# JEUNES ET RÉSEAUX SOCIAUX

# DES ESPACES DE LIBERTÉ SOUS MULTIPLES SURVEILLANCES

---



Ligue des droits de l'Homme
FONDÉE EN 1898

# TABLE DES MATIÈRES

# INTRODUCTION

Les réseaux sociaux font de plus en plus partie de nos vies depuis une quinzaine d'années. Leurs effets, intérêts et défauts commencent à être étudiés. Malgré tout, en raison de l'évolution rapide des pratiques et des outils, il n'est pas facile de bien comprendre ces phénomènes au quotidien.

On peut relever une problématique s'agissant de ces outils (et qui pourrait être élargie au numérique en général) : il existe une différence d'approche entre des individus qui ont grandi « sans », et ont appris à les utiliser avec leurs connaissances précédentes, face à ceux qui n'ont connu qu'un monde « avec ». Comme pour toute évolution technique majeure, l'expérience des premiers est intéressante pour essayer de conserver les « meilleurs aspects » et adopter une approche critique vis-à-vis de ces nouvelles pratiques. Problème : le dialogue avec les seconds n'est pas toujours évident. En effet, la connaissance et les usages de ces outils par les premiers sont souvent plus limités (quand ils ne sont pas absents) et très différents. Les natifs de l'ère numérique n'en sont pas des génies pour autant. S'ils doivent, par défaut (ou du moins y sont fortement incités), utiliser ces outils au quotidien, ils n'en maitrisent pas forcément les enjeux ni ne savent les remettre en question.

Il est utile de fournir aux formateurs de la société civile des éléments pour comprendre ces outils et pratiques, leurs intérêts et leurs dangers. Il s'agit d'essayer d'améliorer le dialogue et, en s'appuyant sur leurs parcours et expériences, les aider à sensibiliser les plus jeunes à de bons usages.

Ce petit guide vise donc à présenter un tour d'horizon des problèmes posés par les réseaux sociaux pour la jeunesse et plus particulièrement des collégiens et lycéens. Il a vocation à être complété par des formations ajoutant des méthodes, contenus et déroulés de séances directement utilisables avec les adolescents.

Il s'articule en 4 grandes parties, tout d'abord une présentation générale de ce que sont les réseaux sociaux et de leurs apports (**I**), suivie d'une présentation de leurs dangers et risques spécifiques (**II**). Ce cadre posé, la troisième partie détaille les méthodes générales qui permettent de limiter leurs problèmes (**III**). Ce guide sera conclu par une liste non exhaustive des sources et outils opérationnels existants pour former la jeunesse à de bons usages.

# I LES RÉSEAUX SOCIAUX NUMÉRIQUES

## I.A. UNE TENTATIVE DE DÉFINITION

Dans le langage courant l'expression « réseaux sociaux » renvoie à un imaginaire commun : autrefois des sites tels que MySpace ou Copains d'avant et désormais Facebook, Twitter ou Instagram. Pourtant, si on se penche vraiment sur le terme, on se rend vite compte qu'il n'est lexicalement pas adapté à ces outils. Au sens strict, un réseau social est un « ensemble d'individus ou d'organisations reliés par des interactions sociales régulières »[1]. Une notion académique bien plus large que le champ des préoccupations des jeunes vis-à-vis des « réseaux sociaux ». Pour tenter de cerner le phénomène et se concentrer sur les services numériques, des termes connexes ont pu être explorés : « médias sociaux », « sites de réseautage social », etc. Retenons celle de « site de réseau social » défini par d. boyd et N. Ellison[2] :

> « Services s'appuyant sur le Web qui permettent aux individus de :
> 1) construire un profil public ou semi-public au sein d'un système délimité et encadré
> 2) d'articuler une liste d'autres utilisateurs avec qui ils partagent un lien, et,
> 3) de voir et traverser leur liste de connexions et celles faites par d'autres au sein du système. La nature et la nomenclature de ces connexions pouvant varier de site en site ».

Cette définition de 2007 présente des limites, notamment parce qu'il peut s'agir d'applications et non pas de « site » au sens strict du terme. Analysée avec finesse, elle répond bien aux caractéristiques des réseaux susnommés sans toutefois être très explicite pour le public.

Pour la développer un peu, on peut revenir sur certains points saillants de ces sites ou services de réseau social qui doivent être gardés en tête pour toute analyse sur ces réseaux.

1/ Ils permettent une **interactivité** entre leurs utilisateurs. Qu'il s'agisse de messagerie directe, d'échanges de contenus (photos, vidéos, textes…), d'invitation à des événements, etc., ces outils permettent d'interagir avec des personnes en partageant des informations et des productions et en voyant celles des autres. Ces interactions peuvent être réalisées au sein d'un groupe plus ou moins grand, mais également à l'égard d'un seul de ses contacts.

2/ Ils sont centrés sur des « **usages sociaux** », sans interaction entre utilisateurs ils n'existent plus réellement (ex. MySpace) et leurs **fonctionnalités** vont principalement viser cette mise en relation. Il existe de nombreux sites qui disposent d'« aspects sociaux » sans que cela soit au cœur de leurs usages les excluant en partie du champ de ce guide[3]. Il faut garder cela en tête : pour un fournisseur de service de réseau social, le plus important est que ses utilisateurs fréquentent le service aussi fréquemment que possible et interagissent toujours plus. Cela va générer plus de données pour le propriétaire du site et lui offrir plus d'opportunités de transmission de messages publicitaires.

3/ Ils permettent des échanges au sein d'une **communauté** (ensemble de personnes partageant un lien commun) ainsi que d'en créer de nouvelles en leur sein. Un point est à relever, dans les usages des réseaux sociaux par les jeunes (hors des réseaux professionnels ou des services dédiés aux rencontres sentimentales), la part du

[1] Entrée « Réseau social ». Wikipédia, dernière édition 28 nov. 2016.
[2] Traduction personnelle de : boyd, danah, et Nicole B. Ellison. « Social Network Sites: Definition, History, and Scholarship ». Journal of Computer-Mediated Communication 13, No. 1 (1er octobre 2007), doi:10.1111/j.1083-6101.2007.00393.x.
[3] Bien que les éléments présentés puissent toutefois s'appliquer à ces fonctionnements.

« réseautage », de l'utilisation du réseau social pour établir de nouveaux contacts, semble faible. Le réseau social va plutôt étendre à un nouvel espace un lien préexistant. Il peut potentiellement succéder au lien antérieur et le faire perdurer au sein du seul réseau social. Une communauté peut aussi se matérialiser autour d'un sujet qui pourra être développé en son sein.

4/ Ils permettent de proposer une **représentation de soi** avec une articulation **délicate entre représentation publique et privée**. Il y aura par défaut un profil public, potentiellement minimaliste, qui pourra être plus ou moins étoffé et, selon le service, la publicité des actions sur le réseau variera et pourra être paramétrée.


Ces éléments apparaissent dans tous les réseaux sociaux reconnus comme tels. Il n'est toutefois pas possible de réellement comprendre les enjeux de ces services pour les jeunes sans entrer dans le détail des différents réseaux. En effet, bien que certains problèmes et questionnements soient transverses, beaucoup sont intimement liées aux spécificités d'un, ou d'un type de réseau social.

## I.B. QUELQUES RÉSEAUX SOCIAUX UTILISÉS

En matière de réseaux sociaux comme plus généralement sur toutes les pratiques numériques, les usages, outils, possibilités, services, etc. changent vite, très vite même ! Cette vitesse d'évolution est renforcée pour les jeunes, souvent plus prompts à essayer de nouvelles applications. Elle se combine à une réelle diversité de pratiques qui varient selon les âges, les milieux sociaux, les zones géographiques et plus généralement habitudes et modes locales. Ainsi une connaissance exacte des réseaux existants aura forcément ses limites. Nul doute que quelques mois après la publication de ces lignes de nouveaux outils seront employés ou que l'utilisation des anciens aura changé. Il s'agit surtout d'essayer de comprendre les fonctionnalités générales et de prendre un peu de hauteur face à ces phénomènes.

Il ne semble toutefois pas totalement inutile de revenir sur les principaux outils utilisés[4] en France par les adolescents. Cela semble nécessaire pour connaître a minima le spectre des pratiques et présenter des fonctionnalités qui auront probablement vocation à perdurer sous une forme ou l'autre. C'est surtout l'occasion de donner quelques éléments précis qui peuvent aider à répondre à des questions ou mieux comprendre les enjeux.

[4] Le choix des outils présentés reste malgré tout arbitraire. Il ne s'appuie pas sur une étude exacte de l'usage des outils, mais sur un sentiment général issu d'une veille active et d'échanges avec les enfants et les acteurs travaillant sur ces sujets.

## 1. FACEBOOK

Nul besoin de présenter Facebook ni ses fonctionnalités, avec 30 millions d'utilisateurs réguliers en France[5], le réseau y reste incontestablement le réseau social le plus commun. L'outil est très utilisé à tous les âges. On constate toutefois que si les enfants s'y inscrivent également, et sans nécessairement respecter la barrière juridique des « 13 ans »[6], leurs usages de Facebook, quoique fréquents, ne sont pas forcément aussi actifs qu'on pourrait le penser. De nombreux profils Facebook de mineurs donnent le sentiment d'un certain contrôle sur la représentation, d'une maitrise sur leur image. La présence de leurs parents, prompts à les ajouter en amis[7], joue largement. Il semble toutefois que l'outil de tchat « messenger » reste très employé et la société Facebook détient par ailleurs deux des outils ci-après cités qui sont particulièrement prisés des adolescents : WhatsApp et Instagram. L'entreprise dispose grâce à ce trio d'une place conséquente dans la vie sociale numérique de la jeunesse.

## 2. WHATSAPP

WhatsApp est une application pour ordiphone (« *smartphone* »[8]). Elle propose un service de messagerie instantanée via Internet. Elle n'est pas nécessairement utilisée comme un service de réseau social. Elle offre toutefois la possibilité de créer des « groupes de discussion » permettant facilement à un groupe d'utilisateurs d'échanger ensemble. Étant un des outils de messagerie les plus utilisés, on retrouve fréquemment cet usage, notamment chez les lycéens. La messagerie de groupe peut renforcer les groupes affinitaires et peut jouer un poids dans les rapports sociaux. D'autres applications sont parfois utilisées pour la même utilisation de tchat et de groupe de discussion (Telegram, Viber, Messenger de Facebook, Snapchat récemment…), les problématiques y sont les mêmes.

## 3. INSTAGRAM

Instagram est une application pour ordiphone. Elle propose un service de partage de photos et de courtes vidéos. Il est particulièrement connu pour ses « filtres » qui vont modifier sensiblement les photos et les rendre facilement plus « attrayantes ». Les utilisateurs vont y suivre les comptes les intéressant, qu'il s'agisse de leurs amis, mais aussi de célébrités ou de communication commerciales. La publication des photos et vidéos est accompagnée de courts textes, mais reste centrée sur le visuel, qui apparaît très maitrisé chez les jeunes : les photos postées doivent participer à une bonne représentation de leur personne. L'outil ne permet pas directement de partager les contenus de quelqu'un d'autre, l'affichage montrera donc surtout les productions des comptes suivis. Instagram est réputé favoriser « l'engagement »[9] des personnes qui « aiment » facilement les photos.

## 4. YOUTUBE

La plateforme de partage de vidéos appartenant à Alphabet (la société mère de Google) est utilisée par les jeunes (et les moins jeunes) pour suivre toutes les vidéos des vidéastes et producteurs de contenus qui leur plaisent. Elle comporte toutefois pour cela de nombreuses fonctionnalités de réseau social et il est fréquent que les jeunes s'y « échangent » des

[5] « Facebook : 1,8 milliard d'utilisateurs, 7 milliards de CA et des inquiétudes pour l'avenir ». *Blog du Modérateur*, 3 novembre 2016.
[6] Fox, Zoe. « 38% of Children on Facebook Are Younger Than 12 », Mashable, 11 avril 2012.
[7] « Les relations parents / enfants sur Facebook ». Blog du Modérateur, 18 février 2013.
[8] Rappelons que ces « smartphones » ne sont ni véritablement des téléphones et sont encore moins « intelligents ». Il s'agit d'ordinateurs plus limités et plus contrôlés que leurs homologues traditionnels.
[9] Un fort investissement des membres dans l'usage du réseau qui multiplie leurs interactions.

vidéos, mais aussi, et surtout, en produisent directement dépassant ainsi largement la seule « consommation ». On trouve des quantités colossales de vidéos de toute nature avec quelques dizaines de visionnages correspondant à des groupes d'amis ou de connaissances assez jeunes sans réel intérêt pour qui n'appartient pas à ce cercle.

### 5. PERISCOPE

Dans la catégorie vidéo, il parait nécessaire de parler de Periscope et plus généralement des applications permettant de transmettre de la vidéo en direct (Youtube, Twitch…). L'application permet de filmer (et notamment de se filmer) et retransmettre en direct la vidéo. Elle inclut différents mécanismes propres aux réseaux sociaux : s'abonner pour être averti des directs (ou voir les enregistrements), fonction de tchat, « aime », etc. Développés par Twitter les deux services sont très liés. On y trouve de nombreux jeunes se filmant face caméra sans rien faire de très particulier (jouer de la guitare, regarder la télévision…) si ce n'est interagir avec le tchat, mais d'autres réalisent des « canulars » téléphoniques ou des défis en direct. Les pratiques sont bien moins importantes en volume que d'autres services, mais les impacts peuvent être conséquents. Deux cas on fait beaucoup parler d'eux, deux adolescents ont agressé une personne prise au hasard dans la rue en se filmant sur l'application[10], une autre a filmé son suicide en direct[11].

### 6. TWITTER

Twitter est un des principaux réseaux sociaux en nombre d'utilisateurs. Sa fonction phare consiste en la publication de courts messages de moins de 140 caractères. Ces messages sont nécessairement publics et les « Twittos » (utilisateurs de Twitter) sont invités à les repartager (ReTweet / like / réponse). Ils peuvent être agrémentés de photos ou de vidéos. Le site permet aussi de s'envoyer des messages privés sans limites de taille dès que les utilisateurs se suivent mutuellement. Les pratiques sont très diverses sur Twitter. Beaucoup de collégiens et lycéens s'en servent pour commenter leur quotidien et réagir aux actualités qui les touchent. Il est plus facile d'y interagir sous pseudonyme que sur Facebook. Si personne ne s'imagine que les tweets sont privés, les fonctionnalités de repartage peuvent donner une audience bien plus considérable à des messages que celle initialement imaginée.


### 7. SNAPCHAT

Cette application (sur ordiphone) est très prisée des jeunes. Elle permet l'échange de messages, de photos ou de courtes vidéos dont la particularité est que la durée de vie des messages est limitée. Ainsi, à la réception du « Snap » celui-ci ne sera affiché qu'un certain temps (quelques secondes pour la majorité des messages, 24h dans certains cas précis) avant de disparaitre. Le ton peut y être plus léger sans crainte que les propos ou photos ne soient ressortis à d'autres moments. Le service est tourné vers le ludique et permet aussi facilement de modifier les photos, notamment les autoportraits (« selfies ») avec des filtres transformateurs (ajout d'attributs, déformation ou permutation du visage, etc.). Cette

[10] C. Brenière, « Une agression gratuite diffusée par deux adolescents sur Periscope » RTL.fr, 29 avril 2016.
[11] « Suicide d'une jeune fille sur Periscope : "Ce qui va se passer risque d'être très choquant" », LeMonde.fr, 11 mai 2016.

application pose de réels problèmes en termes de confidentialité. En effet, ses utilisateurs s'attendent à ce que les messages ne puissent pas être conservés alors que des méthodes continuent de permettre leur enregistrement. De plus, l'entreprise elle-même peut accéder au contenu après son effacement des téléphones.

Cette liste est nécessairement limitée. Il ne faut pas oublier que beaucoup d'interactions similaires à celles réalisées sur les réseaux sociaux peuvent transiter par des jeux vidéos en ligne où souvent les questions d'identité sont moins importantes. Le phénomène semble s'être éteint, mais les sites offrant des possibilités de questions anonymes tels que « ask.fm » ou pire de « potins anonymes »[12] avaient pu poser d'importants problèmes de cyberharcèlement.

## I.C. FONCTIONS ET CARACTÉRISTIQUES DES RÉSEAUX SOCIAUX

On le voit à la liste des services mis en valeur, les réseaux sociaux utilisés par les jeunes passent désormais principalement par des applications pour ordiphones plus que par un navigateur d'ordinateur et sont intiment prévus et imbriqués dans des usages mobiles. La pratique majoritaire reste similaire à celle des textos, mais des textos enrichis (photos / vidéos / textos de groupe, etc.). Ces services peuvent ainsi prendre une part conséquente dans la vie quotidienne en étant utilisés tout au long de la journée.

### PRINCIPALES FONCTIONNALITÉS

On peut relever plusieurs fonctions de ses outils qui s'appliquent plus ou moins bien selon chaque service :

- Le **partage de contenus de tiers**, qu'il s'agisse de vidéos ou de photos provenant de différents médias ou directement de célébrités ;
- Le **partage de productions personnelles**, photos, courtes vidéos, blagues, émotions et sentiments, etc. ;
- Des **interactions simples en direct ou en différé**, par le biais de mécanismes montrant l'appréciation (« j'aime » et assimilés) ou d'une **messagerie simple et rapide** permettant d'échanger facilement avec ses contacts qui en sont notifiés ;
- Des fonctions de **messagerie de groupe** permettant facilement d'échanger à plusieurs par groupe affinitaire ;
- Une **façon de se représenter** vis-à-vis des autres, plus ou moins publiquement, par le biais du profil, du « mur » ou de la page regroupant les contenus, qui se construit à chaque ajout dans le profil où à chaque nouvelle publication.

Les mécanismes de représentation publique jouent un rôle notable dans l'usage du réseau social. Ainsi, la publicité, totale ou partielle, du profil, seconde identité de soi sur le réseau va changer les comportements. Selon le service, de nombreux adolescents vont souvent adopter de faux profils en parallèle à leur profil principal pouvant ainsi jouer des rôles et identités multiples. Cela est toutefois impossible, ou peu utile, quand le service est rattaché à un numéro de téléphone (ex. WhatsApp) ou lorsqu'il requiert que les autres vous connaissent directement pour interagir avec eux (ex. Facebook).
Dans les réseaux plus ouverts (ex. Instagram ou Twitter) où la publication est, par défaut, publique les comportements varient.
Au-delà du seul profil comportant les informations remplies par l'utilisateur, le fil d'actualité (ex. le mur de Facebook), les comptes suivis, les contenus sur lesquels on est identifié directement (« taggué ») vont tout autant jouer sur cette représentation publique. Les récits d'expérience des adolescents montrent que ces formes d'extériorisation publique sont très importantes à leurs yeux et souvent très maitrisées. Ils ont tendance à utiliser largement les

[12] X. Berne, « La CNIL met en demeure l'application « Gossip, les potins anonymes » », Next Inpact, 14 oct. 2016.

fonctionnalités permettant de s'assurer que le profil corresponde à la représentation d'eux-mêmes qu'ils souhaitent afficher.

Ainsi les jeunes semblent bien loin « **d'abandonner leur vie privée** ». S'ils offrent, facilement et sans grande considération, de nombreuses données personnelles aux entreprises gérant les réseaux sociaux, vis-à-vis de leurs proches c'est une autre histoire. Leurs publications sur les réseaux vont parfois témoigner d'une grande exposition personnelle, parfois même s'agissant d'éléments d'identification très précis ou très sensibles. À l'inverse, elles peuvent être extrêmement contrôlées avec une réelle volonté que l'information reste privée et dans un cadre très restreint.

## I.D. LES APPORTS ET INTÉRÊTS DES RÉSEAUX SOCIAUX

Les réseaux sociaux sont incontestablement des outils puissants et ce d'autant plus qu'ils sont massivement utilisés. On verra que cela implique de **réels dangers** qui doivent être pris en compte. Il faut toutefois reconnaitre les **intérêts de ces outils**, pour inciter à ces pratiques et les mettre en valeur.

S'il est préférable de les questionner, les apports génériques des réseaux sociaux sont toutefois assez clairs. Ils facilitent les communications, les échanges de messages et de contenus. Ils permettent notamment de garder un lien avec des personnes qui sont éloignées, de se regrouper par champs affinitaires ou divers sujets, de diffuser ses productions, de parler de ses passions, etc.

Il est ainsi adéquat de nuancer les critiques questionnant la réalité des liens et des échanges entre les utilisateurs. Tous ces outils offrent la possibilité d'avoir de vraies relations avec d'autres personnes, que cela soit numérique et passe par les réseaux ne semble pas devoir les discréditer par défaut. Les interactions qu'ont les jeunes sur ces réseaux sont bien réelles et vont avoir des conséquences sur leur développement et leurs choix.

Il faut essayer de participer à la promotion de leurs aspects positifs : en **facilitant la communication**, ils peuvent favoriser l'**entraide** et la **coopération**. En ce même sens, ils témoignent de la proximité des liens qui unissent les humains les uns aux autres (phénomène dit du « petit monde »[13]).

Ils peuvent, de plus, être employés en tant qu'**outils pédagogiques**, à des fins d'éducation. Cela peut passer par l'utilisation des fonctionnalités des outils[14] ou en profitant d'un cadre moins formel et plus ludique où les élèves se sentent plus à l'aise. Beaucoup de ces outils, couplés aux autres avancées de l'informatique, permettent facilement aux apprenants d'exercer **une réelle liberté d'expression** : ils peuvent diffuser des messages qui pourront potentiellement être vu par tous.

En ce même sens, grâce à la facilité de partage de contenus et d'échanges, ils peuvent aussi **favoriser la diffusion d'informations**, évitant ainsi que la seule charge « d'informer » soit attribuée à des médias centralisés. Cela libère ainsi des opinions minoritaires et permet d'accéder à une plus grande diversité d'information et donc, avec une pointe d'optimisme, d'améliorer la **responsabilité collective**. Sur ce point, force est de reconnaitre que des limites réelles existent s'agissant des pratiques actuelles (vues en II.B.3). Mais même avec

[13] Ainsi, une étude, financée par Facebook (« Anatomy of Facebook », Facebook, 22 nov. 2011), a pu révéler qu'en moyenne chaque utilisateur du réseau était relié à n'importe quel autre par une chaine de 4,74 personnes. Voir aussi l'entrée « Étude du petit monde ». Wikipédia.fr, dernière édition 29 oct. 2016.
[14] On peut en ce sens citer les (trop) nombreux exemples de professeurs « prouvant » sur ces outils qu'une photo peut facilement être reprise à l'autre bout du monde en quelque temps.

de forts mécanismes d'« **entre-soi** » (la fameuse « bulle de filtre »[15]), il est indéniable qu'ils participent à faire découvrir des informations que les jeunes n'auraient pas cherchées par eux-mêmes et donc à une ouverture sur le monde.

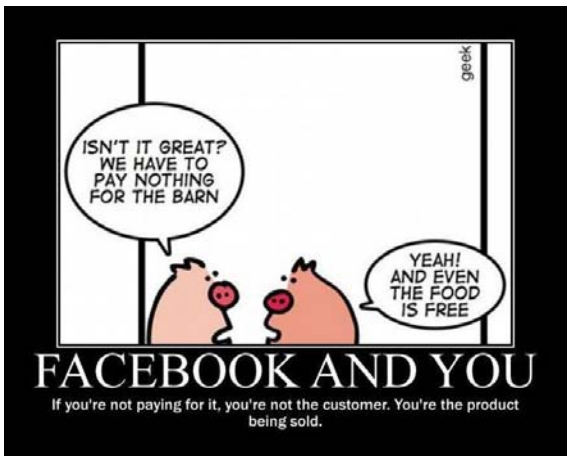
Qu'on le regrette ou non, les réseaux sociaux appartiennent au quotidien d'une grande majorité de jeunes et aux mécanismes de construction de leurs identités et de leurs personnalités. Ils constituent en cela une **forme d'espace public**[16] où les jeunes se réunissent et échangent, avec des contraintes « techniques », mais aussi des libertés conséquentes vis-à-vis de l'espace public « physique ». Oui, il n'y est pas possible de s'y toucher (au soulagement surement de certains parents), mais les contraintes temporelles, de sécurité physique, de transport, etc. y disparaissent également. Les réseaux sociaux peuvent ainsi pallier les difficultés d'accès à un espace de rencontre physique.

En exerçant un trop fort contrôle sur les pratiques de leurs enfants sur les réseaux sociaux, de même que pour leurs autres activités, les parents peuvent avoir des impacts néfastes sur le bon développement, la construction de l'identité et de l'autonomie de ceux-ci. Il est bon que, comme pour toute activité, les parents s'intéressent à ces pratiques. Néanmoins, les **adolescents aussi ont droit au respect de leur vie privée**, et ils en ont particulièrement besoin[17] !

[15] Pariser, Eli. The filter bubble: what the Internet is hiding from you. New York, États-Unis d'Amérique, Penguin Press, 2011.
[16] Un espace public numérique qui vient pour partie remplacer les espaces publics physiques qui pour des raisons géographiques ou de craintes vis-à-vis de la sécurité sont moins employés (voir en ce sens les travaux de d. boyd).
[17] Hartnett, Annie H. « The gift of privacy: How Edward Snowden changed the way I parent ». Salon, 24 juillet 2016.

## II. LES RÉSEAUX SOCIAUX NUMÉRIQUES : QUELS DANGERS, QUELS RISQUES ?

« Si c'est gratuit, c'est vous le produit », ou plus justement : **si un service commercial a l'apparence du gratuit, c'est vous le produit**. Cette maxime[18] est bien connue : oui le cochon est nourri sans qu'il ait à produire le moindre effort, sans échange monétaire, « gratuitement », son destin n'est pas pour autant des plus roses !




Tous les services précédemment présentés ont un coût de mise en place et d'entretien loin d'être négligeables et sont portés par des entreprises ayant pour principal objectif de réaliser des profits. Pourtant, ces services se sont développés sans que les utilisateurs aient à payer pour les utiliser. Ces entreprises cherchent donc à gagner de l'argent par d'autres méthodes. Les méthodes pour réaliser ces profits peuvent toutefois poser de sérieux problèmes sociaux et sociétaux, notamment en matière de libertés et d'équilibres démocratiques (A).

Au-delà de ces problématiques relatives à la place des réseaux sociaux dans la société, leurs usages peuvent présenter d'autres dangers ou conséquences dommageables à titre individuel qu'il convient de limiter par tout moyen (B).

### II. A. LES PROBLÉMATIQUES SOCIALES ET SOCIÉTALES DES RÉSEAUX SOCIAUX

Les principaux réseaux sociaux commerciaux disposent d'une quantité très conséquente d'utilisateurs qui constituent la base de leur pouvoir économique et politique. Ils disposent de différentes méthodes pour rentabiliser la présence des internautes sur leurs services, par exemple :

- faire acheter des produits dérivés ou des services supplémentaires, ce qui est susceptible de poser problème vis-à-vis de la jeunesse qui peut réaliser des achats compulsifs peu pertinents pour, par exemple, continuer de jouer à un jeu dont le début est « gratuit » ;
- faire payer les acteurs économiques tiers pour accéder à leurs réseaux (pour y proposer une application, y disposer d'un espace privé…) ;
- vivre temporairement sur du « capital-investissement » en visant une rentabilité future, etc.

[18] Reprise pour insister sur le fait que ces services ne sont pas gratuits ! Voir en ce sens : L. Chemla, « Si vous êtes le produit, ce n'est pas gratuit », La Quadrature du Net, 17 août 2016.

## II.A.1. UN POUVOIR ÉCONOMIQUE S'APPUYANT SUR L'EXPLOITATION DES DONNÉES À CARACTÈRE PERSONNEL

A l'heure actuelle l'essentiel des revenus générés par ces plateformes provient de l'exploitation des données de leurs utilisateurs à des fins publicitaires. La clef des revenus colossaux de ces entreprises est leur base de données utilisateur. Elles vont vendre aux annonceurs des espaces publicitaires et/ou des profils de consommateurs aussi précis que possible à des fins de marketing. Il s'agit d'afficher la publicité ayant le plus de chance de faire réaliser un acte d'achat au meilleur moment. Au même titre que TF1, Facebook et Google vendent du « temps de cerveau disponible ». Ils ont toutefois la particularité de disposer de bien plus d'informations pour vendre le « temps de cerveau disponible » le plus réceptif possible et le plus facilement manipulable par une publicité ou un message précis. Là où les chaines de télévision vendent l'attention de leurs spectateurs « en gros », les réseaux sociaux peuvent vendre « au détail ».

### UN TRAÇAGE PUBLICITAIRE INTENSIF

Pour cela ces acteurs vont enregistrer l'ensemble des informations et actions réalisées sur le réseau afin de « profiler » au mieux leurs utilisateurs. Ils vont notamment utiliser les informations données activement (âge, amis, préférences, « like »…), mais également des données comportementales : temps passé à regarder un contenu, vidéo lue ou non, profils regardés…
Pire, les plus grands de ces acteurs vont nous « traquer » bien au-delà de leurs services à travers Internet. Ils vont nous suivre au travers de nos navigations par différentes méthodes. En voici quelques-unes :

- en identifiant les sites dont proviennent les utilisateurs et où ils vont ;
- au travers d'outils appelés des « cookies tiers » présents dans les boutons de « partage sur les réseaux sociaux » 

présents sur de nombreux sites permettant à ces entreprises de savoir que vous vous êtes rendus sur ces sites ;
- en faisant plus généralement installer des outils de surveillance appelés « traqueurs » à de nombreux sites (Google analytics par exemple qui offre des statistiques d'utilisation au propriétaire du site, mais aussi à Google) ;
- en demandant aux personnes de s'identifier à différents sites par leurs identifiants Facebook, Google, Twitter, etc. établissant ainsi un lien direct ;
- en achetant des données de connexions à d'autres acteurs utilisant des méthodes similaires qu'ils vont recouper avec les leurs[19].

Ils vont essayer de nous suivre partout, au hasard de nos navigations, pour compléter toujours un peu plus notre profil avec toujours plus d'informations, pour toujours plus de « personnalisation »… et surtout de vente d'« impact publicitaire efficace » aux annonceurs.

### UN QUASI-MONOPOLE DE FAIT

Les données collectées par ces entreprises sur leurs utilisateurs, et même sur des tiers non-inscrits[20], leur offrent un pouvoir économique considérable. De plus, ce pouvoir se renforce pour les acteurs qui ont réussi à disposer du plus grand nombre d'inscrits du secteur par le mécanisme dit « **le gagnant emporte tout** ». Le fait qu'un réseau social soit le plus fréquenté va être un argument conséquent pour le rejoindre : même en présence d'un service concurrent de meilleure qualité, si personne ne s'y rend, peu de personnes y trouveront un intérêt. Le fait qu'un service ait réussi à s'imposer massivement lui offre une

[19] Mattu, J. Angwin, T. Parris Jr , Surya. « Facebook Doesn't Tell Users Everything It Really Knows About Them », ProPublica, 27 décembre 2016.
[20] Que ce soit en se servant des informations données par leurs utilisateurs et même en collectant des données sur différents sites en utilisant notamment des « cookies tiers ».

garantie forte que ces utilisateurs ne partiront pas facilement et donc un certain monopole de fait.

#### « DIGITAL LABOR » — UNE EXPLOITATION NUMÉRIQUE SUBIE

Ces services profitent également de cette position dominante pour faire générer directement de la valeur à leurs utilisateurs. Ceux-ci vont potentiellement produire de la valeur pour le réseau social à chacune de leurs actions. Cela peut provenir de l'exploitation directe de leurs données personnelles, comme précédemment évoqué (revente de données, publicité ciblée, etc.), mais peut aussi provenir de l'exploitation directe de leurs actions[21] et de leurs publications. Ils vont produire des contenus, en indexer d'autres, les évaluer, les diffuser... Ils peuvent aussi jouer le rôle de modérateur, d'animateurs de communauté, etc. Sans leur travail le réseau social serait une coquille vide. Un travail gratuit, s'appuyant toujours sur des données, personnelles ou non, générées par les actions de l'utilisateur, sans que celui-ci n'en bénéficie à aucun moment.

### II.A.2. UN POIDS POLITIQUE CONSÉQUENT

Ce pouvoir n'est pas qu'économique, il est aussi directement politique pour différentes raisons :

#### - Un impact sur les opinions et les comportements.

Ces outils ont une place importante dans la vie quotidienne et ils peuvent devenir une source principale pour s'informer[22]. Ils peuvent favoriser un accès à l'information, ce qui est une composante de la liberté d'expression. Il ne faut toutefois pas oublier que le **« code fait loi »**[23] et que les « algorithmes » de ces services vont jouer sur la nature des contenus qui vont s'afficher pour chaque utilisateur. Les informations qui vont être affichées sur le « mur Facebook », ou sur les fils d'actualité en général, vont dépendre de choix réalisés par ces entreprises qui peuvent (ou non) prendre en compte certains de vos comportements (que vous l'ayez souhaité ou non). Ces entreprises peuvent jouer sur les informations transmises par vos « amis » que vous allez donc voir ou non. Elles ont ainsi un rôle clef dans l'accès à l'information (voir III.C.). Par ces choix généraux, elles peuvent influencer subtilement tout ce que vous allez voir et donc jouer sur les visions du monde de millions d'utilisateurs. Une étude réalisée par Facebook a ainsi montré que le réseau pouvait influer l'expression de l'émotion de ces utilisateurs[24].

#### - Un impact sur les modes d'organisations et de représentation sociale.

En ce même sens, en raison de l'ampleur de leurs usages, les fonctionnements des réseaux sociaux peuvent peser un poids conséquent sur la société qui n'est pas toujours facilement évaluable. Pour donner quelques exemples parlant :

- une personne refusant de rejoindre un réseau social peut se retrouver coupée d'invitation à des événements et ainsi d'opportunités de sociabilité à laquelle elle aurait pourtant eu accès s'il n'existait pas ;

---

[21] Un exemple marquant non spécifique aux réseaux sociaux est celui de Google qui utilise son programme de « captcha » de protection contre les « bots » pour faire exécuter de la reconnaissance de caractère ou d'objets à ses utilisateurs.

[22] On observe une perte d'intérêt chez les jeunes pour la télévision et la radio, la télévision de rattrapage (« en replay ») se développe toutefois largement. Voir Maillard, Matteo. « Les jeunes et les écrans : moins de télé, plus d'Internet et de replay ». Le Monde.fr, 11 décembre 2014, sect. Campus.

[23] « Code is Law – Traduction française du célèbre article de Lawrence Lessig de janv. 2000 : Le code fait loi – de la liberté dans le cyberespace », trad. Sur le Framablog, 22 mai 2010

[24] A. D. I. Kramer, J. E. Guillory, et J. T. Hancock. « Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks ». Proceedings of the National Academy of Sciences 111, No. 24 (17 juin 2014), doi:10.1073/pnas.1320040111.

- en imposant l'utilisation d'une véritable identité pour créer son profil, Facebook peut priver d'accès à ses fonctionnalités des personnes se présentant, pour différentes raisons, par leur pseudonyme. Il peut s'agir de célébrités, mais aussi des personnes transgenres et autres personnes déjà stigmatisées ou persécutées pour leurs idées renforçant leur marginalisation ;
- ils peuvent facilement inciter les citoyens à réaliser une action, par exemple : aller voter[25] ou arborer un symbole sur son avatar en soutien à une cause[26] ce qui a des implications sociales certaines ;
- dans un autre sens, la facilité de création et de diffusion d'un événement a pu aboutir aux phénomènes des « apéros Facebook » qui ont été massivement suivis pour le meilleur et pour le pire.

### - Un contrôle sur les contenus : une censure privée.

Les entreprises disposent en tant que propriétaires d'un réseau social d'un potentiel droit de regard directement sur les contenus postés. Ils peuvent ainsi décider de supprimer les contenus, ou de limiter leurs audiences ou fabrications potentielles (par exemple en les « démonétisant » ou en fermant des comptes, avec ou sans préavis). Cela peut survenir si les contenus ne leur conviennent pas (par exemple, qui les critiquent ou qui ne conviendraient pas avec un État autoritaire avec qui ils sont en négociation commerciale ou même simplement à leur morale subjective[27]). À l'inverse, ils peuvent survaloriser artificiellement des contenus qui les favorisent ou leur conviennent mieux. Ces pratiques sont particulièrement problématiques. Bien que l'on dispose du choix d'être ou non sur ces services, ils disposent d'une place conséquente, parfois incontournable dans la société. Ainsi, en censurant activement certains contenus et en montrant les conséquences d'un irrespect de leur cadre imposé (suppression temporaire ou non du compte, restrictions, surveillance possible des publications, démonétisation, etc.) : ils conduisent des individus à s'autocensurer. Pour ne pas subir ce pouvoir, des personnes vont ainsi limiter leurs expressions, qui pourraient pourtant être tout à fait légales, pour ne pas subir de sanction.

### - Des informations permettant une modélisation et des statistiques sociales sans précédent.

Grâce à la quantité de données qui leur sont livrées, plus ou moins volontairement, ils peuvent disposer de **modélisation et statistiques sociales** très précises. Facebook peut par exemple étudier les tendances et les modes des jeunes en étudiant les « like » et interactions des profils. Le cas de « Google grippe » étudiant l'évolution des recherches de symptômes de maladies épidémiques est aussi bien connu. Bien que ces outils présentent encore des limites, leurs potentialités sont alarmantes. Ces statistiques et modèles peuvent permettre de renforcer les possibilités de manipulations publicitaires, mais, surtout, de les aider à « comprendre » les populations et individus à un degré de précision et de granularité dont aucun État ne dispose. Ces réseaux peuvent deviner des comportements futurs[28] ou des pensées et potentiellement même nous analyser mieux que nous nous comprenons nous-mêmes.

### - Un risque de surveillance privée abusive.

Les dirigeants des entreprises proposant des services de réseaux sociaux et, plus généralement, les personnes (notamment les salariés) ayant des accès directs aux données

[25] B. Hue, « Comment Facebook et Snapchat encouragent les Français à aller voter ». RTL.fr, 30 déc. 2017.
[26] R. Ligneul, « "Changez votre photo de profil" : Facebook et le bleu-blanc-rouge en un clic ». Rue89, 17 nov. 2015.
[27] Par exemple, l'affichage de photos d'allaitement ou d'œuvres d'art représentant des personnes nues sur Facebook, qui sont très fréquemment censurées.
[28] Par exemple, si un couple risque de se séparer, ou de se former « Flings or Lifetimes? The Duration of Facebook Relationships »1 Facebook, 12 fév. 2014, K. Heaney « Facebook Knew I Was Gay Before My Family Did ». BuzzFeed, 19 mars 2013

et profils utilisateurs sont susceptibles de vouloir en profiter. Le pouvoir a tendance à corrompre, les personnes qui le détiennent peuvent, et risquent donc d'en abuser : cette possibilité ne doit pas être oubliée. Même si les entreprises et le droit prohibent, heureusement, de telles intrusions à des fins personnelles[29], de nombreux abus ont déjà été exposés dans des situations similaires[30].

### II.A.3. DES OUTILS DE POUVOIR CONVOITÉS

Ces pouvoirs étendus détenus par les réseaux sociaux et les quantités de données dont ils regorgent sont évidemment convoités par différents acteurs.

#### - Les adjoints d'une surveillance publique.

C'est le cas des pouvoirs publics par le biais des autorités de police et des services de renseignement. En 2013, les révélations d'E. Snowden ont prouvé que la NSA disposait d'accès (directs[31] ou indirects) aux données de nombreux grands réseaux sociaux et s'en servait à des fins de surveillance. Que ce soit volontairement ou sous la contrainte, ces entreprises participent donc à la surveillance des populations avec des finalités plus ou moins légitimes. Il est légitime que, par exemple, sur décision d'un juge, il soit possible d'accéder à des données concernant un membre d'un réseau de grand banditisme. Un accès indiscriminé aux contenus des discussions Facebook ou même à leurs métadonnées pour y détecter des intentions de participer ou d'organiser une mobilisation publique est par contre abusif. Il est également abusif pour les autorités américaines de demander l'intégralité des comptes sur les réseaux sociaux aux personnes souhaitant se rendre aux États-Unis[32].

#### - Des cibles privilégiées pour des individus mal intentionnés.

En raison de la forte concentration d'individus et d'informations sensibles sur quelques services, leurs bases de données et des failles de sécurité permettant d'accéder à certaines informations deviennent des objets extrêmement convoités par des attaquants divers. Pour les mêmes motifs et en raison de la propagation de l'information, ces sites sont souvent d'excellents vecteurs de propagation de virus, de spams, de tentatives d'escroquerie ou d'utilisation de failles informatiques en général.

#### - Des vecteurs de désinformation ou de déstabilisation.

Si la problématique est ancienne, elle est arrivée avec force récemment dans le débat public. Des personnes, maitrisant les fonctionnements de ces outils, de leurs algorithmes, ainsi que les méthodes de manipulation intellectuelle, profitent des réseaux sociaux pour diffuser largement (ou au contraire sur des populations très ciblées) de fausses informations à des fins de manipulations politiques ou économiques. Cela semble avoir joué un rôle (dont l'évaluation est difficile) dans la campagne présidentielle américaine[33]. Plus généralement, cela pose de réelles questions face à des articles promouvant des pseudosciences en matière de santé ou diffusant des théories conspirationnistes sans aucune base scientifique ou politique.

---

[29] L. Vaas, « Facebook explains when and why it peeps at your account ». Naked Security, 3 mars 2015.
[30] T. B. Lee, « 5 Americans who used NSA facilities to spy on lovers », 27 sept. 2013, Washington Post ; B. Chapman, « Uber employees used app to 'spy on ex-lovers, politicians and celebrities' ». The Independent, 13 déc. 2016 ; K. Zetter « Ex-Googler Allegedly Spied on User E-Mails, Chats ». WIRED, sept. 2010.
[31] « PRISM (programme de surveillance) ». Wikipédia, page du 30 octobre 2016.
[32] E. Cario, « États-Unis : la douane veut connaître les réseaux sociaux des arrivants ». Libération, 26 déc. 2016.
[33] Voir par exemple : O. Solon, « 2016 : The Year Facebook Became the Bad Guy ». The Guardian, 12 déc. 2016.

## II. B. LES PROBLÉMATIQUES INDIVIDUELLES

Les problématiques sociétales préalablement exprimées ont des conséquences directes à l'échelon individuel et sont complétées par des dangers plus isolés, plus personnels, qui vont toucher directement les jeunes.

### II.B.1. LES RISQUES DE PRÉDATION EN LIGNE

#### - Un risque de surveillance privée

La surveillance peut provenir des sites eux-mêmes ou des États, mais elle peut aussi provenir d'individus tiers, qui peuvent être des proches ou des inconnus. Il peut s'agir d'un professeur qui se renseigne sur ses élèves, d'un patron sur ses salariés, des candidats à l'embauche ou des clients, d'une personne fâchée qui souhaite vous faire du tort (exemple un amour déçu), d'une personne qui s'intéresse un peu trop à vous pour de mauvaises raisons (harcèlement, pédophilie…) ou encore un inconnu qui a des visées lucratives. Les réseaux sociaux sont des cibles privilégiées pour obtenir des informations sur autrui que ce soit de façon légale ou non. Les informations peuvent être collectées directement en raison de réglages trop permissifs des paramètres de confidentialité. Cela peut également provenir d'une recherche extensive d'informations sur la personne pour lui nuire (« cyberpistage » ou « cyberharcèlement »), mais aussi de l'utilisation d'un bug ou d'une faille de sécurité qui peuvent apporter des informations à des personnes non souhaitées.

#### - Les dangers de cette surveillance

Ces informations récupérées sur des personnes peuvent être utilisées contre elles. La vie privée ce n'est pas forcément se cacher, c'est partager selon ses propres souhaits. La protéger, c'est choisir qui peut accéder à quelle information. Les informations obtenues sur Internet peuvent servir en dehors. Des cambrioleurs seront, par exemple, contents d'apprendre que des personnes partent en vacances pendant une période donnée. Des connaissances mal intentionnées seront également intéressées par vos secrets, que cela soit pour vous faire chanter ou pour vous faire du mal.

#### - L'usurpation d'identité

Les informations collectées peuvent aussi servir à **usurper votre identité** que ce soit pour obtenir encore plus d'informations sur vous, pour accéder à d'autres comptes notamment vos comptes bancaires et vos courriels, ou pour utiliser cette identité en dehors d'Internet. Les risques peuvent être colossaux et occasionner de sérieux soucis. À plus petite échelle, une personne qui va se faire passer pour une autre sur un réseau social grâce à des informations récupérées facilement, sans même accéder au véritable compte, peut déjà faire beaucoup de mal à la réputation et à la tranquillité de quelqu'un.

#### - Hameçonnage et ingénierie sociale

Des individus mal intentionnés peuvent se servir des réseaux sociaux et, souvent, de comptes de connaissances déjà compromis pour tenter soit de compromettre plus de personnes soit de récupérer de l'argent ou des informations sensibles. On parle

d'« hameçonnage » (« *phishing* »[34]) quand on va utiliser un message un peu générique pour détecter les personnes les plus susceptibles de se laisser abuser. On parle d'ingénierie sociale quand une personne (ou un groupe) spécifique va être visée en utilisant un maximum d'informations personnelles pour réussir à la persuader.

### II.B.2. LES RISQUES D'EXPOSITION DE SOI

Cela a été présenté (I.C et D), les réseaux sociaux imposent une forme de représentation publique de soi. Si celle-ci peut présenter des effets bénéfiques et être maitrisée, elle peut impliquer certains écueils.

#### - Une « e-réputation » à soigner

Contrairement à nos actions physiques, nos activités en ligne laissent des traces qui sont durables et potentiellement accessibles à beaucoup de monde. Il devient important de soigner sa réputation numérique et de faire attention à ce que les autres peuvent voir de nous en ligne. Les besoins de cette e-réputation vont varier selon le public qui peut accéder aux informations : on accepte que certaines informations soient vues par nos camarades, mais pas par nos professeurs et inversement. L'usage des réseaux sociaux implique donc une attention très particulière à ce que l'on publie et qui peut y accéder. Le problème est que d'autres peuvent également y mettre des informations sur nous sans que l'on en soit nécessairement informé. Certains jeunes sont ainsi contraints d'être présents sur des réseaux sociaux afin de pouvoir contrôler ce que l'on y dit sur eux.

#### - Harcèlement en ligne

Le harcèlement scolaire n'a pas attendu Internet. Il y trouve toutefois un nouveau terrain d'expression particulièrement saillant. Ainsi, les réseaux sociaux peuvent servir de continuité à des formes de harcèlement existant déjà dans les interactions physiques, mais peuvent également servir de point de départ. Une mauvaise blague débutée par un camarade sur le « mur » d'un autre, un « piratage de compte » laissé ouvert sur un ordinateur, etc. peuvent ouvrir la porte à des moqueries et à un phénomène de stigmatisation. Ce phénomène peut être aggravé vis-à-vis des interactions sociales du quotidien, car le public potentiel peut être bien plus large (d'autres adolescents ou même des adultes peu compréhensifs). Un adolescent non identifié comme tel peut se retrouver assailli de commentaires négatifs d'internautes « lambda » après avoir posté un « tweet » de mauvais goût.
La distance physique induite par le numérique peut aussi éloigner le jeune, qui participe à une forme de harcèlement, des conséquences de ses actes. De plus, une impression d'anonymat peut aussi inciter des adolescents à aller plus loin ou à passer à l'acte, là où ils ne se seraient pas exposés autrement.

#### - Attention au futur

Il n'est pas toujours possible de faire disparaitre les traces que l'on a laissées sur Internet. Même si les services permettent d'en retirer certaines, supprimer une information gênante peut s'avérer très difficile si les données ont été disséminées au travers de différents sites et relayées par de nombreuses personnes. Il est important de prendre cela en compte s'agissant de nos comportements en ligne. Une photo

[34] Contraction de « fishing » (pêche) et « phreaking » (terme désignant le piratage de ligne téléphonique phone-freak).

« rigolote » à un moment de sa vie peut devenir compromettante à un autre. Il n'est pas certain que les photos ou messages ne seront pas retransmis ou sauvegardés ailleurs, ou même que l'on ne perdra pas l'accès à l'outil qui permettrait de le supprimer. Chaque contenu publié implique de faire preuve d'une grande prudence : il peut un jour porter préjudice, et pire porter préjudice à un ami ! Il faut aussi envisager qu'un contenu transmis de façon « privée » puisse un jour être vu par des yeux indiscrets en raison d'un bug ou d'un piratage. Les principaux réseaux sociaux ne facilitent pas la tâche pour nettoyer les traces de son passé et le "droit au déréférencement" (v. III.B.) reste limité.
L'évolution des techniques peut également créer de nouveaux dangers. On peut penser à la reconnaissance faciale, où des logiciels arrivent déjà à identifier facilement une correspondance entre une photo d'une personne dans l'espace public et son profil sur un réseau social. Souhaite-t-on vraiment faciliter cette identification en mettant toujours plus de photos de soi ou de ses proches sur Internet ?

### - Narcissisme, recherche d'attention et surexposition de soi

L'adolescence est une période complexe où les « apparences », les perceptions que les autres ont de nous et que l'on a de soi-même, comptent beaucoup. Pour beaucoup de jeunes, les réseaux sociaux prennent une place centrale dans cette apparence et certains s'y consacrent de façon excessive. Cela peut se traduire par une exposition de leurs moindres faits et gestes, une recherche compulsive des « like » de leurs « amis » avec des photos ou des messages toujours plus racoleurs, une déformation de la vérité pour la rendre plus attractive et potentiellement une absence de prise en considération (et donc d'empathie) des conséquences de messages qui peuvent faire du mal à d'autres personnes, etc.
Ce phénomène peut rester bénin et limité dans le temps, mais il comporte toutefois de sérieux dangers. D'un point de vue du développement de l'individu, cela peut l'enfermer dans une spirale de conformisme avec son image. « *Les autres attendent que je sois cela, je dois ou ne peux pas faire ça (même si j'en ai envie ou pas)* ». Cela peut aussi entrainer l'individu dans une course à la recherche d'attention qui peut s'avérer dangereuse (en réalisant des actions dangereuses ou en se dévoilant trop). Plus généralement, une trop grande importance attachée à l'apparence peut avoir des conséquences désastreuses le jour où « la roue tourne » et que cela se retourne contre la personne[35]. Il est nécessaire de garder une place mesurée à cette apparence numérique et de ne pas se définir qu'à travers d'elle.

## II.B.3. LES RISQUES D'ABUS DANS L'USAGE DES RÉSEAUX

Internet, notamment par le biais des réseaux sociaux, a permis l'exercice d'une véritable liberté d'expression, d'accéder facilement à des informations de différentes sources ainsi qu'à une abondance quasi infinie de contenus (jeux, vidéos, lectures, musique…) et d'outils. Ces possibilités ont toutefois leurs revers.

### - Abus de la liberté d'expression et « trolling »

La liberté d'expression est une liberté fondamentale, mais comme toutes les libertés elle comporte des limites nécessaires pour les équilibres de la vie en société[36]. Ainsi,

[35] On peut citer en exemple fictionnel le premier épisode de la troisième saison de la série Black Mirror : Nosedive.
[36] Cela même aux États-Unis, malgré une croyance fréquente dans le caractère « absolu » du premier amendement.

« l'abus » de la liberté d'expression a toujours été encadré[37]. En France, on sanctionne par exemple l'injure, la diffamation, les provocations à commettre un délit ou les incitations à la haine, le harcèlement, etc. L'essentiel de ces limites trouve une explication simple dans « ma liberté s'arrête là où commence celle des autres ». Les réseaux sociaux offrent des facilités d'expression à tous, et notamment à des personnes qui autrefois n'auraient pas eu cette possibilité. On peut s'en réjouir, néanmoins cela libère également des paroles de haine. De plus, les jeunes accèdent à une parole publique sans en avoir nécessairement compris les enjeux : le poids des mots, les dangers d'une expression abusive, etc. On observe notamment de nombreux propos qui sous couvert « d'humour » vont comporter une grande violence vis-à-vis des personnes à qui ils s'adressent, et ce d'autant plus qu'ils peuvent être répétés (harcèlement par addition). Il n'est pas aisé de se mettre à la place de l'autre et de comprendre qu'il « n'entendra » pas nécessairement ce message comme nous. La distance qu'offre Internet rend facile le fait de s'amuser aux dépens d'autres personnes, de provoquer « pour le lol[38] » (phénomène du « Troll »[39]). Les abus de liberté d'expression sur Internet peuvent donc provenir d'intentions malveillantes, mais également d'une certaine forme d'inconscience ou de manque d'empathie. La formation de la jeunesse à une expression respectueuse (ce qui n'empêche pas la critique !) et bienveillante sur les réseaux est en tout cas un enjeu conséquent.

### - De fausses informations mensongères et dangereuses

La facilité d'accès et de production d'informations a son contrecoup : la fabrication de « fausses informations » et leur diffusion. Les intentions peuvent être humoristiques sans que cela pose de problèmes si c'est clairement exprimé[40], mais elles peuvent aussi être de réaliser une véritable désinformation et d'influencer l'opinion publique. Détecter ces fausses informations n'est pas chose aisée, particulièrement pour la jeunesse[41], et demande souvent un important travail pour lutter contre ses propres préjugés[42], vérifier l'information et exercer un véritable esprit critique. Relayer une information mensongère peut participer à construire des opinions ne s'appuyant donc pas sur des faits établis. Cela peut aboutir à influencer de nombreuses personnes, mais également à déstabiliser des esprits trop crédules et les pousser dans des approches dénuées de toute réalité et notamment dites « conspirationnistes ». Dans un réseau où l'information est libre, il est de la responsabilité de chacun d'évaluer les informations qu'il reçoit et de ne pas relayer n'importe quoi (en y apportant donc son crédit).

### - Addiction numérique, perte de temps et de concentration

La rengaine est trop souvent entendue : Internet, les jeux vidéos, les réseaux sociaux, etc. seraient responsables de tous les maux : addiction et dépendance, violence, perversion, etc. Ces discours alarmistes, parfois réactionnaires, doivent

---

[37] « Liberté d'expression et ses limites », Internet responsable – eduscol, 4 oct. 2016.
[38] Contraction de « Laughing Out Loud », l'expression « lol » est utilisé pour signaler initialement le rire, l'amusement dans les communications textuelles sur Internet.
[39] Entrée « Troll (Internet) ». Wikipédia Fr, dernière édition 15 décembre 2016.
[40] Il est toutefois facile de se faire avoir si la fausse information confirme un de ses préjugés, ainsi au début du « Gorafi », je m'étais fait avoir par l'information « Trop souriant dans le métro il finit en garde à vue », la prenant pour un fait.
[41] M. Tual, « Fausses informations en ligne : les adolescents « facilement dupés », selon une étude ». Le Monde.fr, 23 novembre 2016.
[42] P. Sastre, « Pourquoi s'offusquer de la post-vérité ? C'est le mode par défaut de notre cerveau ». Slate.fr, 4 janvier 2017.

impérativement être modérés, ils agitent des généralisations abusives pour tenter de discréditer massivement des pratiques. Cependant, comme toute pratique, celle des réseaux sociaux peut être raisonnable ou excessive. Il est indéniable qu'il existe des comportements abusifs et de nombreux travaux témoignent de l'existence de comportements addictifs et de dépendance aux réseaux sociaux[43]. Ces cas extrêmes peuvent avoir des conséquences extrêmement délétères sur la vie des individus et requérir des soins, ils restent encore rares. Néanmoins, il n'est pas évident pour quiconque, encore moins pour les jeunes, de maitriser le temps consacré aux réseaux sociaux et les conséquences sur sa vie. Cela a été dit, l'intérêt des entreprises disposant de réseaux sociaux est de vous y faire revenir aussi souvent que possible[44] et d'y passer un maximum de temps pour des raisons économiques[45]. Pour cela, elles peuvent jouer sur des mécanismes neuronaux (activation des circuits de la récompense, présentation surtout de contenus positifs, etc.) et il n'est pas forcément évident de bien contrôler ses usages. Attribuer la « juste » place aux réseaux sociaux (celle qui nous semble adaptée) demande un véritable travail, une réflexion profonde et potentiellement requiert même d'être appuyée par une aide humaine ou par d'autres outils (III.A.2).

[43] Voir en ce sens, A.-S. Glover-Bondeau, « Dépendance aux écrans : les clefs pour s'en sortir », 15 janvier 2015 et ses références.
[44] Voir Eyal, Nir Morechay, et Ryan Hoover. Hooked: how to build habit-forming products. London, Royaume-Uni, Portfolio Penguin, 2014.
[45] A. Maruani, « Le grand entretien : Tristan Harris : "Des millions d'heures sont juste volées à la vie des gens" », Rue89, 4 juin 2016.

# III. Un usage pertinent, sécurisé et raisonné des réseaux sociaux

Transmettre une compréhension extensive des enjeux développés ici, de bonnes pratiques, un regard critique, etc. et particulièrement à la jeunesse est une tâche ardue. Chacun a sa propre pratique des réseaux sociaux, ses attentes, ses besoins, etc. Chaque expérience est différente. Bien entendu, il reste possible et nécessaire de sensibiliser sur ces sujets, mais l'évolution des pratiques ne pourra être forcée par la contrainte. Les réseaux sociaux sont souvent pour les jeunes des espaces de liberté et un contrôle extensif, une approche trop moralisatrice, trop ancrée dans la sanction apparaît peu efficace. Les jeunes ont déjà majoritairement pris des mesures de contrôle de ces « extériorisations d'eux-mêmes », ne serait-ce que par nécessité pratique.

Au-delà de la sensibilisation, de l'explication des problèmes pour espérer des prises de conscience, la découverte de notions ignorées, il s'agit donc surtout d'essayer de renforcer leur « pouvoir de maitrise de leur vie numérique », leur « autodétermination informationnelle ».

Au-delà d'une écoute, si possible individuelle, des problèmes rencontrés par chacun, il est pertinent de détailler les outils et méthodes qui leur permettent de se protéger, de faire comprendre qu'ils disposent d'éléments pour se défendre face à ces risques. On peut transmettre les bases d'une hygiène et autodéfense numérique (A.), enseigner des droits et devoirs applicables en la matière (B.) et donner des clefs d'autodéfense intellectuelle (C.).

## III.A. UNE NÉCESSAIRE MAITRISE DES OUTILS ET DES PARAMÈTRES

Limiter les problèmes engendrés par les réseaux sociaux est un problème sociétal qui requiert des décisions collectives. Il est toutefois possible de participer à ce travail à l'échelon individuel, ne serait-ce que pour se protéger « égoïstement » de conséquences dommageables. Une telle démarche implique d'essayer de comprendre les mécanismes intellectuels de ces outils, et également de maitriser leurs fonctionnalités. Il s'agit de ne plus être passif et seulement "subir" ces outils. Pour cela d'autres outils tiers peuvent aider.

### III.A.1. MAITRISER LA TRANSMISSION DES DONNÉES PERSONNELLES

#### - Adopter une bonne hygiène numérique

Avant de développer les outils et méthodes permettant de protéger ses données sur les réseaux sociaux, il est préférable de revenir sur quelques notions de base en informatique. Des conseils préliminaires qui peuvent éviter de nombreux problèmes dans beaucoup de cas. Sans maitrise de ces notions, les autres protections qui pourront être mises en place peuvent facilement être vaines.

- **Réaliser des sauvegardes.**

S'il y a des informations que l'on souhaite conserver ou protéger : il ne faut pas oublier que nos appareils sont faillibles et qu'il est nécessaire de réaliser des sauvegardes.

- **Protéger ses appareils et ses données.**

Les appareils récents proposent des protections faciles permettant d'éviter à un tiers d'accéder « trop » facilement à nos données. Il est bon de les utiliser. Il est ainsi bienvenu de configurer une méthode de déverrouillage sur son appareil (schéma de déblocage, code de session, etc.) et de chiffrer ses données[46]. Il est important de penser à se déconnecter à la fin de l'utilisation du réseau social, surtout si on est sur un ordinateur public et d'utiliser la « navigation privée » pour limiter ses traces.

- **Adopter des phrases de passe[47].**

Les mots de passe, plus c'est long, plus c'est efficace. Malheureusement, la mémoire est capricieuse et il est difficile de se rappeler de nombreux mots de passe complexes et longs. Il est préférable de disposer d'un mot de passe long et facile à retenir (unephrasetrivialeparex. ou des mots aléatoires[48]) que d'un mot de passe très court même s'il est aléatoire. Il est en tout cas fondamental que les mots de passe des services les plus critiques soient différents (deux réseaux sociaux où l'on est très investi par exemple).

- **Activer l'authentification en 2 étapes.**

La plupart des services de réseaux sociaux permettent de protéger votre compte par un mécanisme d'authentification en 2 étapes. Ce mécanisme exigera, en plus du mot de passe, un autre élément quand vous vous connectez à un nouvel appareil (souvent un code transmis par texto). C'est un bon moyen de protection pour éviter que quelqu'un accède illégitimement à votre compte. Pour sécuriser le réseau social, il est nécessaire de sécuriser également le courriel qui y est rattaché : activez-y également l'authentification en 2 étapes.

- **Segmenter ses usages et ses différents comptes.**

Bien qu'il soit tentant de tout connecter à son compte Google ou Facebook pour limiter les mots de passe à retenir et les procédures d'identification cette pratique est à proscrire. Elle confère bien trop de pouvoir à ces acteurs et si un seul compte est compromis, tous les autres services suivront. Il est préférable de continuer à créer des comptes distincts, avec des informations et mots de passe différents. Il s'agit aussi d'éviter qu'ils puissent être facilement liés les uns aux autres si cela ne sert à rien. Cela permet de plus d'expérimenter différentes représentations de soi sans être jugé sur l'ensemble.

- **Limiter les informations transmises et utiliser des pseudonymes.**

On transmet déjà par défaut énormément d'information sur soi en surfant sur Internet et en agissant sur les réseaux sociaux. Nul besoin d'en donner plus, bénévolement. Pour chaque questionnaire, demande d'informations personnelles, on va chercher à distinguer ce qui est obligatoire et facultatif. Même si l'information est présentée comme obligatoire, il convient de s'interroger : en ont-ils réellement besoin ? S'il n'y a aucune légitimité ou raison à la demande, on peut choisir de donner des données inexactes ou incomplètes. De la même façon, l'usage de pseudonymes peut vous protéger s'ils sont bien employés.

---

[46] Le chiffrement des données ne sera pas détaillé ici, mais il peut être extrêmement simple sur la plupart des ordiphones et doit donc être recommandé.

[47] Pour plus de détails s'agissant de la gestion des mots de passe, voir la fiche pratique du Cecil qui y est consacrée.

[48] Voir en ce sens le strip d'XKCD « Password Strength »

- **Mettre à jour ses applications.**

Dans l'essentiel des cas, les mises à jour de sécurité[49] proposées par votre appareil ou vos applications sont là pour protéger l'utilisateur : une faille a été découverte et la mise à jour vient la combler. Si l'on ne l'applique pas, on risque de devenir une cible, la faille étant désormais connue.

- **Se méfier légitimement, même de ses amis.**

La confiance dans les autres est absolument nécessaire et il ne faut pas devenir paranoïaque (et encore moins sans raison valable). Attention toutefois à ne pas confondre confiance et inconscience. Quelqu'un qui est un ami un jour, peut ne plus l'être le lendemain (même si cela peut n'être que temporaire : tout le monde peut changer), des sentiments peuvent être simulés, etc. **Sans motif légitime, on ne confie pas ses mots de passe**, même à ses amis, et on ne confie pas plus "en gage de confiance" des fichiers compromettants pour vous (par exemple des photos explicites). **La confiance se construit aussi dans le respect de l'intimité de l'autre**.

### - Maitriser et régler ses applications et leurs paramètres

Les principaux réseaux sociaux sont paramétrables. Bien évidemment il est important d'aller consulter les paramètres relatifs à la confidentialité, à la sécurité et à la vie privée. Malheureusement, les entreprises gestionnaires de réseaux sociaux ne choisissent que rarement « par défaut » les plus protecteurs. Les autres paramètres, mot de passe et authentification en 2 étapes, les notifications, les permissions, etc. peuvent aussi contenir des réglages importants qui permettent de se protéger. Pour prendre l'exemple de Facebook, tous les onglets des paramètres ont leur importance :

- « Général » : accès à une archive contenant théoriquement la copie de « toutes » ses données, à la modification du mot de passe et du mail de contact classique et publicitaire.
- « Journal et identification » ainsi que « publications publiques » : de nombreux paramètres qui sont en réalité des paramètres de confidentialité.
- « Notifications » : permet de désactiver des notifications inutiles et dérangeantes qui peuvent limiter la concentration et à l'inverse d'activer des notifications de sécurité.
- « Mobile », « Applications », « paiements » et « vidéos » : certains paramètres peuvent avoir des implications fortes en matière de sécurité. Il est bon de les consulter.
- « Publicités » : permet de s'opposer aux publicités ciblées, mais aussi de consulter les « préférences publicitaires » : les points d'identification que Facebook accepte de vous transmettre et qui servent à vous cibler.


[49] Malheureusement dans le cas des applications, il peut y avoir des mises à jour de fonctionnalités qui peuvent même demander des « permissions d'accès » plus extensives.

Il faut avoir conscience des limites de ces paramètres contre la surveillance du réseau lui-même ou de ses autres conséquences néfastes. Malgré tout, il est nécessaire de maitriser ses paramètres et de les consulter régulièrement pour tenter de se protéger au mieux contre les tiers et comportements non désirés. Prendre un petit temps pour vraiment se renseigner sur les possibilités et le cadre d'un outil que l'on utilise quotidiennement n'est pas un luxe, **c'est une nécessité**.

Bien évidemment, les paramètres spécifiques de sécurité et de confidentialité/vie privée sont les plus importants.

Un des enjeux conséquents en matière de confidentialité et de bien comprendre l'audience de ses publications et actions sur le réseau social. À qui je m'adresse ? Dans quel cadre ? Qui peut voir ce que je publie ? Dans quelle mesure cela peut-il être vu par d'autres personnes ? Est-ce que je souhaite que mes « like » et nouveaux contacts soient connus de tous ? Est-ce que j'accepte que mes amis puissent épier mes cycles de sommeil [50]? Etc.

À titre d'exemple, les « amis des amis » peuvent représenter une partie conséquente des personnes que l'on peut croiser au quotidien sans forcément avoir de volonté d'interagir avec elles. De la même façon, un « tweet » peut facilement être relayé par un compte très suivi et se retrouver avec une audience phénoménale.




How One Stupid Tweet Blew Up Justine Sacco's Life

By JON RONSON FEB. 12, 2015

Ces questionnements doivent être posés et si beaucoup de jeunes y font déjà attention, il faut sensibiliser ceux pour qui ce n'est pas le cas. C'est un élément fondamental qui s'appuie sur un travail régulier et continuel : les paramètres et conditions peuvent changer. Un petit tour régulier dans les listes d'utilisateurs de ses groupes Snapchat, des personnes qui ont accès au mur Facebook, etc. peut éviter bien des problèmes futurs !

Cela vaut la peine de rappeler de « nettoyer » régulièrement : pas besoin de laisser dans notre profil / sur notre flux d'actualité un message ou une photo qui ne sera plus consultée dans son juste contexte et qui pourrait nous causer du tort.

Il est également pertinent de regarder les « permissions » demandées par les applications de réseaux sociaux : est-il forcément légitime qu'un service de

[50] G. Kristanadjaja, « Comment Facebook permet de savoir si vos amis dorment bien la nuit ». Libération.fr, 29 février 2016.

messagerie par texte puisse accéder à l'ensemble de la mémoire ainsi qu'aux fonctions d'enregistrements vidéo et audio ? Il est difficile d'agir sur ses permissions sans outils adaptés, mais avoir conscience des possibilités de vos outils reste une nécessité. Cela devrait, a minima, questionner la nécessité de leurs usages.

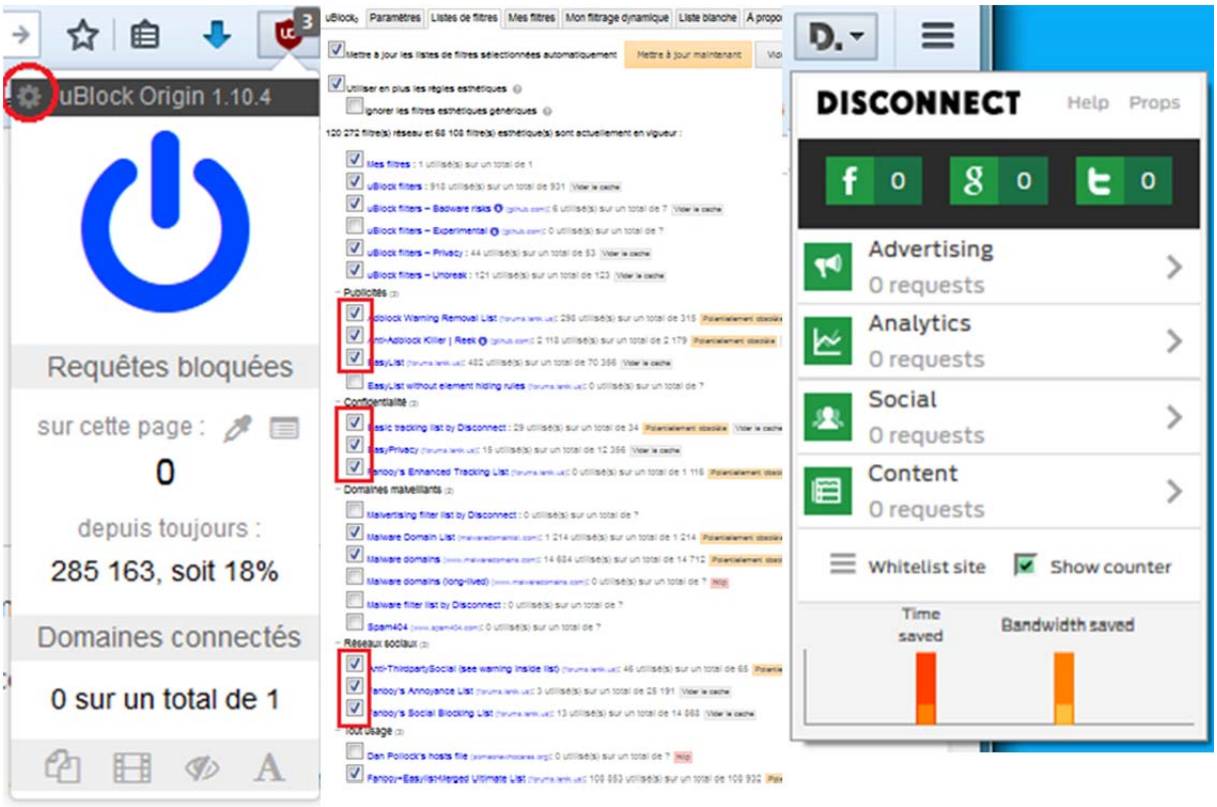
**- Limiter la surveillance des réseaux sociaux : bloquer les tentatives de traçage**

Afin d'éviter que le réseau social ne vous connaisse trop bien, la première bonne pratique est de ne pas lui donner volontairement trop d'informations. Néanmoins, les réseaux sociaux peuvent examiner vos comportements sur leurs outils, mais également en dehors. En effet, par des mécanismes de « cookie – tiers » ils peuvent tracer leurs utilisateurs (et même des utilisateurs non-inscrits) à travers le Web.

Il existe une méthode très simple pour limiter fortement cela. Installer des outils qui vont bloquer cette traque.

On peut conseiller d'installer le navigateur « Firefox » (disponible également sur mobile), de la fondation Mozilla, qui s'engage en faveur de la protection de la vie privée.
Il suffit ensuite de lui adjoindre deux modules supplémentaires : principalement uBlock Origin (qui a l'avantage de bloquer également les publicités) et Disconnect.

Par défaut, ces deux outils vont bloquer de nombreuses méthodes de surveillance privée et sont facilement configurables par un rapide tour dans les paramètres pour leur faire éliminer l'essentiel des traqueurs en ligne.



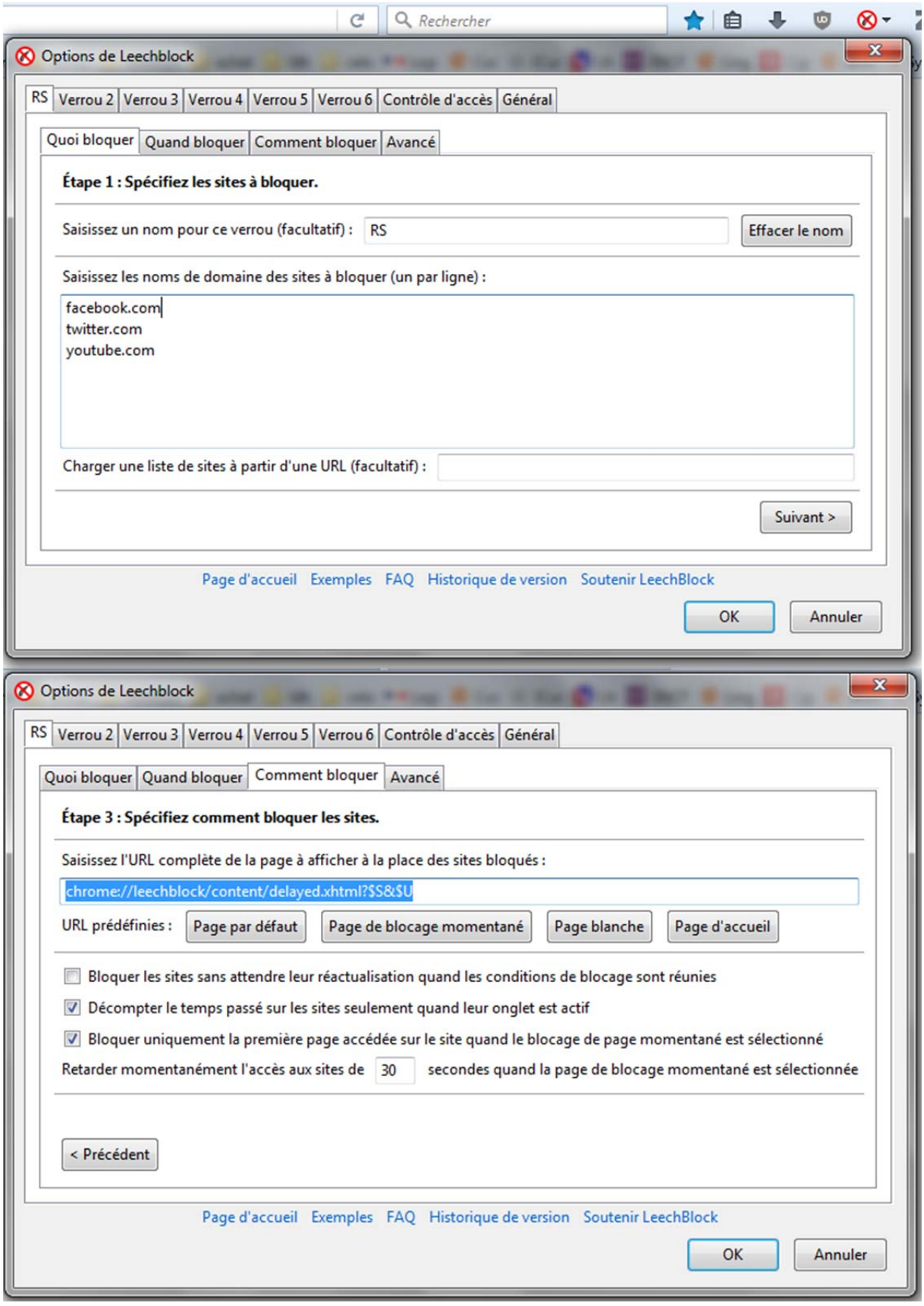
### III.A.2. MAITRISER SES TEMPS D'USAGE

Il n'est pas évident d'arriver à garder les réseaux sociaux à la bonne place dans notre vie, celle que l'on souhaite. Il est facile d'y passer plus de temps que prévu, de s'y "perdre". Il semble inadéquat et peu efficace de dire à des jeunes de passer « moins de temps » sur les réseaux sociaux. Néanmoins, si certains d'entre eux reconnaissent y passer trop de temps (cette interrogation peut être soulevée) et le désir de mieux encadrer leur pratique, il convient de donner des pistes pour les y aider[51].

Une meilleure maitrise de ces outils requiert d'adopter de bonnes habitudes d'hygiène de vie. Pour citer quelques exemples : ne pas se coucher avec son ordiphone, ne pas l'allumer et le regarder dès le réveil, le mettre en mode avion quand on n'a pas besoin de la connexion ou l'éteindre quand il ne sert à rien, limiter drastiquement les notifications « subies » des réseaux sociaux (aussi bien sur ces sites que sur l'ordiphone) en les supprimant ou en évitant de regarder son téléphone pour tout (une montre basique donne l'heure sans imposer de notifications !), etc.

Afin de faciliter cette maitrise, on peut également mettre en place des outils de suivi du temps passé sur ces réseaux. Le module « Leechblock » pour Firefox offre des possibilités conséquentes pour s'aider à limiter ses usages. Il peut étudier le temps investi sur les sites indiqués et, si vous le souhaitez, peut bloquer l'accès « automatique » à ceux-ci de façon plus ou moins contraignante.

[51] Il convient d'aider les personnes souhaitant remettre ces services à une place plus limitée dans leur vie. Attention, cela ne signifie pas pour autant que la responsabilité des abus des réseaux sociaux leur incombe : tout est fait pour que l'on « perde » du temps sur ces services et il s'agit là d'un enjeu de politique publique. Voir en ce sens les travaux de Tristan Harris précités et sur son blog : http://www.tristanharris.com.


Rechercher
Options de Leechblock
RS
Verrou 2
Verrou 3
Verrou 4
Verrou 5
Verrou 6
Contrôle d'accès
Général
Quoi bloquer
Quand bloquer
Comment bloquer
Avancé
Étape 1 : Spécifiez les sites à bloquer.
Saisissez un nom pour ce verrou (facultatif) :
RS
Effacer le nom
Saisissez les noms de domaine des sites à bloquer (un par ligne) :
facebook.com
twitter.com
youtube.com
Charger une liste de sites à partir d'une URL (facultatif) :
Suivant >
Page d'accueil
Exemples
FAQ
Historique de version
Soutenir LeechBlock
OK
Annuler
Options de Leechblock
RS
Verrou 2
Verrou 3
Verrou 4
Verrou 5
Verrou 6
Contrôle d'accès
Général
Quoi bloquer
Quand bloquer
Comment bloquer
Avancé
Étape 3 : Spécifiez comment bloquer les sites.
Saisissez l'URL complète de la page à afficher à la place des sites bloqués :
chrome://leechblock/content/delayed.xhtml?$S&$U
URL prédéfinies :
Page par défaut
Page de blocage momentané
Page blanche
Page d'accueil
Bloquer les sites sans attendre leur réactualisation quand les conditions de blocage sont réunies
Décompter le temps passé sur les sites seulement quand leur onglet est actif
Bloquer uniquement la première page accédée sur le site quand le blocage de page momentané est sélectionné
Retarder momentanément l'accès aux sites de
30
secondes quand la page de blocage momentané est sélectionnée
< Précédent
Page d'accueil
Exemples
FAQ
Historique de version
Soutenir LeechBlock
OK
Annuler

Pour les ordiphones, il existe également des applications permettant d'étudier ses habitudes et de bloquer certaines applications en cas d'abus. On peut citer[52] : RescueTime, Offtime, AppDetox, BreakFree, Moment. Elles peuvent donner un sérieux coup de main pour se rendre compte de ses pratiques et s'aider à les modifier.

### III.A.3. UTILISER DES RÉSEAUX SOCIAUX PLUS RESPECTUEUX DE LA VIE PRIVÉE

De nombreux problèmes découlant des réseaux sociaux proviennent de la nature et des objectifs de leurs exploitants : monétiser votre vie privée. Face à ce constat, des projets se sont montés pour développer des réseaux sociaux qui conserveraient les avantages des outils existants tout en étant plus respectueux de la vie privée et des libertés individuelles de leurs membres. Ils visent notamment à décentraliser les informations, pour éviter qu'une seule entité détienne les informations de tout le monde, à assurer une confidentialité réelle des échanges et à ne pas exploiter commercialement la vie privée des utilisateurs.

Il existe différents projets, plus ou moins aboutis[53], pour exemple, deux recommandations[54] :

- Diaspora, une alternative à Facebook, développé par la fondation Diaspora (sans but lucratif) qui est ancrée dans une volonté de protéger la vie privée. Il est possible de rejoindre ce réseau par différents « pods » : les serveurs qui hébergent les données d'utilisateurs et offrent un point d'entrée pour accéder à l'ensemble du réseau. On peut recommander de passer par le pod de l'association Framasoft : Framasphere.org.

- Le projet Movim.eu est assez prometteur en termes de fonctionnalités, mais il dispose d'un assez faible nombre d'utilisateurs. Il propose toutefois des passerelles aisées vers les autres réseaux sociaux (Facebook, Twitter…) afin de pouvoir adopter une approche progressive.

Force est de reconnaitre que ces réseaux sont encore loin de provoquer l'adhésion du grand public et peuvent difficilement être recommandés « tels quels » à des adolescents. Il reste pertinent de les interroger sur les outils qu'ils utilisent, de savoir si une autre solution plus respectueuse ou même moins « technique » ne pourrait pas satisfaire le même besoin[55].

S'agissant des usages « réseaux sociaux » de messagerie sur ordiphone, les applications ne manquent pas et de nombreux acteurs qui se positionnent sur la protection de la vie privée de leurs utilisateurs apparaissent. Pour remplacer les applications de discussion trop « bavardes » on peut suggérer[56], Riot, Silence, Signal ou Wire. Il est surtout important de continuer à faire de la veille sur ces outils et promouvoir des outils toujours plus respectueux.

---

[52] Une liste conséquente est disponible ici : http://alternativeto.net/software/appdetox/
[53] Pour les plus respectueux de la vie privée on peut voir : https://prism-break.org/fr/all/#social-networks
[54] Des informations supplémentaires sur la fiche pratique du Cecil « des réseaux sociaux alternatifs ».
[55] Et même de voir s'il s'agit réellement d'un besoin ou seulement d'une habitude peu utile
[56] Il ne s'agit que de suggestions, chacune de ses propositions a par ailleurs ses limites (fonctionnalités, compatibilité, facilité d'usage…), mais elles apparaissent comme bénéfiques pour les droits de l'utilisateur face à WhatsApp par exemple.

La proposition d'utiliser des outils alternatifs ne peut qu'être complémentaire de la sensibilisation aux bonnes pratiques qui est fondamentale.

## III.B. QUELLES RÈGLES, QUELS DROITS, QUELS DEVOIRS ?

Internet n'est pas une zone de non-droit : un grand nombre de règles existent qui viennent protéger la vie privée et donner un cadre à la liberté d'expression. Au-delà de ces règles contraignantes, les réseaux sociaux requièrent un véritable effort, en raison de la distance qu'ils provoquent, pour se mettre à la place de l'autre et rester respectueux en toutes circonstances.

### III.B.1. LA VIE PRIVÉE : UNE LIBERTÉ PROTÉGÉE

La protection de la vie privée est une liberté fondamentale reconnue notamment par le Code civil en son article 9 « chacun a le droit au respect de sa vie privée » ainsi que par l'article 12 de la Déclaration universelle des droits de l'homme « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

C'est une liberté importante interconnectée avec d'autres qui en découlent : la liberté d'opinion, la liberté d'expression, la protection du secret des correspondances, la protection du domicile, etc.

Pour assurer la réalité de cette protection, des règles existent et notamment les articles 226-1, -2 et -2-1 du Code pénal :

> « Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :
> 1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
> 2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.
> Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé. »

Pour le -2 :

> « Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1. »

Et le récent -2-1 qui sanctionne expressément la diffusion d'élément touchant à l'intimité sexuelle d'une personne sans que celle-ci n'y ait consentie :

> « Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende.

> Est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1. »

Ainsi, les propos et photos échangés de façon privée qui constituent des morceaux de l'intimité d'une personne sont protégés par le droit et quelqu'un qui les transmettrait sans consentement à des tiers réalise une infraction et peut être sanctionné.

Les intrusions et les modifications illégitimes (« frauduleuses ») qui peuvent être effectuées sur un outil informatique sont également sanctionnables[57]. Ainsi, le simple « piratage » basique d'un compte d'un réseau social laissé ouvert sur un ordinateur, la récupération de données présentes sur une clef USB à laquelle on sait qu'on ne devrait pas accéder, l'utilisation d'une faille (technique ou humaine, ex. : « deviner » le mot de passe de quelqu'un) pour accéder à des données d'un autre utilisateur, etc. sont prohibés.

Au-delà de ces protections, une loi a été spécialement créée pour protéger les « données à caractère personnel » face aux évolutions permises par l'informatique, la loi « Informatique et libertés » du 6 janvier 1978 (« LIL »).

### III.B.2 LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

La loi « informatique et libertés » prévoit un régime d'encadrement et de protection complet des données personnelles des citoyens. Elle a mis en place une autorité, la CNIL (Commission nationale de l'informatique et des libertés). Elle a également soumis les responsables de « traitement de données à caractère personnel » au respect d'un certain nombre d'obligations contraignantes et protectrices des individus. Enfin, elle prévoit des droits positifs dévolus aux personnes qui peuvent les exercer pour se protéger.

Ainsi, chaque citoyen dispose :

- d'un droit d'accès (article 39 LIL), qui lui permet de demander à tout responsable de traitement d'accéder aux données personnelles détenues le concernant.
- d'un droit de rectification et de correction (article 40 LIL), qui vient compléter le droit d'accès en permettant de demander la rectification des informations inexactes.
- d'un droit d'opposition (article 38 LIL), qui permet de s'opposer, pour des motifs légitimes (ce n'est donc pas toujours possible), à figurer dans un traitement et de s'opposer à ce que les données vous concernant soient diffusées, transmises ou conservées.

[57] Articles 323-1 et s. du Code pénal sur les « atteintes aux systèmes de traitement automatisé de données » :
323-1 : « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende. »
323-3 : « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. »

Plus récemment, une décision de la Cour de justice de l'Union européenne du 13 mars 2014 a reconnu en s'appuyant sur ces droits préexistants la possibilité pour un internaute d'obtenir le « déréférencement » de contenus le concernant sur Internet.
La presse a pu parler de « droit à l'oubli ». Ce droit au déréférencement permet en pratique de demander, notamment aux moteurs de recherche et réseaux sociaux, de « désindexer » des contenus qui contiennent des données vous concernant. Cela peut éviter que ces contenus puissent être facilement trouvés par une simple recherche d'éléments d'identification (nom et prénom) sur ces outils. Ce droit est évidemment encadré en raison de problématiques d'accès et de droit à l'information. Il constitue néanmoins un outil important pour un adolescent sur lequel des éléments problématiques se retrouveraient diffusés sur différents sites sans qu'il ne puisse faire supprimer les contenus par un autre biais.

Enfin, la loi « pour une république numérique » de 2016 et un récent règlement européen pour la protection des données institue un « droit à la récupération » et à « la portabilité des données » qui sera applicable fin mai 2018. Celui-ci devrait notamment permettre d'exiger d'un réseau social qu'il nous transmette toutes les données que nous lui avons confiées dans un format aisément réutilisable pour pouvoir, par exemple, les importer sur un autre réseau social plus respectueux.

Ces droits offrent de réelles possibilités d'actions aux citoyens, d'autant plus qu'ils sont appuyés par des obligations conséquentes pour les responsables de traitement qui sont malheureusement trop souvent bafouées.

Il est toutefois possible de les utiliser pour faire respecter avec vigueur sa vie privée et éviter les abus.

### III.B.3. DES LIMITES À LA LIBERTÉ D'EXPRESSION SUR LES RÉSEAUX SOCIAUX

Au même titre que la vie privée, la liberté d'expression est une liberté fondamentale proclamée notamment par :
Les articles 10 et 11 de la Déclaration des droits de l'homme et du citoyen de 1789 :

> « (10) Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la Loi.
>
> (11) La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi. »

L'article 10 de la Convention européenne des droits de l'Homme de 1950 :

> « 1 - Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière.
> 2 - L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de

la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire. »

On le voit facilement : ces textes protègent la liberté d'expression, mais fixent expressément des limites en cas d'abus. En effet, la liberté d'expression ne doit pas servir à piétiner les libertés des autres citoyens, dont le droit à la tranquillité, à la vie privée, etc.

Le droit pénal interdit ainsi notamment :

- Les atteintes à l'intimité et à la vie privée (vues précédemment)
- La diffamation : toute allégation ou imputation d'un fait qui porte atteinte à l'honneur de la personne.
- L'injure : toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait.
- Les provocations à commettre des crimes ou des délits dans certaines conditions.
- Les apologies des crimes les plus graves (crimes de guerre, crimes contre l'humanité, terrorisme).
- Les appels à la haine ou à la discrimination (pour des motifs religieux, sexuels, etc.)
- Certaines formes de harcèlement contre autrui, qui peuvent même être constituées par un seul message.

Toutes ces infractions sont des délits qui peuvent conduire quelqu'un en prison[58]. Une simple insulte publique d'un camarade de classe peut justifier une plainte et un renvoi devant le juge compétent. Ce « risque » pénal ne doit toutefois pas être le premier pris en compte, ces infractions visent surtout à protéger indirectement les individus contre les conséquences néfastes d'expression abusive. Ainsi, il parait important d'insister sur la réalité des rapports humains et des personnes qui échangent sur les réseaux pour que chacun tâche d'être respectueux, et ce bien au-delà de la loi.

### III.B.4. AU-DELÀ DU SEUL DROIT : DES DEVOIRS MORAUX

Les réseaux sociaux offrent une réelle facilité d'expression et un contact facile avec de nombreuses personnes. Cela peut être quelques contacts, mais peut aussi facilement être le monde entier, en passant par les « amis des amis » (qui constituent aussi un très grand nombre de personnes). Il n'est du coup pas forcément évident de savoir quel ton y adopter.

De la même façon qu'il peut être important de « tourner cinq fois sa langue dans sa bouche avant de parler », il est préférable de prendre un temps de réflexion avant de « poster ».

On peut ainsi se poser certaines questions :
*Est-ce que ma publication à un intérêt pour moi ou pour les autres ? Quel est l'objectif de ce message ? Ce message ou son ton peut-il offenser, manquer de*

[58] Exception faite de la diffamation et de l'insulte quand elles sont réalisées dans un cadre privé qui ne sont passibles que d'une contravention.

*respect ou blesser quelqu'un ? À qui s'adresse-t-il ? Qui pourra le voir ? S'il venait à être divulgué publiquement ou à être vu par une audience conséquente, cela me gênerait-il ? Risque-t-il d'être mal compris par certains ? Peut-il se retourner contre moi ? Suis-je sûr de ce que je dis ? Est-ce que les éléments que j'y diffuse peuvent gêner d'autres personnes ? Etc.*
Si les services de messagerie où la durée de vie des messages est limitée peuvent circonscrire certains risques, ils ne les annulent pas et ne dispensent pas des questionnements liés au respect des autres.

Il faut, par exemple, faire très attention à la vie privée des autres : seraient-ils contents que je diffuse cette photo ou ces informations sur eux ? Protéger sa vie privée c'est bien, mais c'est encore plus important de protéger celles des autres !

Une bonne communication implique de se mettre à la place de son auditoire, d'être empathique. Il s'agit déjà de ne pas infliger ce que l'on ne souhaite pas recevoir (des insultes, du spam, des critiques non constructives, etc.). Il est de surcroît préférable d'essayer de se mettre réellement à la place de l'autre et de respecter ces attentes et besoins propres. Cela veut dire de ne pas forcément infliger, imposer, ce qui pourtant nous conviendrait (exemple : de l'humour déplacé, une attention particulière non souhaitée, etc.). Cela demande un réel effort en présence d'une multitude d'auditeurs, les mots (et toute expression) ont une force, il faut y faire attention ! Tâcher autant que possible d'être bienveillant envers ses interlocuteurs ne peut jamais faire de mal !

La liberté d'expression est un droit à chérir et à utiliser avec parcimonie, l'attention des autres, leur énergie et leur bien-être sont précieux, il faut les respecter.

Il est aussi important de rester attentifs aux autres sur les réseaux sociaux. Ce n'est pas parce que les échanges sont numériques qu'ils ne sont pas réels. Ainsi, **si un ami se comporte bizarrement** par rapport à ses habitudes, exprime des sentiments très sombres ou autre **il faut s'interroger, ouvrir la discussion ou éventuellement le signaler à une personne compétente** si cela semble vraiment inquiétant.

## III.C. PROMOUVOIR LE DIALOGUE ET LA PENSÉE CRITIQUE FACE À LA DÉSINFORMATION

### III.C.1. S'INFORMER SUR LES RÉSEAUX SOCIAUX : CROISER LES INFORMATIONS.

Internet joue un rôle conséquent sur les équilibres médiatiques d'accès à l'information. La production d'information était précédemment le privilège d'un certain nombre de médias centralisés qui étaient les seuls canaux d'accès à ces nouvelles. Cela leur a offert un important pouvoir et leur a permis de contrôler largement ce « qu'est l'information ». Si des faits ne rentrent pas dans la ligne éditoriale, ils peuvent ne pas être traités ou sous un angle qui convient mieux à ses dirigeants.
Les médias sont un pouvoir et il est nécessaire de les questionner. Il ne faut pas croire dans une réelle « neutralité » de l'information, mais au contraire essayer de rechercher la compréhension complexe d'un sujet obtenue en croisant différentes sources d'informations et plusieurs points de vue. Tout au plus, on peut attendre d'un certain type de journalisme une « recherche d'objectivité », en présentant différents camps, des contre-arguments et en adoptant certaines règles de la recherche scientifique. Il n'en reste pas moins que les plus grands médias (télévision, radio,

papier) sont des entreprises soumises aux volontés de personnes qui les détiennent. Cette détention n'est pas gratuite et les propriétaires de ses médias espèrent en tirer des avantages, qu'il s'agisse uniquement de profits financiers ou d'un poids politique[59]. Néanmoins, les grands médias centralisés ont un avantage : ils sont soumis à une certaine responsabilité, peuvent être contactés, on peut les critiquer, connaitre leur ligne éditoriale, les attaquer en justice s'ils ne respectent pas la loi, etc.

Internet permet à tous de devenir un média. De créer facilement un site qui va diffuser de l'information : cela a provoqué un changement complet de paradigme dans la possibilité de produire et d'accéder à l'information.

On a pu voir certains des problèmes qui en découlent : de la désinformation, des informations de piètre qualité ne respectant pas le socle des valeurs journalistiques, une surproduction d'information et une concurrence sur le « temps d'attention » (qui résulte aussi en production de contenus « leurres à clic » de faible intérêt), etc.

Il n'est pas facile de profiter des multiplications et diversifications des sources d'informations sans tomber dans ces écueils.

Le problème s'est de plus renforcé avec l'évolution de certains réseaux sociaux (principalement Facebook, YouTube et Twitter) vers des plateformes exclusives d'accès à l'information. Ces services permettent en effet d'obtenir des informations qui vont provenir ou être relayées par ses « amis » et contacts sans forcément sortir du réseau. Ces plateformes recréent ainsi une forme de centralisation dans l'accès à l'information en pouvant adapter pour chacun les informations reçues. Cela leur offre un pouvoir conséquent (voir II.A.2.) sur lequel il faut demeurer critique.

Il est donc important de ne pas se tenir à une seule plateforme pour s'informer, ainsi que de diversifier ses sources et de les recouper.

### III.C.2. LIMITER L'ENTRE SOI ET LA BULLE DE FILTRE

En 2011, Eli Pariser publiait un ouvrage étudiant les conséquences, notamment des réseaux sociaux, dans la création de ce qu'il appelle une « bulle de filtre »[60]. Le concept est depuis largement repris. On peut toutefois douter de ses réels apports scientifiques, en effet, les notions « d'entre soi » sont depuis longtemps connues et étudiées. Malgré tout, les enjeux qu'il décrit sont importants.

Les réseaux sociaux (comme notre milieu social, les choix d'établissements scolaires, etc.) vont avoir tendance à ne nous présenter que ce que nous souhaitons voir. Pour eux, l'objectif reste que l'on revienne le plus souvent possible. De plus, certains offrent l'option d'effectivement bloquer ou de limiter l'apparition de contenus qui ne conviennent ou ne plaisent pas. Ces mécanismes permettent de se protéger. Il parait toutefois adéquat de ne pas en abuser pour garder une distance critique face à ce que l'on reçoit. Il est nécessaire d'avoir conscience de ce mécanisme et de s'efforcer de sortir de cette bulle ! Il est important de prendre le temps de consulter

[59] On peut voir sur ce sujet le documentaire « les Nouveaux Chiens de garde » ou consulter les travaux d'Acrimed sur la question, notamment l'infographie : « Médias français : qui possède quoi ».
[60] Pariser, Eli. The filter bubble: what the Internet is hiding from you. New York, États-Unis d'Amérique, Penguin Press, 2011. Voir par ex. sa conférence Ted : ted.com/talks/eli_pariser_beware_online_filter_bubbles

des opinions contraires, de ne pas s'informer « que » par Facebook, d'essayer de multiplier ses sources d'informations, de ne pas trop facilement « bloquer » cet ami dont les opinions ne vous conviennent pas, de rester ouvert au dialogue et à la discussion posée. Bref de garder un esprit curieux… et critique !

### III.C.3. DÉVELOPPER SON ESPRIT CRITIQUE FACE À LA DÉSINFORMATION

L'éducation aux médias n'est pas évidente, elle requiert de comprendre ce qu'est une information, d'étudier de qui elle provient, d'être capable de l'analyser, etc.

C'est toutefois un enjeu fondamental pour ne pas se laisser manipuler et protéger des aspects démocratiques de notre société.

Des contenus conséquents sont disponibles dans les ressources sur ces enjeux, mais pour donner quelques lignes directrices : si je découvre un contenu choquant, étrange, « très étonnant », comment réagir ? Comment ne pas se faire avoir par des contenus mensongers ou des manipulations pour nous amener vers des discours de haine ?

Différents outils intellectuels existent pour cela, qui peuvent relever de ce qu'on appelle « l'autodéfense intellectuelle ». Il est en effet trop facile de convaincre par les mots en utilisant des méthodes de manipulation.

Un point important est de commencer par essayer remonter aux sources premières de l'information : je découvre quelque chose d'étonnant : d'où cela provient-il ? Quelles sont les références visées ? Il est simple, par exemple, pour un journaliste de « travestir » une étude scientifique aux enseignements très mesurés pour lui faire dire quelque chose de sensationnel. De la même façon, quelqu'un peut dire l'opposé d'une source qu'il cite ou même en inventer de toutes pièces.

Il faut ensuite évaluer les données et preuves qui sont développées. S'il n'y en a pas : le contenu n'est pas sérieux et ne doit pas être considéré comme un fait établi, il ne faut pas se laisser influencer par celui-ci outre mesure.

Il est préférable d'adopter une attitude de scepticisme scientifique vis-à-vis de chaque contenu. Il s'agit de douter de ce qui n'est pas strictement et correctement prouvé. Pour cela, on peut s'appuyer sur l'adage « Une affirmation extraordinaire demande des preuves plus qu'ordinaires ». Plus l'affirmation va être extraordinaire et sembler farfelue, plus il faut la questionner et évaluer ses preuves.
L'essentiel des discours dits « conspirationnistes ou complotistes » sont très extraordinaires : ils impliquent qu'un nombre conséquent de personnes agissent dans l'ombre sans pour autant se faire massivement détecter. Ils s'appuient pour cela souvent sur des faits ou phénomènes avérés (par exemple, l'existence de lobby, des mécanismes d'influence, etc.), mais qu'ils vont totalement dévoyer pour soutenir leur discours notamment grâce à des « moisissures argumentatives »[61]. Il ne faut pas tout prendre pour argent comptant, être capable de questionner les informations reçues, leur contexte de production, la véracité et la fiabilité des sources d'origine, etc.

[61] Le CorteX, « Petit recueil de 20 moisissures argumentatives pour concours de mauvaise foi », Cortecs.org, 25 oct. 2016.

Un outil important pour cela est un principe de la logique appelé : le rasoir d'Ockham. Il en existe différentes formulations, en voici une : « les hypothèses suffisantes les plus simples sont les plus vraisemblables » : si un phénomène peut être expliqué par différentes hypothèses, il est raisonnable de préférer la plus simple.

Renverser cette présomption implique de fournir de nouvelles preuves en faveur de l'hypothèse plus complexe.

Le ton et les objectifs de l'article doivent aussi être pris en compte : plus l'article est violent ou semble avoir un objectif de conversion à une pensée extrême ou à un discours de haine, plus il doit être questionné et appréhendé avec tact (et non pas relayé illico parce qu'il confirme un de nos préjugés).

Extrait de : ***Connexions*** - *Manuel pour la lutte contre le discours de haine en ligne par l'éducation aux droits de l'homme* (page 204) publication du Conseil de l'Europe (voir bibliographie)

**Conseils utiles : vérifier l'argumentation**
• Les sources des affirmations étaient-elles indiquées, ou les arguments étaient-ils simplement basés sur le « sens commun » ?
• Les sources sont-elles citées et reconnues comme faisant autorité sur le sujet ?
• Les arguments étaient-ils irréfutables ou laissaient-ils la place à d'autres conclusions ?
• Les arguments reposaient-ils sur des « faits » ou faisaient-ils appel aux émotions, à des croyances traditionnelles, voire seulement à des issues *probables* ?
• Les « faits » ou les arguments avancés pouvaient-ils être testés ?
• Les arguments contenaient-ils des généralisations sur des individus ou des groupes ?
• Y avait-il des généralisations racistes ou discriminatoires ?
• D'autres perspectives sont-elles envisageables et prouveraient-elles la fausseté de l'argument ?
• Les affirmations s'appuyaient-elles sur des arguments *ad hominem*, en d'autres termes, des arguments qui s'en prennent à la partie opposée pour ce qu'elle est, et non pour ce qu'elle dit ?
• L'argument est-il rendu plus convaincant par le *mode de présentation*, par exemple par l'utilisation d'images frappantes ou du multimédia ?

Il ne s'agit que de quelques premiers éléments, il est nécessaire d'aller plus loin pour réellement comprendre les méthodes permettant de résister efficacement aux discours de désinformation et de manipulation mentale.

# RECENSEMENT NON EXHAUSTIF DE DOCUMENTS ET SUPPORTS…

…permettant d'aller plus loin ou fournissant des contenus pédagogiques sur ces questions.

Codes de classement des sources et contenus présentés :
L = plutôt destinés aux lycéens
C = plutôt destinés aux collégiens
F = à destination des formateurs
T = sans distinction / accessible et pertinents pour les trois (souvent des contenus différents présentés)

Appréciation subjective du contenu de 1 à 3 * (* = digne d'intérêt ; ** = bien / très bien ; *** = excellent / à consulter à tout prix)

## BIBLIOGRAPHIE


- Bellon, Jean-Pierre, et Bertrand Gardette. *Harcèlement et cyberharcèlement à l'école : une souffrance scolaire 2.0*. Issy-les-Moulineaux, France, ESF éditeur, 2013.
- Boyd, Danah, et Sophie Pène. *C'est compliqué : les vies numériques des adolescents*. Traduit par Hervé Le Crosnier. Caen, France, C&F éditions, 2016. (***, F)
- Bronner, Gérald. *La démocratie des crédules*. Paris, France, PUF, 2013. (**, F)
- Cabourg, Céline et Boris Manenti. *Portables : la face cachée des ados – Leurs vie secrètes : réseaux sociaux, applis*…. France, Flammarion, 2017.
- Conseil de l'Europe. *Connexions : manuel pour la lutte contre le discours de haine en ligne par l'éducation aux droits de l'homme*. Rédigé par Ellie Keen, Mara Georgescu, et Rui Gomes. Strasbourg, France, Conseil de l'Europe, 2014. (***,T)
- Cordier, Anne. *Grandir connectés : les adolescents et la recherche d'information*. Caen, France, C&F éditions, 2015.
- Greenhow, Christine, Julia Sonnevend, et Colin Agur, éd. *Education and social media: toward a digital future*. Cambridge (Mass.), États-Unis d'Amérique, The MIT Press, 2016. (**, F)
- Manach, Jean-Marc. *La vie privée, un problème de vieux cons ?* Limoges, France, FYP, 2010. (***, F)
- Pariser, Eli. *The filter bubble: what the Internet is hiding from you*. New York, Etats-Unis d'Amérique, Penguin Press, 2011. (*, F)


## SITOGRAPHIE

### Sitographie générale

- Le site de la CNIL, ainsi que spécifiquement la plateforme du collectif « EducNum » : pour citer quelques outils intéressants : les ateliers « les bonnes utilisations des réseaux sociaux », une webographie très complète… (***, T)

- Le site du commissariat à la protection de la vie privée du Canada dispose aussi d'un grand nombre de conseils pertinents aux individus sur ces sujets. (**, F+L)
- Le site d'Internet Sans Crainte et notamment le dossier « Réseaux sociaux », nombreux articles et informations sur les liens entre jeunesse et réseaux sociaux, des jeux (notamment 2025 ExMachina), une exposition, des conseils pour les jeunes... (***, T)
- Le dossier « les jeunes et les réseaux sociaux » de la Fondation « Child Focus » et les contenus de préventions en général : dont un guide à l'attention des parents, un dossier pédagogique « réfléchis avant de publier », un jeu vidéo assez bien réalisé qui a de réels intérêts pour sensibiliser, mais où on incarne le parfait « cyberstalker », etc. (***, T)
- Sur le site « enseignement.be » de la fédération Wallonie-Bruxelles, différents contenus autour des « TICE en classe » et notamment pour « éduquer aux réseaux sociaux » et « éduquer avec les réseaux sociaux » (ex. : Twitter). (**, T)
- Le site « e-enfance.org » et notamment les pages « dangers des réseaux sociaux » : Une présentation rapide de quelques réseaux sociaux, des conseils à destination des parents et des enfants et un renvoi vers quelques ressources multimédias tierces relatives au cyberharcèlement et aux risques de transmission d'informations (dont une infographie intéressante de trendmicro). (*, F+L)
- La page ressource du site du CECyF prévention du Centre expert contre la cybercriminalité français, contient des contenus dépassant la question des réseaux sociaux, mais certains restent pertinents dans le thème. (**, T)
- Les francas, l'éducation en mouvement, Rapport Médias 2011, « Les réseaux sociaux, une question d'éducation ? ». (*, F)
- "Bien vivre le digital (sic)" dossier "réseaux sociaux" sur le site d'Orange, de nombreuses informations factuelles et infographies à destination des parents avec différents guides pratiques (en PDF ou vidéos). (**, F)
- La société proposant le logiciel de contrôle parental « Witigo » offre de nombreuses informations et des réponses aux problèmes liés aux réseaux sociaux, notamment 2 infographies et des conseils. (**, T)
- La « Radio Télévision Suisse » a fait réaliser une opération spéciale « enquête ouverte : donnez-moi mes données » qui contient un grand nombre de contenus de qualité sur la protection de la vie privée, notamment un jeu sérieux : Datak. (***, T)
- Quelques autres sites regroupant des contenus pertinents en anglais : Chatdanger.com, BetterInternetForKids.eu, Webwewant.eu (qui comporte aussi deux guides à destination des éducateurs et des jeunes traduits en français)

## Sondages et données chiffrées

- Sondage IFOP : observatoire des réseaux sociaux automne 2010.
- MinorMonitor : "Surveys 1,000 Parents of Children on Facebook, Shares Results on Realities, Parental Concerns", résumé dans une infographie.
- « Les jeunes et les réseaux sociaux » Étude réalisée sur des jeunes de 18 à 25 ans de la région Rhône-Alpes en 2015.
- Facebook et les enfants une infographie de France Inter.

## Sitographie sur les questions de désinformations

- Le site gouvernemental « on te manipule » (**, T)
- Le site Hoaxbuster, le site clef pour vérifier des informations sur les canulars. (***, T)
- Une expérience d'apprentissage en Haute-Savoie par l'institutrice Rose-Marie Farinella à la compréhension d'Internet et à la détection des intox décrite dans un article de rue89, et sa vidéo introductive. (**, F)
- Cette expérience est réalisée en collaboration avec la chaine YouTube « Hygiène Mentale » qui met à disposition de nombreuses vidéos apportant des bases de logique, de zététique et donc pour développer son esprit critique. Les vidéos sont d'excellents supports pédagogiques à tout âge. (***, T)
- On peut aussi citer les travaux du Cortecs, pour se former sur ces questions (notamment les « 20 argumentaires moisis ». (**, F)
- Conspiracy Watch, un site questionnant et analysant les théories conspirationnistes. (*, L)

## AUTRES SOURCES DIVERSES

- Une présentation du dispositif des « promeneurs du Net pour repérer les jeunes en souffrance », La Gazette Santé Social, 18 nov. 2016. (*, F)
- Un autoquestionnaire pour évaluer son « addiction » à Internet par le centre d'addictoviligance d'Auvergne. (***, T)
- Le « portrait Google de Marc L. », du journal Le Tigre, 7 janv. 2009, qui retrace une vie entière à partir de traces laissées sur les réseaux sociaux. (***, T)
- Document « non au harcèlement » du ministère de l'Éducation nationale pour la journée mondiale, 3 nov. 2016, les principaux contenus sur le cyberharcèlement / cyberviolence y sont répertoriés. (**, T)
- « Et si on laissait tomber Facebook ? » une traduction de l'équipe de Framalang d'un article de Salim Virani qui réunit et expose les atteintes du service au libertés. (***, L+F)
- J. Anderson, « A lawyer rewrote Instagram's privacy policy so kids and parents can have a meaningful talk about privacy ». Quartz, 6 janvier 2017, un article qui évoque de nombreuses questions autour de la question des conditions générales d'utilisation et de l'accès aux réseaux sociaux par la jeunesse et notamment une « réécriture » des conditions générales d'utilisation d'Instagram. Une traduction en a été effectuée par Marie Turcan sur le Busness Insider France. (**, F)

## CONTENUS VIDÉOS

- M. Carotte – Lucie et le Périscope, chaîne « les Parasites » sur YouTube, un court métrage reprenant les codes du film « c'est arrivé près de chez vous » mis à jour à la sauce « Periscope » : attention la vidéo comporte une scène de viol et ne doit pas être diffusée à tout public. Elle peut toutefois servir pour sensibiliser un public « averti ». (**, L)
- Chaine YouTube de « Sulivan Gwed » / « Un panda moqueur » : un adolescent (16 ans en 2016) qui a réalisé de nombreuses vidéos qui affichent

des compteurs de vues très conséquents, beaucoup parlent de son rapport avec les réseaux sociaux (ex. 10 choses à ne pas faire sur les réseaux sociaux). Cela peut donner une idée (principalement pour les plus anciennes), de certaines pratiques. (*, F)

- Il existe sur YouTube de nombreuses vidéos produites par des associations, établissements scolaires / des élèves qui touchent à ces problématiques, par exemple :
    - "Les dessous de la toile - Les réseaux sociaux, sans danger ?", Lycée Les Sept Mares – Maurepas
    - "Les dangers des réseaux sociaux", Association Résilience

  Ces vidéos renvoient vers d'autres similaires sur les mêmes sujets. (variable)

- Privés de vie privées ? #Datagueule40 sur YouTube, une visualisation des enjeux de la vie privée et des méthodes de surveillance, plus large que les réseaux sociaux, mais pertinente et suffisamment bien faite pour fonctionner avec des lycéens. (***, L+F)
- Vidéos « interactives » de la CNIL « Share the Party » sur YouTube une suite de vidéos mettant en scène un jeune photographiant une soirée avec des choix de partager ou non les photos et un « résultat » selon les choix effectués. (*, L).
- Parents parlons-en ! Episode 5 : Cyber-harcèlement. (*, L+F)
- « Paye ton like », saison 1 épisode 3 de la Websérie documentaire « Do Not Track » d'Arte. Contenu documentaire sous-titré assez rythmé proposant à l'auditeur de connecter son Facebook pour voir ce qui peut en être déduit. (**, F+L)
- « Pourquoi on est addict à Facebook, YouTube, etc.? 5 étapes de la Web-addiction + Comment décrocher » chaîne « Autodidacte » sur YouTube qui présente un livre consacré à l'addiction au numérique et des pistes pour s'en séparer. (**, F+L)
- HightonBros, « What's on your mind » disponible sur YouTube, un court métrage sur les représentations publiques sur Facebook. (*, L)
- « Nosedive », saison 3 épisode 1 de la série Black Mirror, mettant en valeur les dangers des représentations publiques sur les réseaux sociaux et de l'évaluation, l'épisode 6 de la saison 3 interroge aussi la question du discours de haine sur les réseaux sociaux. (***, F+L)
- « vous avez 0 amis », saison 14 épisode 4 de la série SouthPark qui parodie certains mécanismes délétères de Facebook, malgré l'emballage classique des épisodes de South Park, l'épisode reste diffusable devant des lycéens. (*, L)

LdH — Ligue des droits de l'Homme
138 rue Marcadet – 75018 Paris
Tél. 01 56 55 51 00 – Fax 01 42 55 51 21
ldh@ldh-france.org – www.ldh-france.org

Avec le soutien de

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE
DE LA VILLE,
DE LA JEUNESSE
ET DES SPORTS