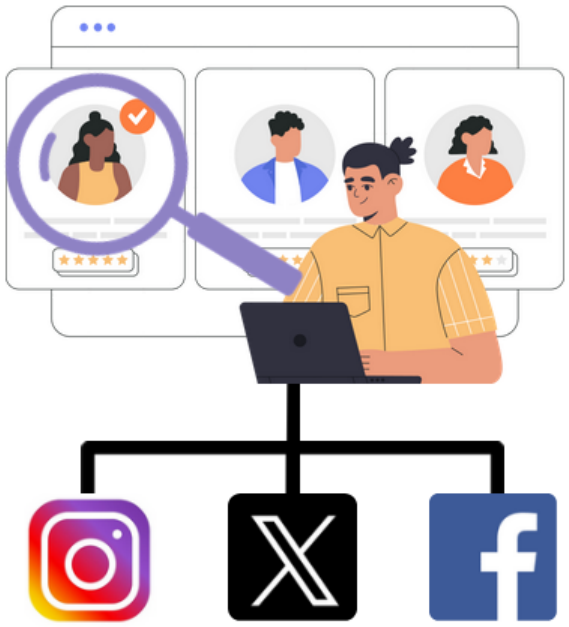
Du bon usage des réseaux sociaux

Le succès planétaire des réseaux sociaux – Facebook en premier lieu – a fait rentrer la société, toutes classes confondues, dans une nouvelle ère, celle de l'exhibitionnisme numérique. Véritables phénomènes, ces réseaux sociaux provoquent des réactions extrêmes. Soit on aime, soit on n'aime pas. Pourtant à y regarder de plus près, les réseaux sociaux offrent souvent autant d'avantages qu'ils présentent d'inconvénients.

Ainsi, l'atout principal de ces plateformes interactives est sans conteste le réseautage à la fois social (puisqu'ils permettent à leurs membres de rester en contact avec leurs amis et leur famille) que professionnel (puisque certains d'entre eux permettent de nouer des contacts utiles et de trouver du travail).



Ces sites permettent également d'envoyer et de recevoir des messages, de télécharger des photos et des vidéos, d'acquérir une notoriété publique en créant un blog ou une chaine Youtube pour faire le « *buzz* » et obtenir un certain nombre de « *vue* » et de « *like* ».

Par ailleurs, ils sont aussi un outil de promotion très efficace pour une entreprise, des services, des produits ou encore des sites. Instagram est ainsi devenu une plateforme incontournable pour les marques.

[Pour plus d'information, voir la fiche pratique **Présentation des principaux réseaux sociaux**]

En revanche, parmi les risques principaux, on peut citer :

- le piratage de compte qui peut aller jusqu'à l'usurpation d'identité ;
- les cambriolages lorsqu'une personne a indiqué non seulement son adresse mais également ses dates de vacances ;

- le voyeurisme lorsque des informations purement privées, telles des photos ou des vidéos sont publiées et peuvent être réutilisées à des fins non souhaitées à l'origine par exemple sur des sites de pédopornographie ;
- le harcèlement en ligne comme cela peut arriver par exemple dans les écoles où des adolescents menacent leurs camarades de révéler des photos coquines ou profèrent des insultes voire même peuvent inciter au suicide de la personne harcelée ;
- le partage indu d'informations sensibles à de parfaits inconnus ;
- l'utilisation non souhaitée des données collectées à des fins publicitaires ;
- les risques de dépendance, notamment chez les plus jeunes qui ne peuvent aller se coucher sans passer par la case Tik Tok.

[Pour plus d'information, voir la fiche mémo **RESEAUX SOCIAUX Principaux risques et conseils pour les éviter**]

Or, s'il n'y a souvent pas de position intermédiaire entre les adeptes du grand déballage public et ceux qui ont choisi de faire leur l'adage « *pour vivre heureux, vivons cachés* », la solution serait peut-être tout simplement d'apprendre à apprivoiser ces réseaux sociaux qui font désormais partie de notre quotidien, ce qui passe notamment par l'adoption de bons comportements.

Des acteurs qui connaissent tout de vous

Souvenez-vous ! En 2007, **Max Schrems,** un étudiant en droit avait été à l'origine du plus grand recours collectif intenté en Europe contre Facebook. La croisade du jeune autrichien contre l'exploitation des données personnelles sur internet était née après qu'il ait demandé à Facebook de lui envoyer une compilation de ses informations collectées sur le réseau social. Il avait alors été choqué de recevoir un fichier de 1.222 pages répertoriant minutieusement toutes ses informations présentes sur le site, même celles qu'il croyait avoir supprimées.

« *Si c'est gratuit, c'est que vous êtes le produit* »

Les réseaux sociaux collectent en effet une grande quantité de données sur leurs utilisateurs**, souvent à leur insu ou sans leur consentement éclairé**.

Cette collecte s'effectue **soit directement** auprès de la personne, par exemple lors de la création du compte utilisateur, soit de **manière indirecte**, par le biais des différentes fonctionnalités proposées, comme par exemple la possibilité de « *liker* » (aimer) une publication.

Les données ainsi collectées sont nombreuses et vont des plus évidentes comme les données d'identification (nom, photo de profil, coordonnées, etc.) ou la liste de ses amis aux données de navigation (contenus postés, sites visités, liens cliqués, etc.) ou encore aux données de géolocalisation et d'interactions avec d'autres utilisateurs.

Or, souvent ces données vont ensuite être utilisées à des **fins de marketing, de profilage** ou **de publicité ciblée.**

Des risques importants pour la vie privée des utilisateurs

Outre une intrusion certaine dans la **sphère privée** des utilisateurs par le biais des publicités personnalisées et une absence, souvent, de consentement préalable à la collecte des données personnelles, le **risque de surveillance** de ces mêmes utilisateurs par les réseaux sociaux est également à prendre très au sérieux.

En analysant le comportement des utilisateurs, leurs activités et leurs interactions sociales, les réseaux sociaux peuvent en effet créer des profils **extrêmement détaillés** et connaître les préférences desdits utilisateurs.

Ce risque est d'autant plus important qu'il entraine dans la plupart des cas des transferts de données vers des **pays ne présentant pas un niveau de protection adéquat**.

La majorité des réseaux sociaux appartiennent à des entreprises américaines telles que la société Meta qui possède Facebook, Messager Instagram, Threads, ainsi que WhatsApp, ou même dans certains cas, chinoises (TikTok par exemple).

Ils stockent donc les données collectées selon la réglementation en vigueur dans leur pays ; règlementation qui est **beaucoup moins protectrice** pour les utilisateurs, que les lois en vigueur en Europe.

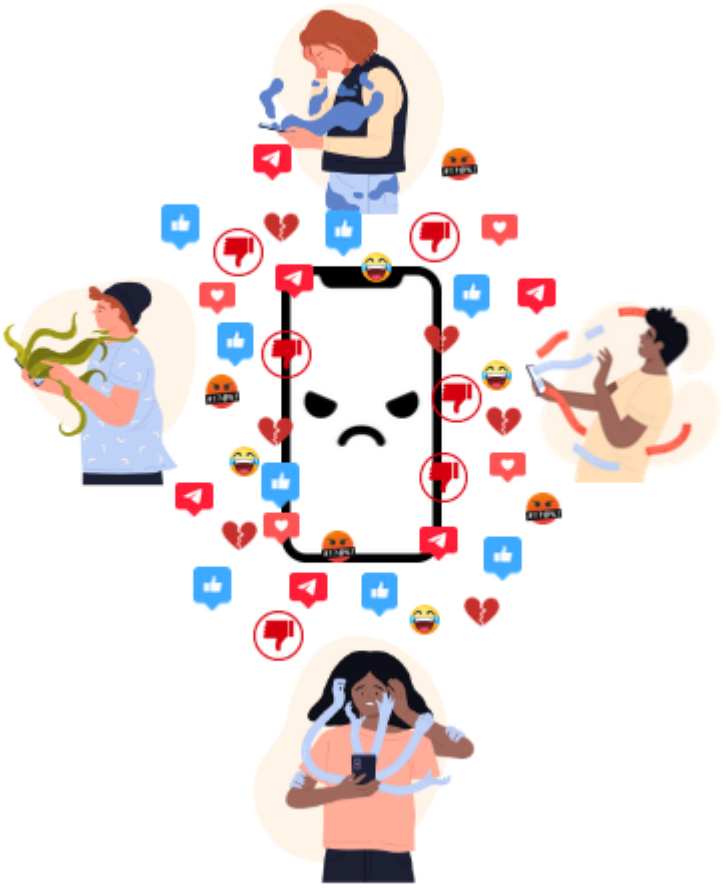
Les bons comportements à adopter sur les réseaux sociaux

Le principe des réseaux sociaux étant en premier lieu d'échanger avec le reste du monde, **l'anonymat est donc chose quasi impossible.**

En revanche, en utilisant de bons comportements, il est tout à fait envisageable de protéger ses données personnelles et limiter les risques de dévoiler, plus que nécessaire, des pans de sa vie privée.

Bien que chaque réseau soit différent, ils sont tous susceptibles de collecter 4 types de données :

- les informations de profil (nom, âge, profession, études, etc.) ;
- les traces de l'activité de l'utilisateur (« *likes* », partages, commentaires, adhésion à des groupes, etc.) ;
- son activité silencieuse (chacun de ses mouvements est enregistré même en mode silencieux) ;
- la géolocalisation de son appareil (utilisée entre autres pour générer des publicités ciblées).



Pour éviter que ces données ne soient partagées sans restriction, les réseaux sociaux ont mis en place leur propre politique de sécurité avec des réglages des **paramètres de confidentialité**. Apprendre à connaître et à configurer ces paramètres est donc le premier bon comportement à adopter afin d'éviter toute mauvaise surprise.

Chaque réseau s'efforce de les améliorer. Ils changent donc sans arrêt, d'où l'importance de vérifier de façon régulière s'ils correspondent toujours à ce que vous souhaitez.

Par ailleurs, une **utilisation raisonnée** des réseaux sociaux est bien entendu recommandée.

Il est également très important de séparer sur n'importe quel réseau vies personnelle et professionnelle.

Enfin n'oubliez pas que **rien de ce qui a été publié n'est jamais totalement effacé.**

A NE PAS FAIRE	A FAIRE
Ne jamais divulguer son nom d'utilisateur ou mot de passe	Avoir des profils séparés « *personnels* » et « *professionnels* »
Ne pas publier sa date de naissance complète qui peut être utilisée par les publicitaires	Choisir un mot de passe sûr et unique, renouvelé régulièrement
Ne pas indiquer ses dates de vacances (responsables de certains cambriolages)	Avoir un mot de passe différent des autres comptes (messagerie, banque...)
Ne pas indiquer en permanence où l'on se trouve	Adapter les paramètres de confidentialité à ses besoins, et ne pas laisser les conditions par défaut
Ne pas accepter n'importe qui comme ami	S'assurer que le correspondant est bien un ami et pas une personne se faisant passer pour lui (vérifier le compte, messagerie...)
Ne pas laisser parler ses amis sur soi sur tout et n'importe quoi	Supprimer régulièrement les amis inopportuns
Ne pas dire tout ni communiquer ses opinions politiques, sa religion ou son numéro de téléphone	Se poser les bonnes questions avant de publier du contenu potentiellement dangereux
Ne pas aimer ou relayer des contenus sans penser que cela révèle ses opinions	Se poser la question :« *est-ce que j'approuverais publiquement ce contenu dans un écrit ou dans une conversation en face en face hors du réseau social et sous ma véritable identité* » ?
Ne pas publier du contenu que l'on n'aurait pas rendu public dans la vie courante sous sa véritable identité	Vérifier la réalité des informations publiées, rester vigilant, signaler aux autorités les contenus problématiques (contraires à la loi notamment) et ne pas les relayer
Ne pas penser qu'il suffit d'effacer un contenu pour qu'il disparaisse à jamais et qu'il n'y aura pas de trace	
Ne pas commenter à tort et à travers, car ce qui est écrit sur le net reste même des années après	

Ne pas diffuser des photos embarrassantes de soi et/ou de ses amis, sa famille car une fois publiées, elles deviennent incontrôlables	Taper régulièrement son nom dans un moteur de recherche pour vérifier quelles informations circulent sur soi
Ne pas penser que les influenceurs savent tout sur tout et font autorité y compris en dehors de leur domaine de compétence initial	Utiliser un logiciel antivirus
Ne pas s'abonner à des applications tierces associées à Facebook (bouton « *j'aime* » par exemple)	Installer la version la plus récente de son navigateur (comme Internet Explorer, Firefox...)
Ne pas lire les conditions d'acceptation avec les nouvelles versions	Supprimer les cookies après déconnexion du réseau (via l'option "*Effacer les données de navigation*"), pour ne pas être pisté, même déconnecté
Ne pas laisser les enfants seuls sur les réseaux sociaux	Préférer une connexion sécurisée (avec le préfixe "*https*")
Ne pas cliquer sur tous les liens partagés, car ils peuvent être infectés	Activer les notifications de connexion qui informent de toutes les connexions à son compte
Ne pas se connecter depuis les bornes Wifi publiques	