Le WIFI, quelles pratiques pour les utilisateurs et les responsables du traitement ?

Nous avons tous l'habitude d'utiliser le WIFI pour nous connecter à Internet, à la maison, au travail, dans les lieux publics. Toutefois, pour l'utilisateur, ce geste habituel ne revêt pas la même sensibilité en fonction du lieu dans lequel s'opère la connexion.

En outre pour les entreprises mettant à disposition un accès WIFI, certaines obligations légales pèsent sur elles, différentes en fonction de la finalité pour laquelle l'accès est ouvert. Cette fiche pratique s'attache à résumer les réflexes à adopter pour toutes les catégories de personnes concernées par de tels traitements.

Le WIFI, Kézaco ?

Wi-Fi est une marque détenue par le consortium Wi-Fi Alliance.

Un constructeur informatique ou un fabricant de smartphones fournissant un produit compatible avec une des normes IEEE 802.11 (réseau sans fil) doit demander à la Wi-Fi Alliance (anciennement WECA) le droit d'apposer le nom Wi-Fi et le logo correspondant.

Le terme « *Wi-Fi* » est aujourd'hui largement connu pour être la contraction de « *Wireless Fidelity* » cependant cette explication est quelque peu erronée…

En effet le consortium Wi-Fi Alliance avait demandé à une agence de publicité de lui proposer un nom plus facile à utiliser que « *IEEE 802.11b Direct Sequence Spread Spectrum*».

L'agence lui a proposé plusieurs noms ; parmi ceux-ci, la « *Wi-Fi Alliance* » qui sonnait un peu comme « *Hi-Fi* », une marque reconnue dans un autre domaine…..

Le Wi-Fi repose sur la norme IEEE 802.11. Il s 'agit d'une technologie dite « *sans fil* » qui permet la connexion de tout type de matériel (ordinateurs portables, tablettes, imprimantes, téléphones mobiles, consoles de jeux, télévisions, équipements électroménagers, automates industriels, etc.) à des réseaux professionnels privés ainsi qu'au réseau public, Internet.

De la même façon que le fait votre téléphone mobile, la technologie « *Wi-Fi* » utilise des ondes radio pour transmettre des données à travers un réseau, tout équipement utilisant le wifi possède donc un adaptateur réseau sans fil qui traduira les données envoyées en un signal radio.

Ce même signal est alors transmis, par l'intermédiaire d'une antenne (Hotspot), à un décodeur : le routeur. Les données, une fois décodées, seront envoyées à l'Internet via une connexion filaire ou optique de la « *box* » vers l'opérateur.

Le terme « *Hotspot* » est utilisé pour définir une zone où la connexion Wi-Fi est disponible.

Vous êtes utilisateur de WIFI, quels risques et quelles précautions prendre hors de chez vous ?

De nombreux consommateurs sont convaincus que l'usage d'un mot de passe pour l'accès au Wi-Fi garantit la sécurité de leurs informations : ce n'est pas le cas.

Comme son nom l'indique, un Wifi-public est « *ouvert* », il n'y a pas vraiment besoin de code pour se connecter. Parfois, une adresse e-mail est demandée pour y accéder.

La principale caractéristique qui intéresse les personnes mal intentionnées est que les Wifi-publics ne sont pas chiffrés, mais d'autres risques existent, même en l'absence de mauvaise intention de la personne mettant à disposition le Wifi, tels que :

- Une **collecte trop importante d'informations** vous concernant ; par exemple, la CNIL a constaté qu'il est fréquent que des données portant sur le contenu des correspondances échangées ou des informations consultées (URLs) sont conservées alors que les fournisseurs du service ne sont pas autorisés à le faire ;

- Une **conservation trop importante d'informations** vous concernant : la CNIL a relevé que la plupart des fournisseurs de service conservent les données issues des journaux de connexion sans qu'aucune durée de conservation n'ait été définie. Or, les données de trafic doivent être conservées pendant 1 an à compter du jour de leur enregistrement ;

- Une **surveillance directe du trafic** internet visité.

Dès lors :

- Lors d'une connexion à un Wi-Fi gratuit, assurez-vous au préalable de n'être connecté à aucune de vos applications ;
- Ne visitez pas de pages (site web) requérant un login et mot de passe. Visitez uniquement des pages authentifiées (HTTPS). Bien réfléchir avant de cliquer sur un lien ;
- Couper « *l'application* » Wi-Fi si elle n'est pas utilisée, et notamment la reconnexion automatique : dans le cas contraire, si vous vous connectez à un point d'accès malveillant, votre équipement pourrait bien s'en souvenir et s'y reconnecter automatiquement lorsque ce point d'accès sera de nouveau à portée de connexion ;
- Garder en permanence le terminal à jour ;
- Certains réseaux Wi-Fi sont complètement fictifs et n'existent que pour récupérer des données. Restez donc vigilant. N'hésitez pas à vérifier la légitimité d'un réseau.

D'une manière générale :

- Evitez de passer par un Wi-Fi public pour transmettre/recevoir des données personnelles, surtout si celui-ci vous est inconnu ;
- Evitez de confier trop de données personnelles en échange d'un accès Wifi gratuit ;
- Préférez passer par le réseau 4G/5G de votre opérateur internet. Si vous n'avez pas le choix, privilégiez toujours la visite de sites HTTPS ;
- Optez pour un abonnement VPN qui apporte un chiffrement de bout en bout assurant la confidentialité des données que vous envoyez et recevez

Vous êtes une entreprise et vous mettez à disposition du public un accès Internet par WIFI :

- **Vous êtes concernée par les dispositions de l'article 10 de la Loi n° 1.430 sur la préservation de la sécurité nationale et de son Arrêté Ministériel d'application, ainsi que par les articles 389-11-2 et 398-11-5 du Code pénal**

L'article 389-11-2 du Code Pénal monégasque dispose qu' *« Il peut être différé* ***pour une durée maximale d'un an*** *aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques pour les besoins :*

1°) de la mise en œuvre des dispositions de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale (…) »

L'article 1er 2° de l'Arrêté Ministériel portant application l'article 10 de la Loi précitée dispose quant à lui que sont notamment qualifiés d' « opérateurs et prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques (…) les personnes qui offrent un accès à des services de communications électroniques au public en ligne, y compris à titre gratuit (…) », donc les responsables de traitement proposant du WIFI à titre gracieux, ou non, pour leurs clients ou visiteurs.

A cet égard, ils doivent donc collecter, « à l'exclusion des contenus des correspondances échangées (…)- Pour les personnes visées au chiffre 2° de l'article premier :

1° l'identifiant de la connexion ;
2° l'identifiant attribué par ces personnes à l'abonné ;
3° l'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;
4° les dates et heure de début et de fin de la connexion ;
5° les caractéristiques de la ligne de l'abonné.

- Pour les personnes visées au chiffre 3 et au chiffre 2, lorsque ces dernières les collectent pour leurs propres besoins :

1° l'identifiant de la connexion au moment de la création du compte ;
2° les nom et prénom ou la raison sociale ;
3° les adresses postales associées ;
4° les pseudonymes utilisés ;
5° les adresses de courrier électronique ou de compte associés ;
6° les numéros de téléphone ;
7° le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour ;
8° le type de paiement utilisé ;
9° la référence du paiement ;
10° le montant ;
11° la date et l'heure de la transaction.
Peuvent également être recueillies, auprès de l'ensemble des personnes visées à l'article premier, les données techniques relatives :

1° à la localisation des équipements terminaux ;

2° à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne ;
3° à l'acheminement des communications électroniques par les réseaux ;
4° à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne ;
5° aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels ».

Attention, l'article 389-11-5 du Code pénal monégasque précise que « *Les données conservées et traitées dans les conditions définies aux articles 389-11-2 à 389-11-4 portent exclusivement sur l'identification des personnes bénéficiaires ou utilisatrices des services fournis par les opérateurs et les prestataires de services, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.* ***Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée****.

Les opérateurs et les prestataires de services prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article.

Le fait, pour les opérateurs ou les prestataires de services chargés de l'exploitation de réseaux et de services de télécommunications et de communications électroniques, ou un de leurs agents, de ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives au trafic, dans les cas où ces opérations sont prescrites par la loi est puni d'un emprisonnement d'un an et de l'amende prévue au chiffre 3 de l'article 26.

Le fait, pour les opérateurs et les prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques, ou un de leurs agents, de ne pas conserver les données techniques dans les conditions où cette conservation est exigée par la loi, est puni d'un emprisonnement d'un an et de l'amende prévue au chiffre 3 de l'article 26 ».

- **Eu égard à la collecte de données à caractère personnel que vous effectuez, vous êtes un responsable du traitement au regard de la Loi n° 1.565 du 3 décembre 2024**

Il s'agit d'un traitement automatisé de données, qui a pour principales caractéristiques :

- la mise à disposition d'un accès Internet par le biais d'une borne WIFI ;
- l'information des personnes concernées par le biais d'une fenêtre/par l'acceptation de conditions générales ;
- la collecte des éléments d'identification et des logs de connexion d'une personne concernée pour une durée d'un an ;
- la restriction de l'accès à des sites indésirables.

Si vous avez au moins 50 salariés, vous devrez impérativement répertorier ce traitement dans votre registre des activités de traitement.

Et vous devez faire attention aux risques de sécurité pour votre système d'information si votre réseau WIFI n'est pas étanche (sécurisé).

En tout état de cause, collectez des données proportionnées à la finalité de la mise à disposition du WIFI.

ATTENTION : les dispositions de la Loi n° 1.430 ne semblent pas s'appliquer si vous êtes un employeur cloisonnant le wifi à une utilisation par ses salariés. Dans ce cas, il ne s'agit que d'une simple modalité particulière de connexion par l'entreprise au réseau Internet, qui est couverte par le traitement de *« Gestion administrative des salariés ».* Toutefois, si vous utilisez un outil de surveillance de consommation de l'Internet, les personnes concernées (les salariés) devront impérativement être informées de cette surveillance et de leurs droits, ceci que la connexion au réseau soit filaire ou par WIFI. Par ailleurs, la réalisation d'une analyse d'impact pourrait être nécessaire.