# CHARTE DE BON USAGE DES RÉSEAUX SOCIAUX

Le succès planétaire des réseaux sociaux – Facebook en premier lieu – a fait rentrer nos sociétés, 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 déteste ! Pourtant à y regarder de plus près, les réseaux sociaux peuvent avoir autant d'avantages qu'ils ne présentent d'inconvénients.

Ainsi, l'atout principal de ces plateformes interactives est sans conteste le réseautage à la fois social (puisqu'elles permettent à leurs membres de rester en contact avec leurs amis et leur famille) et professionnel (puisque certaines d'entre elles 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.

En revanche, parmi les risques principaux, il y a :

- 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 ;
- le harcèlement en ligne comme cela peut arriver par exemple dans les écoles où des adolescents menacent leurs camarades de révéler des photos intimes ;
- 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 réseaux sociaux.

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. Cela passe notamment par :

- la connaissance des principaux réseaux et de leurs fonctionnalités ;
- l'adoption de bons comportements ;
- le paramétrage de la sécurité et de la portée des publications.

## DESCRIPTION DES PRINCIPAUX RESEAUX SOCIAUX

### Facebook

Créé en 2004, Facebook est sans conteste le réseau social le plus connu. Il permet à ses utilisateurs de publier du contenu (images, photos, vidéos, fichiers…), d'échanger des messages et d'interagir sur les messages des autres utilisateurs.

C'est également une base de données marketing extraordinaire pour les entreprises car toutes les classes d'âge et catégories de population y sont réunies. De ce fait, le réseau propose aux entreprises de faire des campagnes publicitaires (Facebook Ads) avec des ciblages très précis en fonction des centres d'intérêt des utilisateurs, de leur comportement ou encore de leurs caractéristiques socio-démographiques et géographiques. De plus, Facebook offre la possibilité d'analyser toutes les retombées des publicités publiées grâce à des outils statistiques très détaillés.

**Twitter**

Créée en 2006, cette plateforme de microblogging permet aux utilisateurs d'envoyer et de lire de courts messages, appelés « tweets ». Ces messages de 140 caractères maximum permettent d'être une source d'information en temps réel, ce qui correspond aux attentes des nouvelles générations. Ce réseau est notamment très utilisé par les influenceurs (dirigeants, journalistes, blogueurs, politiques...) pour transmettre de l'information rapidement. Twitter permet également de diffuser des publicités à une cible très précise en fonction des centres d'intérêt des utilisateurs et de critères socio-démographiques ou géographiques et d'en analyser les résultats.

**Instagram**

Créé en 2010, Instagram est un réseau social très simple d'utilisation qui permet de partager des photos et de courtes vidéos disponibles sur plateformes mobiles. Depuis 2016, les utilisateurs peuvent également réaliser et diffuser des « stories » qui disparaissent au bout de 24 h. Il y est très rare de mettre beaucoup de textes, quelques mots et des hashtags suffisent.

**Youtube**

Créée en 2005 et appartenant désormais à Google, YouTube est la première plateforme d'hébergement et de partage de vidéos à grande échelle. Il permet aux utilisateurs d'envoyer, de regarder, d'évaluer, de commenter et de partager sur d'autres réseaux sociaux les vidéos.

**Snapchat**

Créé en 2011, cette application est très prisée par les jeunes de 25 ans. Elle permet d'envoyer des photos et vidéos qui n'apparaissent que pendant quelques secondes. L'application permet également de créer et de diffuser des stories (suite de photos et/ou vidéos) visibles à volonté mais uniquement pendant 24 h.

**LinkedIn**

Créé en 2003, LinkedIn est un réseau social professionnel qui a pour mission de « connecter les professionnels du monde entier afin de rendre leur activité plus productive et plus prospère ». Les membres du réseau partagent ainsi leur identité personnelle, communiquent avec leur réseau, échangent des informations et des points de vue professionnels, publient des articles et trouvent des opportunités commerciales et professionnelles.

Le contenu de certains de ces services peut toutefois être également visible par les simples visiteurs.

**Pinterest**

Créé en 2010, Pinterest est un réseau social ayant pour but le partage de photos de qualité dont l'audience est presque uniquement féminine. Une fois qu'un membre a téléchargé et partagé les images qu'il trouve intéressantes, ces images sont transformées en « PIN » et peuvent être placées, dans n'importe quel ordre,

et ce, selon différentes thématiques, laissant libre cours à l'esprit créatif des utilisateurs.

Les sujets les plus populaires sur ce réseau sont la mode, la bijouterie, l'artisanat, les voyages, l'alimentation et les loisirs créatifs.

## LES BONS COMPORTEMENTS A ADOPTER SUR LES RESEAUX 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 possible 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 quatre (04) types de données :

- les informations de profil (nom, âge, profession, études, etc.) ;
- les traces de votre activité (likes, partages, commentaires, adhésion à des groupes, etc.) ;
- votre activité silencieuse (chacun de vos mouvements est enregistré même si vous êtes silencieux) ;
- la géolocalisation de votre 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.

A titre d'exemple, il est possible sur Facebook, de configurer chaque élément séparément. Vous pouvez ainsi créer des groupes d'amis pour déterminer qui pourra voir quoi ou bien encore autoriser ou non que votre profil apparaisse sur les moteurs de recherche tels que Google.

Sur Twitter, tous les messages sont publics par défaut et impossibles à effacer. Il convient donc de faire très attention avant de tweeter. Par ailleurs, pour éviter de recevoir trop de mails de la part du réseau social, il faut configurer les notifications dans les paramètres de son compte.

Il est par ailleurs très important de **séparer sur n'importe quel réseau vie personnelle et vie professionnelle**. Avec Twitter, vous pouvez ainsi vous créer deux profils et choisir les personnes que vous voulez suivre en fonction de vos intérêts.

De même, si vous utilisez Facebook et le réseau professionnel en ligne LinkedIn, il convient de garder le premier pour vos relations personnelles et d'opter pour le second pour vos relations de travail.

Mais avant de voir de façon plus détaillée les règles de paramétrage pour les réseaux sociaux les plus importants, le tableau suivant récapitule les comportements de base à adopter quelle que soit la plateforme utilisée.

| A NE PAS FAIRE | A FAIRE |
|---|---|
| • **Ne jamais divulguer son nom d'utilisateur ou mot de passe ;**<br>• **Ne pas publier sa date de naissance complète qui peut être utilisée par les publicitaires ;**<br>• **Ne pas indiquer ses dates de vacances (responsables de certains cambriolages) ;**<br>• **Ne pas indiquer en permanence où l'on se trouve ;**<br>• **Ne pas accepter n'importe qui comme ami ;**<br>• **Ne pas dire tout ni communiquer ses opinions politiques, sa religion ou son numéro de téléphone ;** | • **Avoir des profils séparés « *personnels* » et « *professionnels* » ;**<br>• **Choisir un mot de passe sûr et unique, renouvelé régulièrement ;**<br>• **Avoir un mot de passe différent des autres comptes (messagerie, banque...) ;**<br>• **Adapter les paramètres de confidentialité à vos besoins, et ne pas laisser les conditions par défaut ;**<br>• **S'assurer que le correspondant est bien un ami et pas une personne se faisant passer pour lui (vérifier le compte, messagerie...) ;**<br>• **Supprimer régulièrement les amis inopportuns ;** |

| | |
|---|---|
| • **Ne pas commenter à tort et à travers, car ce qui est écrit sur le net reste même des années après ;**<br>• **Ne pas laisser parler ses amis sur vous sur tout et n'importe quoi ;**<br>• **Ne pas diffuser des photos embarrassantes de vous et/ou de vos amis, votre famille car une fois publiées, elles deviennent incontrôlables ;**<br>• **Ne pas s'abonner à des applications tierces associées à Facebook (bouton j'aime par exemple) ;**<br>• **Ne pas lire les conditions d'acceptation avec les nouvelles versions ;**<br>• **Ne pas laisser les enfants seuls sur les réseaux sociaux ;**<br>• **Ne pas cliquer sur tous les liens partagés, car ils peuvent être infectés ;**<br>• **Ne pas se connecter depuis les bornes Wifi publiques.** | • **Se poser les bonnes questions avant de publier du contenu potentiellement dangereux ;**<br>• **Utiliser un logiciel antivirus ;**<br>• **Installer la version la plus récente de son navigateur (comme Internet Explorer, Firefox...) ;**<br>• **Supprimer les cookies après déconnexion du réseau (via l'option "*Effacer les données de navigation*"), pour ne pas être pisté, même déconnecté ;**<br>• **Préférer une connexion sécurisée (avec le préfixe "*https*") ;**<br>• **Activer les notifications de connexion qui informent de toutes les connexions à votre compte ;**<br>• **Taper régulièrement votre nom dans un moteur de recherche pour vérifier quelles informations circulent sur vous.** |

## LE PARAMETRAGE DE LA SECURITE ET DE LA PORTEE DES PUBLICATIONS

Les profils sociaux étant une extension de l'identité réelle de chaque utilisateur, il est donc important d'en prendre soin en maîtrisant les paramètres, filtres et autres options de sécurité mis à disposition.

De manière générale, trois (03) règles de base sont à respecter :

- une activité raisonnée ;

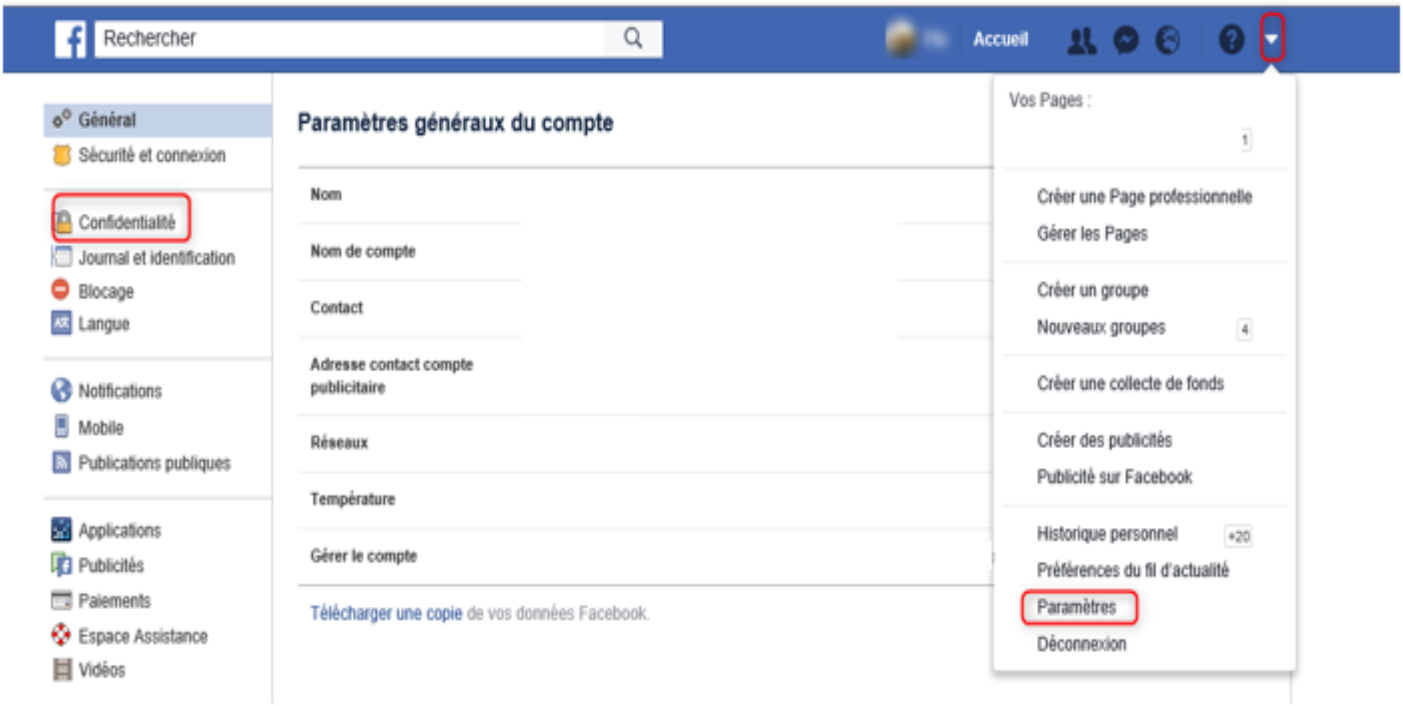
- une authentification forte (mot de passe unique et fort, composé de caractères minuscules, de caractères majuscules, de chiffres et de caractères spéciaux) ;
- des paramètres de sécurité et de confidentialité adoptés à vos besoins.

Les deux premières étant du seul ressort de chaque individu, nous allons passer en revue les paramètres de sécurité et de confidentialité de quelques-uns des principaux réseaux sociaux.

## ➢ Les paramètres de sécurité Facebook

Réseau le plus populaire avec près de 1,7 milliard de membres, Facebook est également le réseau le plus attaqué et le plus critiqué. Pourtant, il est possible de limiter la diffusion de ses données personnelles depuis que le réseau a été forcé d'adapter sa politique de confidentialité suite à diverses actions menées contre lui.

Aujourd'hui, Facebook fournit des explications claires et précises dans une section intitulée « **Sécurité du compte** ». Par ailleurs, les paramètres de confidentialité peuvent être consultés et modifiés très facilement en cliquant sur la flèche pointant vers le bas située dans le coin supérieur droit de n'importe quelle page Facebook. Il suffit ensuite de sélectionner « **Paramètres** » dans le menu déroulant, puis de sélectionner « **Confidentialité** » dans le menu de gauche de la page qui s'est ouverte.




Parmi les paramètres à configurer, vous pourrez notamment choisir de :

- ✓ **Recevoir des notifications en cas de connexion depuis un autre appareil :** Pour configurer cette option, il faut se rendre dans « **Paramètres** », puis dans « **Sécurité** », et enfin dans « **Renforcement de la sécurité** » pour choisir de recevoir des notifications. Pour augmenter d'un cran cette protection, il est possible de demander au réseau social d'envoyer un code de sécurité à votre portable à chaque nouvelle connexion depuis un navigateur inconnu.
  Sur cette même page, un historique de vos connexions est disponible. Il indique les heures auxquelles votre compte est connecté, géolocalise la position de l'utilisateur et identifie l'appareil utilisé. Il est possible d'établir une liste des navigateurs d'où vous souhaitez pouvoir vous connecter, et d'en exclure certains. Vous pouvez aussi choisir des contacts de confiance dans votre liste d'amis qui pourront vous aider en cas de difficultés à accéder à votre compte ;

- ✓ **Paramétrer la confidentialité :** Par défaut, un statut Facebook est public et les photos que vous publiez sont visibles de tous. C'est donc à vous de paramétrer votre compte pour que seuls vos amis puissent voir vos photos et ce que vous publiez sur votre mur. Pour ce faire, il faut aller dans « **Paramètres** », puis dans « **Confidentialité** »et

déterminer qui a accès à vos publications, futures comme antérieures. Facebook offre la possibilité de créer des listes d'amis afin de différencier vos « **amis proches** » - avec qui vous souhaitez partager la totalité de vos contenus vidéos, photos et partages - des « **connaissances plus éloignées** ». Il suffit pour cela de créer des listes classifiant vos « **amis** » Facebook, et de paramétrer les contenus vous concernant selon l'accès que vous leur laisserez. En cas de cyberharcèlement ou d'invitations trop répétitives à jouer à une application, vous pouvez également bloquer totalement la personne importune ou l'application visée ;

- ✓ **Sécuriser les accès à vos publications :** Le réseau social propose de multiples options de sécurité qui ne sont pas activées par défaut et qui permettent par exemple de « **contrôler l'accès aux photos Facebook** » que vous postez ou aux photos taguées postées par un tiers. Pour ne pas voir les photos prises de son smartphone automatiquement publiées sur Facebook, l'option « **Synchronisation** » des photos doit être désactivée depuis le menu « Paramètres » de l'application. Autre fonctionnalité intéressante, Facebook autorisant l'usage des **pseudonymes** lors de la création d'un compte, vous pouvez ne pas mentionner votre véritable nom pour garantir votre anonymat.

**Facebook connait 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 pensait avoir supprimé.

Ce que Facebook sait de nous est en effet vertigineux et tout un chacun peut également s'en rendre en compte très facilement. Pour récupérer votre propre dossier et savoir quelles sont les informations concrètes que Facebook possède, il suffit d'aller sur le site de Facebook, de sélectionner **Paramètres** puis de cliquer sur **Télécharger une copie de vos données Facebook**.

Il vous faudra alors juste confirmer le mot de passe de votre compte.

Vous recevrez ensuite, dans un laps de temps variable, un e-mail avec un lien cliquable vers le téléchargement de l'archive. Après avoir cliqué sur le lien,

l’ensemble de vos données sera téléchargé sur le disque dur de votre ordinateur.

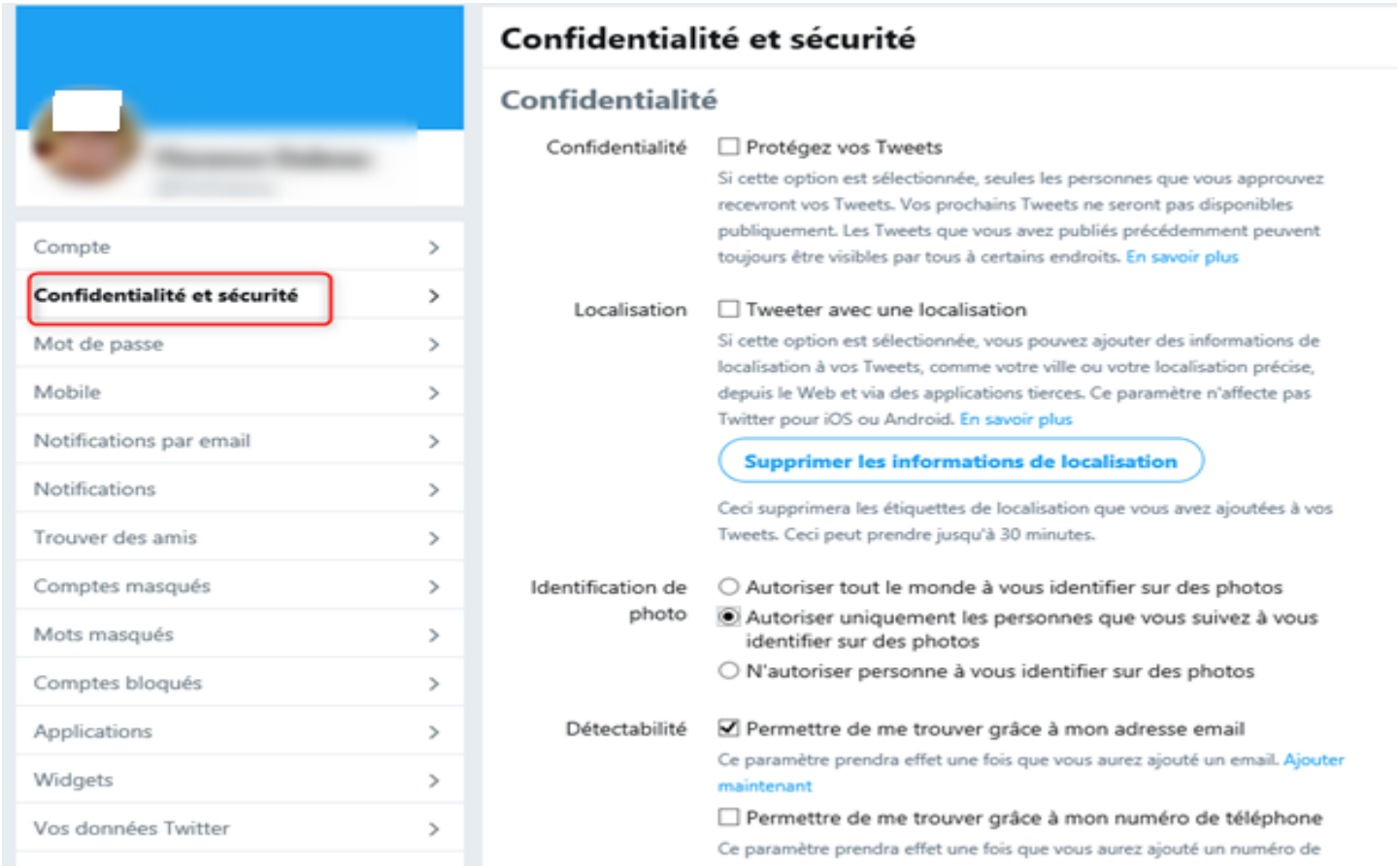
## ➢ Les paramètres de sécurité Twitter

« **Ce que vous dîtes sur les Services Twitter est visible partout dans le monde instantanément. Vous êtes ce que vous tweetez !** »

Public par défaut, ce réseau social peut inclure des photos, des vidéos et des liens vers d’autres sites (qui sont, eux aussi, publics par défaut).

La politique de confidentialité de Twitter est toutefois plutôt transparente et protectrice de votre identité visuelle. En effet, la plupart des options ne sont pas cachées, elles sont rassemblées au même endroit et leur paramétrage par défaut est souvent optimal au niveau de la sécurité. Il n'y a donc pas énormément de manipulations à faire.

Pour commencer, il convient d’aller sur votre compte, de cliquer sur l'icône de votre image personnelle en haut et de choisir ensuite « **Paramètres et confidentialité** ».




Parmi toutes les options proposées, vous pourrez :

- vérifier les demandes de connexion (cette fonctionnalité est désactivée par défaut) ;
- réinitialiser votre mot de passe (cette fonctionnalité est désactivée par défaut) ;
- vous connecter avec code (utile en cas d'oubli de votre mot de passe) ;
- toujours demander un mot de passe pour vous connecter à votre compte ;
- réduire aux seules personnes que vous connaissez la possibilité de vous identifier sur une photo ;
- protéger vos tweets en passant en mode protégé, ce qui vous permettra de réserver vos tweets à vos seuls abonnés. Ceux-ci disparaitront également

de la recherche Google, donc vous n'aurez plus à craindre qu'on vous retrouve par ce biais ;

- désactiver la fonction détectabilité qui permet à d'autres utilisateurs de trouver en entrant votre numéro de téléphone ou votre adresse mail.

## ➢ Les paramètres de sécurité Linkedin

Le réseau social professionnel a mis à jour ses conditions générales le 8 mai dernier afin, notamment, de permettre un meilleur contrôle des données partagées avec les annonceurs et d'encadrer les usages pour éviter le harcèlement.

Comme le précise le réseau social, le contenu partagé par ses utilisateurs peut se retrouver en dehors de ses services puisque par exemple, des aperçus ou extraits de contenu peuvent être retrouvés dans des moteurs de recherche d'autres prestataires. Un contrôle est toutefois possible pour gérer la manière dont ces contenus sont partagés. « *Conformément aux paramètres disponibles, nous respecterons vos préférences concernant la visibilité du contenu et des informations (par exemple, le contenu des messages que vous envoyez, le partage de contenu uniquement avec des relations Linkedin, la limitation de la visibilité de votre profil pour les moteurs de recherche ou le fait de ne pas notifier votre réseau lors de la mise à jour de votre profil Linkedin). Par défaut, aucune notification n'est envoyée à vos relations ni au public pour les activités de recherche d'emploi* », peut-on ainsi lire dans l'article 2.5 des nouvelles conditions d'utilisation.

Par ailleurs, la section dédiée à la confidentialité de Linkedin, offre des informations utiles permettant aux utilisateurs de gérer leurs préférences et énumère quelques bonnes pratiques relatives à la sécurité d'un compte, parmi lesquelles :

- modifier son mot de passe régulièrement ;
- ne pas inscrire son adresse email ou son numéro de téléphone dans la section Résumé du profil ;
- activer la vérification en deux étapes ;
- signaler les contenus inappropriés ou les problèmes de sécurité.

## ➢ Les paramètres de sécurité Instagram

Fin août 2017, le réseau social Instagram annonçait publiquement avoir fait l'objet d'un piratage massif des données personnelles de ses utilisateurs, concernant les numéros de téléphone et les adresses mails d'environ 6 millions de comptes, dont des célébrités.

Les hackers auraient profité d'une faille de sécurité pour mettre en vente les données en ligne, sur plusieurs sites. La faille a depuis été corrigée mais elle aura eu pour effet bénéfique de rappeler aux utilisateurs l'importance de protéger leurs informations personnelles. Vous pouvez ainsi trouver toutes les informations utiles dans les pages d'aide de la section « **Espace Confidentialité et Sécurité** », comme par exemple apprendre :

- comment contrôler votre visibilité ;
- comment résoudre les abus et bloquer les personnes ;
- comment partager les photos en toute sécurité ;
- comment signaler les comptes piratés, une usurpation d'identité…

S'il y a très peu de réglages de confidentialité, il vous est toutefois possible de sécuriser votre compte en l'activant en tant que compte privé, ce qui permet de limiter l'accès à vos photos aux seuls utilisateurs que vous avez préalablement acceptés.

Par ailleurs, il convient de noter que par défaut, Instagram épingle vos photos sur une carte visible à partir de votre profil, ce qui permet à toute les personnes qui vous suivent de savoir exactement où vous êtes. Cette fonctionnalité peut toutefois être désactivée.

Enfin, petite originalité à souligner, il vous est également possible de modifier les paramètres de votre compte Instagram à partir de Facebook. Pour cela, il faut cliquer sur la flèche pointant vers le bas située en haut à droite de votre page Facebook, de sélectionner « **Paramètres »**, puis dans la colonne de gauche « **Applications »**. En dessous de l'cône Instagram, vous n'aurez alors plus qu'à cliquer sur la roue dentée pour accéder aux paramètres de ce compte.