

FICHE PRATIQUE N° 1

REGLEMENTATION DU WiFi PUBLIC

Seriez-vous concerné sans le savoir ?

LE WiFi PUBLIC EN FRANCE

Les bornes WiFi permettant d'accéder à internet via les réseaux sans fil, se sont multipliées dans les lieux publics français. Les utilisateurs équipés d'appareils mobiles compatibles WiFi (ordinateurs portables, téléphones portables, assistants personnels) ont ainsi la possibilité de se connecter au Web ou à des applications professionnelles (extranet,...) pendant leurs déplacements.

Cependant, l'essor du WiFi a posé une nouvelle problématique dans la lutte contre les infractions liées aux nouvelles technologies. S'il est possible d'être clairement identifié lors de l'utilisation de moyens de communications traditionnels (téléphonie fixe et mobile, accès internet à la maison), les bornes WiFi offrent, quant à elles, **un moyen de communication permettant d'œuvrer anonymement et donc impunément.**

Parmi les infractions liées à l'usage d'internet, on distingue :

Les fraudes et la cyber-délinquance

- Atteinte à la vie privée,
- Escroquerie en ligne,
- Piratage de réseaux privés

La cybercriminalité

- Pédopornographie,
- Crimes organisés,
- Terrorisme...

Pour répondre à ces menaces croissantes, l'Etat français a mis en place, conformément aux directives européennes, un cadre législatif visant à limiter l'anonymat des utilisateurs de WiFi public, dans le but d'assurer la sécurité des citoyens, tout en garantissant le respect des libertés individuelles.

Cette fiche pratique a pour vocation d'apporter, en s'appuyant sur la réglementation en vigueur, l'indispensable éclairage sur les responsabilités et les risques inhérents à la mise à disposition d'un service WiFi.

Les organismes en charge de la réglementation du WiFi public en France

ARCEP

L'Autorité de Régulation des Communications Electroniques et des postes a été créée en 1996 pour réguler la concurrence dans le secteur des télécommunications. Cette autorité contrôle également le respect des normes d'émissions.

HADOPI

L'Hadopi est une institution exclusivement dédiée à la diffusion des œuvres et la protection des droits sur internet. Elle crée un précédent inédit propre à faire évoluer les débats et problèmes rencontrés par le droit d'auteur sur internet.

CNCIS

La Commission Nationale de Contrôle des Interceptions de Sécurité est une autorité administrative indépendante chargée de veiller au respect des dispositions relatives aux correspondances émises par la voie des communications électroniques.

CNIL

La Commission Nationale de l'Informatique et des libertés a été instituée par la loi n° 78-17 du 6 janvier 1978. Cette autorité indépendante fixe les règles relatives à l'informatique, aux fichiers et aux libertés.

WIRELESS LINK

Association loi 1901 rassemblant les principaux opérateurs WiFi français autour de la promotion d'un service WiFi de qualité en terme de connexion, de performances réseau, de disponibilité du service, d'assistance ou encore de sécurité.

L'AUTORITE JUDICIAIRE*

L'autorité judiciaire veille au respect de la réglementation du WiFi public. Elle s'appuie pour cela sur les enquêtes des services de police et de la gendarmerie nationale dans le cadre de réquisition judiciaire classique. Une procédure de réquisition administrative spécialement créée pour la lutte contre le terrorisme permet aux services concernés, tels que la Direction de Surveillance du Territoire (DST), d'agir plus rapidement.

*Ministère de l'intérieur

QU'EST-CE QU'UN FOURNISSEUR D'ACCES INTERNET?

L'article L32 du Code des Postes et des communications considère comme fournisseur d'accès internet :

- Les fournisseurs d'accès à des réseaux de communications électroniques accessibles via une borne WiFi,
- Les individus dont l'activité a spécifiquement pour objet l'offre d'un service payant de connexion en ligne tels que les gérants de « cybercafés »,

- Les personnes qui offrent, dans un cadre public, une connexion internet à leurs clients ou à des visiteurs, notamment les hôtels/restaurants, les aéroports ou encore le transport public.

**OUVRIR UN ACCES WiFi PUBLIC,
C'EST DEVENIR FOURNISSEUR D'ACCES INTERNET.**

Cas pratique

Un transporteur souhaite offrir un accès internet à ses passagers, s'offrent à lui deux possibilités :

- 1.** Il décide de faire appel à un fournisseur d'accès internet ; c'est à dire à un professionnel déclaré à l'ARCEP, dans le but de lui confier son service d'accès public.
Conséquence : le transporteur n'est pas considéré comme un opérateur de communications électroniques. Il n'est pas soumis à la réglementation, son fournisseur d'accès internet prenant à sa charge le bon respect des obligations légales pour son compte.
- 2.** Il décide de gérer lui-même son service d'accès.
Il achète du matériel WiFi et fait alors appel à un opérateur téléphonique qui se chargera de déployer et éventuellement de maintenir les équipements.
Conséquence : Le transporteur est considéré comme un fournisseur d'accès internet. Il a l'obligation déclarative de son activité auprès de l'ARCEP, il prend à sa charge la taxe administrative annuelle de 10 K€ à 20 K€ en fonction de son chiffre d'affaires et le bon respect de l'ensemble des obligations légales inhérentes à son statut d'opérateur.

LA REGLEMENTATION

Définitions et principes édictés par l'article L32 du Code des Postes et des Communications électroniques.

Communications électroniques

« On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique. »

Réseau ouvert au public

« On entend par réseau ouvert au public tout réseau de communications électroniques établi ou utilisé pour la fourniture au public de services de communications électroniques ou de services de communication au public par voie électronique. »

Opérateur

« On entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques. »

OBLIGATIONS D'UN OPERATEUR WiFi

1. La collecte et le stockage de données techniques pendant un an.

La loi de janvier 2006 introduit dans le code des postes et télécommunications² des dispositions qui obligent les opérateurs de communications électroniques à conserver pendant une durée d'une année certaines données de caractère technique concernant leurs utilisateurs.

En effet, les nouvelles obligations doivent permettre aux autorités de disposer d'indices suffisants en cas de recherche de preuve dans le cadre de la prévention des actes de terrorisme.

Cette obligation concerne bien évidemment les opérateurs WiFi³.

Catégories d'information dont la conservation est obligatoire⁴ :

- Les informations permettant d'identifier l'utilisateur
- Les données relatives aux équipements terminaux de communication utilisés
- Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication
- Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs
- Les données permettant d'identifier le ou les destinataires de la communication

Les opérateurs n'ont aucune obligation de constitution de fichiers nominatifs des utilisateurs : Les organismes fournissant une connexion WiFi peuvent choisir d'offrir cette prestation sans procéder à l'identification des personnes. Ils ne sont alors tenus que de détenir les données techniques créées par l'utilisation de leurs services.

Les opérateurs ne doivent conserver que les seules données techniques.

Ils ne doivent pas conserver les informations relatives au contenu des communications : le texte d'un SMS, l'objet et le contenu d'un email, etc.

LA REGLEMENTATION

Article L34-1 du Code des Postes et des Communications électroniques

« 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. »

La commission Nationale de Contrôle des Interceptions de Sécurité peut à tout moment procéder à des contrôles relatifs aux opérations de communications électroniques. Le non respect de cette loi est sanctionné pénalement : jusqu'à 5 ans d'emprisonnement et 300 000 € d'amende.

¹ Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant sur les diverses dispositions relatives à la sécurité et aux contrôles frontaliers.

« Afin de prévenir les actes de terrorisme, les agents des services de police et de gendarmerie nationale peuvent exiger des opérateurs la communication des données conservées et traitées par ces derniers. »

² Code des postes et des télécommunications, Art. L 34-1.

³ Avis n° 2005-0918 du 13 octobre 2005 sur le projet de loi relatif à la lutte contre le terrorisme.

⁴ Code des postes des télécommunications, Art L 34-1 1.

2. Le respect des libertés individuelles des utilisateurs

Les données à caractère personnel doivent être collectées de manière loyale et doivent être destinées à des finalités déterminées, explicites et légitimes.

La collecte des données personnelles doit au préalable avoir reçu le consentement de la personne concernée et celles-ci doivent être librement consultables et modifiables.

Seuls la collecte et le traitement des données techniques définies dans l'article L.34-1 du code des postes et des communications électroniques (cf page 6) font exception à la règle d'accord préalable.

Mises à part ces données techniques, la loi informatique et Libertés s'applique à la collecte et le traitement de toutes les données à caractère personnel.

Le non respect de la loi Informatique et Libertés est sanctionné pénalement : jusqu'à 5 ans d'emprisonnement et 300 000 € d'amende.

LA REGLEMENTATION

Loi du 6 janvier 1978 Informatique et Libertés :

« L'informatique ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »

Toutes ces obligations légales ont amené les transporteurs suivants à faire le choix d'un fournisseur d'accès internet responsable : ICON France SAS

ID BUS
RATPDEV / Orly & Roissy bus
COURRIERS RHODANIENS
GROUPE SALAÛN
GROUPE PHILIBERT
KEOLIS ATLANTIQUE / AUDE / VAL DE SAONE
GUDERZO TOURISME
MASTERCAB SERVICES / PSG

ICON SA créée en 1999 et sa filiale ICON France SAS créée en décembre 2013 sont opérateurs de réseau WiFi embarqué et fournisseurs de services de communications électroniques au public.

Elles s'adressent plus particulièrement aux :

- Autocars et autobus,
- Trains et tramways,
- Bateaux
- Taxis

Les engagements d'un fournisseur d'accès internet responsable :

ICON SA vous garantit un service WiFi embarqué en totale conformité avec la réglementation en vigueur et ses évolutions.

- Les données techniques nécessaires sont collectées, stockées et traitées sur des plateformes sécurisées et transmises systématiquement aux autorités dans le cadre de réquisitions judiciaires.
- Le respect des libertés individuelles est garanti et aucune donnée nominative n'est ni collectée ni utilisée sans l'accord préalable de l'intéressé.
- Toutes les installations sont conformes aux normes édictées par l'ARCEP sur la fréquence et la puissance des émissions des ondes électromagnétiques.

**Faire confiance à ICON SA, c'est l'assurance
d'un service WiFi conforme à la
réglementation.**