LE WiFi PUBLIC EN FRANCE

Depuis le début des années 2000 ; 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, ou leurs séjours à l'hôtel par exemple.

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 :	***La cybercriminalité :***
Atteinte à la vie privée,	Pédopornographie,
Escroquerie en ligne,	Crimes organisés,
Piratage de réseaux privés	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 rubrique 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.

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.

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.

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'Accès Internet (FAI) ?

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 à 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 :

☑ 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.

☒ 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 en fonction de son chiffre d'affaires (en K€) 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. »

Extrait des conditions générales des opérateurs de télécommunications français

Orange
Article 38
« FOURNITURE DE LA CARTE PAR ORANGE BUSINESS SERVICES 38.2. Sauf autorisation préalable et écrite d'Orange Business Services, le Client s'interdit d'associer la Carte avec des solutions techniques ayant pour objet le réacheminement de Communications par tout procédé technique, la mutualisation d'un Service auprès de plusieurs Utilisateurs, ou la mise en relation. De façon générale, et notamment dans de telles hypothèses, Orange Business Services se réserve la possibilité de suspendre, puis de résilier la Commande concernée. Le Client se verra alors facturer rétroactivement des Communications sur la base d'un tarif au compteur qui lui serait applicable. »
Article 44
« CAS PARTICULIER DE L'ACCES A UN SERVICE COMPRENANT DES COMMUNICATIONS ILLIMITEES dans le cadre du Service concerné, le Client et ses Utilisateurs s'interdisent toute utilisation frauduleuse telle que notamment : l'utilisation des Communications illimitées à des fins commerciales (revente des Communications illimitées), l'association des Cartes à toute solution de réacheminement de trafic, sauf accord exprès d'Orange Business Services, l'utilisation ininterrompue du forfait par le biais notamment d'une composition automatique et en continu de numéros sur la Ligne, envoi de SMS en masse de façon automatisée ou non. En cas de non-respect d'un comportement raisonnable relatif à des communications illimitées voix, Orange Business Services se réserve le droit de suspendre le Service. En cas d'utilisation frauduleuse, sauf exception telle que précisée au paragraphe ci-dessous, Orange Business Services se réserve le droit de suspendre le Service puis de résilier la Commande concernée conformément aux stipulations des présentes. En cas d'utilisation des Communications illimitées à des fins commerciales (notamment revente des Communications illimitées), Orange Business Services résiliera de plein droit et sans préavis la Commande concernée.

Bouygues
Article 9.3
« Par ailleurs, concernant les offres de communications illimitées, le Client s'interdit toute utilisation frauduleuse telle que notamment : l'utilisation des communications illimitées à des fins commerciales (revente des communications), l'utilisation d'offres ou services « voix » à des fins d'usage data, notamment pour les besoins d'application de type Machine to Machine. »
Article 7.6
« Sans préjudice de l'application des dispositions précédentes, s'agissant plus spécifiquement des cartes SIM, le Client s'interdit toute utilisation avec un boîtier de raccordement radio ou avec toute autre solution technique ayant pour objet la modification d'acheminement du Service et/ou des services en option. »

SFR
Article 3
« L'Abonné est seul responsable de l'utilisation et de la conservation de la carte SIM dont il s'interdit toute duplication. La carte SIM ne peut pas être utilisée par l'Abonné pour proposer une offre commerciale à un tiers. Plus généralement, l'abonné s'interdit toute utilisation commerciale de l'accès au réseau SFR qui est mis à sa disposition, notamment en
permettant à des tiers d'accéder au réseau de SFR moyennant une contrepartie notamment financière. La carte SIM ne peut pas être utilisée, par l'Abonné, par un exploitant de réseau de télécommunication ou par un fournisseur de services de télécommunication, aux fins de modifier l'acheminement d'un service de télécommunication sur un réseau public de télécommunication. Notamment, elle ne peut pas être utilisée dans le cadre de boîtiers radio ni en émission, ni en réception. Tout usage frauduleux de la carte SIM, ou contraire aux présentes conditions, engage la responsabilité personnelle de l'Abonné »

Obligations d'un opérateur WiFi

Offrir un accès WiFi au public doit se faire dans le respect du cadre règlementaire en vigueur en France

La collecte et le stockage de données techniques pendant un an

La loi de janvier 2006[1] introduit dans le Code des Postes et Télécommunications[2] 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 WiFi[3]

Catégories d'information dont la conservation est obligatoire :

- 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, la durée, et le lieu** 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 Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS) peut à tout moment procéder à des contrôles relatifs aux opérations de communications techniques.
Le non-respect de cette loi est sanctionnée pénalement : jusqu'à 5 ans d'emprisonnement et 300.000 euros d'amende.

LA REGLEMENTATION

[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] Articles L34-1 et L34-1-1 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. »

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

Le respect des normes d'émission d'ondes

Dans un souci de prévention de tout risque lié aux ondes WiFi sur la santé publique, l'Autorité de Régulation des Communications Electroniques et des postes (ARCEP) a fixé les conditions d'émissions des ondes électromagnétiques émises par les bornes WiFi. Ces conditions ont été reprises par le décret n° 2002-775 du 3 mai 2002 qui a légiféré sur la fréquence et la puissance des ondes émises par les bornes WiFi.

La fréquence :
Plus la fréquence d'une onde est basse, plus elle est susceptible de pénétrer dans la matière et donc d'avoir d'impact sur les individus exposés.
L'ARCEP a fixé à 2540 Mhz le niveau des champs électromagnétiques produits par les réseaux WiFi public.
Pour comparaison, la radio FM et la téléphonie mobile (GSM) utilisent toutes deux des fréquences bien plus basses, et donc plus nuisibles avec respectivement des fréquences comprises entre 87,5 et 108 Mhz d'une part et entre 900 et 1900 Mhz d'autre part.

La puissance :

L'ARCEP a fixé la puissance des ondes émises depuis une borne WiFi à une limite maximale de 0,1 Watt, soit une puissance 20 fois plus faible que celle des téléphones portables (2 Watts).
La distance entre l'émetteur et l'individu fait fortement diminuer la puissance des ondes. En effet, à une distance de 20 centimètres de la borne WiFi, l'énergie des ondes est déjà divisée par deux et **au delà de 50 centimètres elle est même divisée par dix**.

AVIS D'EXPERTS

La Fondation Santé et Radiofréquences a, lors d'une rencontre scientifique organisée en octobre 2007, conclu que « les études menées jusqu'à aujourd'hui n'ont permis d'identifier aucun impact des radiofréquences sur la santé en deça des limites de puissance légales. »

L'Agence Française de Sécurité Sanitaire de l'Environnement et du Travail (AFSSET) qui fait office de référence en matière d'avis sanitaire sur l'impact des radiofréquences a rendu le même avis sur le WiFi. Dans son rapport sur la Téléphonie Mobile daté d'avril 2005, l'ARSSET conclue ainsi :
« l'exposition au WiFi est toujours en champ lointain (au moins 50 cm) et ***la puissance d'émission est faible. S'agissant de la technologie WiFi, les puissances très faibles engagées, ainsi que les fréquences élevées impliquent une exposition très inférieure par rapport à celle de la téléphonie mobile classique****. »*

Le non-respect des normes d'émissions WiFi est sanctionné pénalement : jusqu'à 6 mois d'emprisonnement et 190 000 € d'amende.

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. »

REGLEMENTATION SPECIFIQUE POUR VEHICULES

Norme ECE R10

Le matériel embarqué doit répondre aux normes de compatibilité électromagnétique. La directive 95/54 CE introduit les notions suivantes :

- ⇨ les fonctions reliées au "contrôle direct" du véhicule, on sous-entend par là, toutes fonctions pouvant agir : par dégradation ou changement au niveau de la motorisation, du changement de vitesse, du freinage, de la suspension, etc…, susceptible d'affecter la position du conducteur, soit par exemple : le siège à mémoires, le positionnement du volant, susceptible d'affecter la visibilité du conducteur tel que les organes liés aux essuie-glaces.
- ⇨ les fonctions liées au conducteur et à ses passagers, aux autres usagers de la route : exemple : airbag
- ⇨ les fonctions susceptibles de créer des confusions pour le conducteur ou autres usagers de la route : perturbations optiques (ex. : feux clignotants, feux stop, fausse information des lampes témoins), perturbations acoustiques significatives (ex. : alarme, avertisseur sonore)
- ⇨ les fonctions liées au fonctionnement des bus de données : blocage de la transmission des données
- ⇨ les fonctions particulières telles que l'odomètre, le tachygraphe

Norme ECE R 118

Relative au comportement au feu de certaines catégories de véhicules à moteur. Il s'agit là du fil entre l'antenne extérieur et la box WiFi, qui doit résister à l'incendie selon la norme.

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

WIIBUS 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 WIIBUS, c'est l'assurance d'un service WiFi conforme à la règlementation