l'affichage de votre photo et la transmission par webcam
- Ne jamais ouvrir de fichiers ou de liens d'inconnus. Ceux-ci peuvent contenir des virus, des chevaux de Troie, etc. Comme dans le cas de la transmission vidéo et téléphonique,

tous les services de messagerie ne bloquent malheureusement pas cette fonction automatiquement.

- Ne jamais cliquer sur un lien reçu dans la fenêtre de messages, sans s'être assuré que la personne qui l'envoie l'a fait intentionnellement. Comme dans le cas des vers contenus dans les e-mails, des parasites attrapés peuvent s'envoyer eux-mêmes à des personnes de la liste de contacts. Même si des liens viennent de personnes que l'on connaît, ils peuvent donc cacher des dangers sans que son expéditeur ne le sache.

2.12. Les données d'autrui: sois fair-play!

- Les droits de la personnalité d'autrui doivent être respectés!
- Ne jamais publier sur la Toile de photos, de films, ni d'informations (nom d'utilisateur, numéros, adresse, mots de passe, etc.) d'autrui sans son autorisation!
- Faire attention aux **données sensibles**!
- Il faut absolument éviter de diffuser des nouveautés sur autrui que la personne concernée ne souhaite pas publier ou n'a pas encore publiées.
- Il est interdit de publier de fausses informations ou des informations dégradantes sur une autre personne. Toute atteinte à la réputation peut être punie!

Respecter le droit pénal

- Des contenus diffamatoires, incitant à la haine raciale, pornographiques ou pédopornographiques et dangereux pour la jeunesse ne peuvent pas être transmis ni diffusés.
- En cas de doute: se distancer et informer une personne de confiance!

Code pénal suisse (CP):

Notamment l'art. 19714. Pornographie

4. Pornographie

1 Quiconque offre, montre, rend accessibles à une personne de moins de 16 ans ou met à sa disposition des écrits, enregistrements sonores ou visuels, images ou autres objets pornographiques ou des représentations pornographiques, ou les diffuse à la radio ou à la télévision, est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

(Source: https://www.admin.ch/opc/fr/classified-compilation/19370083/index.html)

Rester soi-même!

Internet n'est pas un espace anonyme et certainement pas un espace dépourvu de droits.
Il convient donc de ne jamais rien y faire qu'on ne ferait pas dans la vraie vie.
Il faut éviter de faire quoi que ce soit que l'on pourrait regretter ultérieurement.
Rester irréprochable, rester soi-même. Même sur la Toile!

3. Glossaire

3.1. Notions de la protection des données

Homme de verre	Transparence totale de la personne et de son comportement Rapport à la protection des données: par la communication d'informations personnelles, nous risquons de perdre notre vie privée.
Droit d'autodétermination informationnelle	Toute personne a le droit de déterminer elle-même Les informations la concernant pouvant être communiquées, ainsi que quand, où et à qui ces données sont communiquées.
Données à caractère personnel (ou données personnelles)	Informations sur une personne précise ou identifiable. Il suffit donc que les données permettent de déterminer à qui elles se rapportent. La mention d'un nom n'est pas nécessaire.
Données sensibles	Informations particulièrement délicates, requérant une vigilance particulière. En font notamment partie les informations d'appartenance à une religion ou sur des activités politiques, des informations relatives à la sphère intime et les données relatives à la santé.
Vie privée	Domaine réservé au sein duquel la personne exerce son droit de développer librement sa personnalité, sans contraintes externes.
Sphère intime	Domaine des pensées et des sentiments les plus profonds et les plus personnels; domaine du vécu dont une personne ne parle habituellement pas et qu'elle protège des tiers par respect des autres ou de soi (sexualité, par exemple)

3.2. Termes de la loi fédérale sur la protection des données

Traitement	Toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données
Communication	Le fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant
Personne concernée	La personne physique ou morale au sujet de laquelle des données sont traitées
Fichier	Tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée (par une fonction de recherche, par exemple)
Maître du fichier	La personne privée ou l'organe fédéral qui décide du but et du contenu du fichier

3.3. Notions touchant à Internet

Bannière	Surface publicitaire (sur Internet, avec lien vers un domaine/un site Web)
Navigateur	Logiciel permettant d'afficher des contenus d'Internet Programme d'ordinateur, permettant d'accéder à Internet (Internet Explorer, Google Chrome, Firefox, par exemple)
Chat	Possibilité de communication en temps réel de plusieurs internautes; communication en ligne, réalisée à l'aide d'un clavier. L'internaute peut choisir parmi différentes «salles de chat» et décider avec qui elles souhaitent s'entretenir, ou non.
Cookies	Fichiers de texte générés lors de la navigation de l'utilisateur sur Internet. Ces fichiers contiennent des informations concernant les habitudes de navigation des internautes. Les cookies peuvent être consultés de l'extérieur. Ils peuvent cependant être bloqués dans les paramètres du navigateur.
Domaine	Alias alphanumériques des numéros/adresses IP On distingue les domaines à thème des domaines géographiques. *Exemples:* *.com = fournisseur commercial* *.ch = fournisseur suisse ou nom de domaine enregistré en Suisse* *.org = domaine initialement non commercial* *.edu = écoles et universités*
Pare-feu	Ordinateur intermédiaire, séparant un réseau d'Internet Il a pour fonction de protéger un système contre les virus et d'empêcher tout accès illicite au réseau propre.
FTP	«File Transfer Protocol»; permet l'échange de données entre deux ordinateurs connectés à Internet (si le protocole FTP est activé sur tous les deux). Ce système permet de copier des fichiers vers ou d'un ordinateur connecté à Internet.
Pirate informatique («hacker»)	Personne violant l'accès à un système informatique tiers
http	«Hypertext Transfer Protocol»; ce protocole permet le transfert de données par un réseau. Il est principalement utilisé pour charger des sites Web du World Wide Web (WWW) sur un navigateur Web.
https	Egalement appelé «SSL HTTPS»; méthode de transfert crypté de données. Les fichiers sont crypté avec SSL et transmis par http.
Adresse IP	Sorte de «numéro de téléphone» attribué à chaque session Internet. Elle se compose de quatre blocs de chiffres entre 0 et 255, séparés par des points.

	Exemple: 62.2.169.0
Malware	Logiciel malveillant – (parfois utilisé comme synonyme de virus) installé par l'utilisateur de manière involontaire ou à son insu et endommageant l'ordinateur
Newsgroup	Forum de discussion sur Internet
Médias sociaux	voir Web 2.0
SNS	«Social Network Services» – sites de réseaux sociaux *Exemple: Facebook*
SSL	Technologie de cryptage pour Internet
Opérateur Internet	Fournisseur de services Internet *Exemples: upc, swisscom, sunrise*
URL	«Uniform Ressource Locator». Système permettant d'atteindre une ressource sur Internet. Peut également être désigné comme «adresse» d'une offre Web. *Exemple: www.sbb.ch*
***Web* 2.0**	Application interactive sur Internet L'internaute n'est pas seulement consommateur, mais y participe lui-même activement par l'apport et le téléchargement d'informations.
WLAN	Wireless Local Area Network – réseau sans fil

Lexique Internet pour les parents et les enfants
https://www.internet-abc.de/eltern/lexikon/ (en allemand uniquement) (parents/adultes)
https://www.internet-abc.de/kinder/lexikon/ (en allemand uniquement) (enfants)

4. Sources, liens et références

Sujet / mots-clés	Lien
Préposé fédéral à la protection des données	https://www.edoeb.admin.ch/edoeb/fr/home.html
Protection des données sur Internet	https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer.html
Conseils et informations sur Internet	https://www.jeunesetmedias.ch/fr/accueil.html http://netla.ch/fr https://www.datak.ch
Sécurité sur Internet	https://www.skppsc.ch/fr/ https://www.ouvrezloeil.ch/fr/home
Violence et risques sur Internet	https://www.jeunesetmedias.ch/fr/opportunites-et-risques/risques/violence.html http://www.netcity.org/
Conseils sur le chat	http://medienundschule.ch/fit4chat/ (uniquement en allemand) http://www.kinder-im-internet.ch/themen/vorbereitung-wissen/fit4chat/ (uniquement en allemand)
Réseaux sociaux	https://www.jeunesetmedias.ch/fr/opportunites-et-risques/reseaux-sociaux.html
Réseau sans fil	https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/wlan.html
L'informatique en nuage («cloud computing»)	https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/cloud-computing/explications-concernant-l-informatique-en-nuage--cloud-computing.html
Téléphone mobile	https://www.handysektor.de/ (uniquement en allemand)
Liens divers (jeunes / Internet)	https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/jeunes-et-internet/liens-sur-le-sujet.html
Informations pour les parents	https://conseils-aux-parents.projuventute.ch/index.php?id=2525&L=1 https://www.internet-abc.de/ (uniquement en allemand)

5. Liste de personnes de contact pour différents problèmes

5.1. Protection des données

Préposé fédéral à la protection des données et à la transparence
Formulaire de contact:
https://www.edoeb.admin.ch/edoeb/fr/home/le-pfpdt/contact/formulaire-de-contact.html
ou Tél. +41 (0)58 462 43 95

5.2. Pour les parents et les enseignants

Urgences parentales: 0848 354 555 ou elternnotruf.ch/fr/

Liste des centres de conseil régionaux
https://www.jeunesetmedias.ch/fr/offres-et-conseils/services-de-conseil.html?tx_jumsad_pi1%5Bfilter%5D%5Bcanton%5D=129&tx_jumsad_pi1%5Bfilter%5D%5Boffer_form%5D=13&cHash=1e9e918d712bade785003544bd3a525b

ECH – Association faîtière des enseignantes et enseignants suisses
https://www.lch.ch/publikationen/bildung-schweiz/ (uniquement en allemand)

5.3. Pour les enfants et les jeunes

Conseil et aide de Pro Juventute:
Téléphone et SMS 147, informations et questions/réponses sur 147.ch/fr

Sites Web destinés aux jeunes (informations, questions/réponses, forums) – parfois en allemand uniquement:
feel-ok.ch, tschau.ch, cybersmart.ch, frageinfach.ch, lilli.ch et drgay.ch

Adresses des centres cantonaux de consultation pour l'aide aux victimes (LAVI) pour les enfants et les jeunes:
http://www.sodk.ch/fr/domaines/famille-et-societe/aide-aux-victimes/wwwaide-aux-victimesch/liste-dadresses/

Netla - Campagne du Conseil pour la protection de la sphère privée
http://www.netla.ch/fr

6. Articles et dossiers en ligne

N°	Sujet/mots-clés	Lien
1	Protection des données, Internet, avenir	https://www.avenir-suisse.ch/fr/publication/la-sphere-privee-et-le-web/
2	Protection des données, Internet	http://www.bilan.ch/economie/protection-donnees-personnelles-nouvel-eldorado-de-suisse
3	Protection des données, logiciel, reconnaissance des données	https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/technologien/biometrie.html
4	Protection des données, Internet, enfants, habitudes de navigation	https://www.cnil.fr/fr/vie-privee-des-enfants-une-protection-insuffisante-sur-les-sites-internet-0
5	Internet, enfants et jeunes, habitudes de navigation	https://www.educa.ch/sites/default/files/protection_des_donnees_0.pdf
6	Actualités multimedia (20 Minutes)	http://www.20min.ch/ro/multimedia/stories/
7	Facebook, protection des données	https://www.tdg.ch/economie/facebook-promeut-protection-donnees/story/25796075
8	Facebook, protection des données, législation	http://www.bilan.ch/entreprises/facebook-se-prepare-a-nouvelle-loi-europeenne-vie-privee
9	Facebook, vie privée	http://www.cnetfrance.fr/produits/confidentialite-et-vie-privee-sur-facebook-mode-d-emploi-39752014.htm
10	Facebook, faux amis	https://www.dna.fr/economie/2016/10/13/attention-aux-faux-amis-sur-facebook
11	Facebook, fichiers personnels	http://translate.google.com/translate?hl=en&sl=de&tl=fr&u=https%3A%2F%2Firights.info%2Fartikel%2Finhalte-auf-facebook-veroffentlichen-was-muss-ich-beachten%2F11555&sandbox=1
12	L'informatique en nuage («cloud computing»)	https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/cloud-computing/explications-concernant-l-informatique-en-nuage--cloud-computing.html
13	Téléchargement de film sur Youtube: déposer plainte?	https://www.lemonde.fr/pixels/article/2016/02/11/que-risque-un-youtubeur-qui-plagie-des-videos_4863915_4408996.html

14	Smartphones, applications, données personnelles	https://www.jedecide.be/les-jeunes/smartphones-applications/applications-et-informations-personnelles
15	IPhone, Apple, données personnelles	http://www.zdnet.fr/actualites/apple-collectera-plus-de-donnees-personnelles-sur-ios-39847914.htm
16	Smartphone, Android, données personnelles	http://www.levif.be/actualite/les-applications-android-ont-acces-aux-donnees-personnelles-sans-autorisation/article-normal-765705.html
17	Mise au pilori sur internet	https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/mises-au-pilori-sur-internet/mises-au-pilori-sur-internet.html
18	Hameçonnage («phishing»)	https://www.melani.admin.ch/melani/fr/home/themen/phishing.html

7. Le PFPDT dans les médias

Séléction d'interviews et d'articles sur des sujets actuels dans le domaine de la protection des données : https://www.edoeb.admin.ch/edoeb/de/home/aktuell/medien/der-edoeb-in-den-medien.html