

Wifi invités : le point juridique



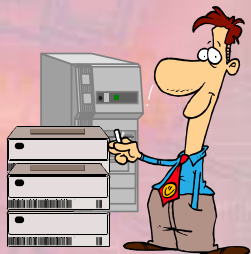
Madame X reçoit depuis quelques jours des appels téléphoniques assez graveleux.

Face à la situation, elle décide de porter plainte auprès de la police française.



Après investigation, il s'avère que les coordonnées de cette dame ont été rentrées sur un site web de rencontre (assez célèbre du reste !).

L'adresse IP à l'origine de cette création est identifiée après réquisition auprès du fournisseur d'accès internet. Il s'agit de la société **FIWI**.



Monsieur Y, informaticien de la société **FIWI** qui est interrogé confirme que cette adresse IP est bien celle de son entreprise et qu'elle correspond à la sortie internet d'un réseau Wifi invité (Guest) mis à disposition des clients qui viennent se former régulièrement sur leurs produits.

Les problèmes vont bientôt commencer pour Monsieur Y



Suivant l'article L.33-1 du Code des Postes et des Communications Electroniques (**CPCE**), avez-vous fait une déclaration à l'**ARCEP** (Autorité de Régulation des Communications Electroniques et des Postes) pour la fourniture au public de services de communications



Mon beau-frère qui travaille justement à l'**ARCEP**, et à qui j'ai posé la question, m'a bien dit qu'une telle déclaration n'est pas exigée pour l'exploitation de « réseaux internes ouverts au public ». L'installation d'un réseau de communication électronique dans un **espace privé, qui bien qu'ouvert au public n'empiète pas sur le domaine public.**



La vraie question qui se pose est de savoir si avec cette architecture en place votre société est devenue un **FAI** (Fournisseur d'Accès à Internet) ou un **OCE** (Opérateur de communications électroniques) – que dit la loi à cet égard



Une réponse de bon sens voudrait qu'un hôtel, un restaurant ou une entreprise privée ne soit pas assimilés à des SFR, Orange ou Free (désolé si j'ai oublié des sociétés représentées dans la salle). Les textes ne sont pas aussi clairs

Les contenus

- La problématique principale de l'utilisation de l'Internet concerne les actions litigieuses et principalement l'accès à des sites non autorisés.
- En tant de fournisseur d'accès, l'entreprise **FIWI** doit bloquer les accès aux sites Internet pédophiles, négationnistes et racistes. Dans la mesure où elle n'est pas hébergeur, elle n'a pas obligation de contrôler les contenus des sites.
- Dans le cadre de la LEN, l'entreprise **FIWI** doit aussi être en mesure de répondre à une sollicitation de la justice pour le blocage de certains sites dont le contenu serait jugé comme illégal (article 43-12)
- Enfin, l'entreprise **FIWI** doit mettre en œuvre les mesures nécessaires pour ne pas être considérée comme complice passif par mise à disposition de moyens, des usagers qui utiliseraient l'accès pour des actions illicites (téléchargement non autorisés, attaques de sites, contamination de sites, envoi de messages abusifs, licencieux ou de diffamatoires, etc.).

Les solutions

- Informer les utilisateurs des droits et des devoirs qu'il ont en utilisant l'accès mis à disposition (charte, affiche..) en précisant que l'entreprise **FIWI** n'est pas tenue responsable des actions qu'ils peuvent réaliser.
- Informer les utilisateurs de l'existence de moyens techniques permettant de tracer et de restreindre les accès à certains services.
- Ne pas laisser de moyen de stockage sur les postes libre service, ni de transfert direct sur support externe, mais mettre en œuvre une procédure de copie de données.

Les textes de loi

- La loi **LCEN** (Loi pour la Confiance dans l'Economie Numérique) du **21 Juin 2004** a pour objet de répondre aux objectifs fixés par la Commission européenne; directive du 8 Juin 2000 sur le commerce électronique (**2000/31/CE** du parlement européen. Elle complète loi N°**86-1067** du 30 Septembre 1986 relative à la liberté des communications. Cette loi impose la conservation des données si l'autorité judiciaire si elle lui en fait la demande. Le FAI reste tenu au secret professionnel. Tout manquement expose la personne à **1 an** d'emprisonnement et à **75K€** pour les personnes physiques et **375K€** pour les personnes morales.
- L'article **L.34-1** du **CPCE** reprend cette exigence. L'**OCE** doit conserver les données permettant l'identification des personnes utilisatrices des services.
- L'article **R.10-13** du **CPCE** issu du décret du 24 Mars 2006 qui décrit les catégories de données à conserver. Ce décret fixe la durée de conservation de données à **1 an**, durée au-delà de laquelle ces données devront être anonymisées.

Les textes de loi (suite)

- La loi '**Informatique et Libertés**' du 6 Janvier 1978 pour respecter les obligations d'information des personnes quant à leur droits d'accès, de rectification, d'opposition et de suppression.
- La loi **Création & internet** (Loi HADOPI) du **12 Juin 2009** impose aux titulaires d'une connexion sans fil de sécuriser celle-ci afin d'empêcher que des activités illicites soient pratiquées depuis l'ordinateur d'un abonné à son insu.

Qu'est-ce qu'un FAI au sens légal du terme ?

- L'article 6-I 1° de la **LCEN** dit qu'il s'agit « de personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne.. » L'entreprise **FIWI** n'est donc pas dans le scope.
- Seulement l'article L.32 du **CPCE** dit que « l'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 communication électronique. L'entreprise **FIWI** revient dans le scope.
- L'**ARCEP** a tenté de calmer le jeu dans une lettre (n°41) en réduisant le scope, mais le texte n'est pas clair pour les entreprises.
- La loi anti-terroriste du 23 Janvier 2006 visant « la lutte contre l'utilisation à des fins terroristes des moyens anonymes de connexion à Internet dans les lieux publics » vient ajouter de la complexité.

Qu'est-ce qu'un FAI au sens légal du terme ?

- La **L.34-1 CPCE**, modifiée par la loi anti-terroriste, dispose que les personnes qui «au titre d'une activité professionnelle principale ou accessoire, offre 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 communication électroniques »
- Le législateur renvoie à la charge du juge la mission de déterminer si le lieu ou l'activité de la personne proposant le service de connexion, la rattache à la catégorie d'**OCE**
- La **CNIL** dans une délibération N°2005-208 du 10 Octobre 2005 relative à la loi 2006, a indiqué, toute en regrettant l'ambigüité de la définition retenue, que les entreprises et leurs salariés devraient être exclus du champs d'application de cette loi et ne pas être perçu comme « public ». Mais quid des visiteurs d'une entreprise ?

La jurisprudence

➤ La cour d'appel de Paris, dans un arrêt du 4 Février 2005, a estimé quant à elle qu'une banque était assimilable à un **OCE**. Dans l'affaire, une société de presse s'était adressée à la banque après avoir découvert que des messages électroniques dommageables avaient été émis depuis le routeur de celle-ci.

Article **43-9** de la loi du **1^{er} Aout 2000** modifiant la loi du 30 Septembre 1986 relative à la liberté de communication, de détenir et conserver des données de nature à permettre l'identification de toute personne ayant contribué à la contenu de services dont elle est prestataire. La cour d'appel a assimilé cette banque à un **OCE**.

➤ L'**ARCEP** va quand à elle à l'encontre de la décision de la cour d'appel de Paris – toute entreprise dont les activités se limitent à assurer la configuration, l'administration, la surveillance et la maintenance de serveurs informatiques *ne peut être considérée comme un opérateur de communications électroniques et être soumise aux dispositions de l'article L.34-1 du CPCE*.

Les autres législations en dehors de France

➤ Japon – Corée

De très nombreux Wifi non sécurisés sont disponibles. En ce qui concerne l'usage illégal d'une connexion Internet (téléchargements illégaux, hébergement ou visites de sites dont le contenu est illégal): un ayant-droit, une administration, ou même la Police se tourneront d'abord vers le FAI. Le FAI avertira une fois l'abonné et lui enjoindra de sécuriser sa connexion. Si des pratiques illégales se poursuivent sur cette connexion, le FAI dégage sa responsabilité, coupera la connexion, et transmettra les coordonnées de l'abonné à la Police ou aux ayant-droits.

En bref: si je parasite le wifi de mon voisin pour commettre quelque chose d'illégal, c'est lui sera tenu pour responsable sauf s'il peut prouver que c'est moi le coupable. Sur ce sujet, la loi est à peu près la même au Japon et en Corée.

Les autres législations en dehors de France

➤ Australie

http://www.acma.gov.au/WEB/HOMEPAGE/pc=PC_1739

➤ Nordic countries

La responsabilité est plus sur les entreprises que sur les **FAI**

➤ Portugal

<http://www.anacom.pt/render.jsp?categoryId=1644&languageId=1>

➤ Italie

Les entreprises doivent conserver 6 mois de logs. Le FAI renforce les contrats de connexion.

➤ Pologne, Inde

Pas de restrictions

| Version | Date | Débit radio max (courte distance) en Mbit/s | Bandes en GHz | Canaux ²⁰ | Largeur des canaux en MHz | Débit applicatif max ²¹ en Mbit/s |
|---------|------|---|--|---|---------------------------|--|
| 802.11a | 1999 | 54 | 5,15-5,35 5,47-5,725 5,725-5,875 | 19 canaux 8 canaux non recouvrants | 20 | 25 |
| 802.11b | 1999 | 11 | 2,4-2,5 | 14 canaux 3 non recouvrants (1, 6, 11) | 22 | 5 |
| 802.11g | 2003 | 54 | 2,4-2,5 | 14 canaux 3 non recouvrants (1, 6, 11) | 22 | 25 |
| 802.11n | 2007 | 600 | Bande des 2,4 ou 5 GHz | - | - | > 100 Mbit/s |

IEEE 802.11 ou ISO/IEC 8802-11

