Quelle réglementation pour le WiFi public ?

Vous avez installé une borne WiFi dans vos locaux ? Saviez-vous qu'il existe des obligations légales quant à la mise à disposition d'un WiFi gratuit ?

La réglementation du WiFi public en France impose plusieurs règles à suivre afin de protéger l'établissement fournisseur ainsi que les clients eux-mêmes.

La législation s'articule autour de plusieurs points qui sont la sécurité des connexions à internet, la protection des données personnelles et l'usage responsable des réseaux WiFi publics. Plusieurs organismes travaillent conjointement sur le sujet du WiFi public : l'ARCEP, la CNIL et l'Hadopi.

POURQUOI AVOIR CRÉÉ UNE LÉGISLATION DÉDIÉE AU WIFI PUBLIC ?

De plus en plus de lieux accessibles au public sont équipés de hotspots WiFi pour offrir un accès facile à internet en mobilité depuis un ordinateur portable, un smartphone ou une tablette. Cependant, une connexion public implique un certain anonymat, ce qui a posé un réel problème lorsque des infractions ont été commises.

Sur un réseau sans fil privé, la justice se tourne automatiquement vers le propriétaire de la ligne mais cela n'est pas applicable dans le cadre d'un accès WiFi public. Parmi ces infractions, on retrouve par exemple le piratage ou le vol de données personnelles si on se restreint aux délits mais on peut également parler de pédopornographie ou de terrorisme si on s'étend aux crimes.

Afin d'apporter une réponse adaptée à l'utilisation du WiFi public, l'Etat français a créé une réglementation pour le WiFi public afin d'en contrôler les usages tout en respectant les libertés individuelles.

LA DÉCLARATION EN TANT QU'OPÉRATEUR WIFI

Par "opérateur", on entend toute personne physique ou morale qui exploite un réseau de communications électroniques ouvert au public ou qui fournit au public un service de communications électroniques (art. L.32 du code des poste et des communications électroniques).

La réglementation du WiFi impose d'effectuer une déclaration d'opérateur à l'ARCEP (Autorité de Régulation des Communications Electronique et des Postes) pour être reconnu officiellement comme établissement offrant un accès Wifi.

Dans le cas où il s'agit d'un "réseau interne ouvert au public", comme dans les hôtels, les gîtes ou chambres d'hôtes, ou d'un "réseau indépendant", dans une entreprise par exemple, l'obligation de déclaration n'est pas applicable.

Si vous souhaitez fournir une connexion WiFi gratuite à vos clients ou vos visiteurs, vous avez deux possibilités :

- souscrire un abonnement auprès d'un opérateur WiFi comme Noodo : les obligations légales évoquées par la suite ne vous concerne plus, c'est l'opérateur WiFi qui va en assumer la responsabilité
- créer votre propre hotspot WiFi, vous déclarer en tant qu'opérateur WiFi (si applicable) et d'acquitter des taxes qui découlent de ce statut, respecter les obligations légales expliquées ci-dessous

Même si vous n'êtes pas concerné par la déclaration d'opérateur WiFi, l'article L34-1 du Code des Postes et des Communications électroniques stipule que "les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques".

Authentifier les connexions au réseau sans fil par l'intermédiaire d'un portail captif

Pour se connecter à un WiFi public, l'utilisateur doit en premier lieu s'identifier et s'authentifier grâce à la création d'un compte ou en fournissant des données personnelles comme son adresse mail. De cette manière, il pourra être reconnu en fonction de son activité lors de sa connexion.

L'intérêt du portail captif n'est pas seulement d'être un panneau publicitaire pour l'établissement, il permet de tracer l'activité des utilisateurs (voir plus loin) en imposant un processus liminaire d'authentification. La connexion à un point d'accès Wifi n'est donc pas anonyme, il est important de le rappeler.

Attention, si vous demandez une adresse e-mail pour s'authentifier sur le réseau WiFi de votre établissement et que vous souhaitez la réutiliser pour des démarches commerciales ensuite, vous devez également respecter la législation, en l'occurrence la loi du 6 janvier 1978 Informatique et Libertés. L'utilisateur doit accepter l'exploitation commerciale de son adresse e-mail.

Conserver les données techniques de connexion pendant un an

La traçabilité des accès et l'enregistrement de l'activité des utilisateurs sur votre accès WiFi est à appliquer pour respecter la loi du 23 janvier 2006 relative à la lutte anti-terroriste ainsi que la directive européenne du 15 mars 2006.

Les traces de connexion doivent être conservées pendant un an (fixé par le décret du 24 mars 2006), transmises à la CNIL (Commission Nationale de l'Informatique et des Libertés) et utilisées en cas de litiges avec la justice.

Attention à bien différencier données techniques (ou données de trafic) et données personnelles. Un opérateur WiFi ne doit en aucun cas enregistrer le contenu des communications effectuées par un utilisateur par l'intermédiaire de son hotspot WiFi. Il n'a donc pas accés

Par données techniques, on entend (d'après le Décret n°2006-358 du 24 mars 2006, article R. 10-13 du CPCE) :

- le terminal utilisé pour se connecter
- la date, l'horaire et la durée des communications

que forme

les informations techniques pour identifier les destinataires des communications

Ces données pourront être demandées par les autorités et notamment la police judiciaire ou spécialisée dans les activités terroristes. Refuser de communiquer ces données est punissable de 30 000€ d'amende.

Lutter contre le téléchargement illégal et la diffusion de contenus sensibles ou choquants

La législation WiFi est également liée à la loi Hadopi (loi « Création & Internet » du 12 juin 2009) pour la protection des droits d'auteurs et interdisant le téléchargement illégal. Cette loi précise que *la personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins illégales*. Elle impose la sécurisation de la connexion sans fil et requiert donc :

un filtrage des accès P2P et des sites de téléchargement pour éviter toute activité illégale (la mise en place d'un pare-feu peut limiter ce genre d'activités)

un filtrage de contenu : les sites interdits par la réglementation comme les sites de pédophilie ou prônant un message terroriste doivent être bannis et bloqués d'accès pour vos clients.

Tous les professionnels utilisant le WiFi pour leur propre activité ou bien pour mettre internet à disposition de leurs clients sont concernés par cette politique de sécurisation imposée par la loi Hadopi.

UNE CONNEXION INTERNET RÉGLEMENTAIRE DANS LES LIEUX PUBLICS AVEC NOODO

Les hotspots WiFi déployés par Noodo, opérateur WiFi déclaré à l'ARCEP, respecte l'ensemble des obligations légales relatives à la mise à disposition d'un point d'accès à internet sans fil.

Le client est déresponsabilisé juridiquement des infractions pouvant être commises sur son réseau. En cas d'enquête, les autorités de police prennent directement contact avec Noodo.

Noodo
FEEL CONNECTED

NOUS SUIVRE

CONNEXION CLIENT

ACTIVEZ VOTRE INSTALLATION