



La réglementation des Hotspots WIFI
23/04/2010 par Julie TOMAS.

L'opérateur Wifi est défini à l'article L32 du CPCE, comme le fournisseur d'accès à des réseaux de communications électroniques accessibles via un Hotspot Wifi, celui dont l'activité a pour objet d'offrir un service payant de connexion en ligne, par exemple le responsable d'un cybercafé et celui offrant, au sein d'un lieu public, une connexion Internet à ses visiteurs, par exemple les hôtels ou restaurant.

Quelles sont les obligations à remplir ?

Les obligations à remplir par l'opérateur Wifi sont précisées à **l'article L34-1 du CPCE** : il doit se plier aux **normes concernant l'émission d'ondes**. Ainsi l'ARCEP a fixé à **2450 Mhz** le niveau des champs électromagnétiques produits par les réseaux Wifi public et à une limite de **0.1 Watt** la puissance des ondes émises depuis un Hotspot.

En cas de non respect de ces normes l'opérateur Wifi peut encourir jusqu'à 6 mois d'emprisonnement et 190 000 Euros d'amende

Il doit respecter les dispositions relatives à **la conservation des données techniques concernant ses utilisateurs**.

Souscrivant à une offre de service d'accès Internet auprès d'un Fournisseur d'Accès Internet (FAI), ce dernier enregistre le trafic effectué depuis la connexion et cela pour des questions de sécurité. En fournissant un accès Wifi au public à partir d'une connexion Internet, l'on endosse les mêmes responsabilités que le FAI puisque de fait l'on devient fournisseur d'accès Wifi.

Ces données techniques correspondent à des données de trafic générées par l'utilisation du réseau de communication. Elles doivent concourir à la recherche et à la poursuite des infractions pénales.

La loi du 23 janvier 2006, précisée par un **décret du 24 mars 2006** introduite dans le CPCE prévoit qu' « 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 »

La loi oblige tous les fournisseurs d'accès, quels qu'ils soient proposant un accès Internet à **conserver les données de connexion de leurs utilisateurs pendant un an**, et à tenir celles-ci à la disposition des services de police ou de la gendarmerie nationale en cas de nécessité. Seules les personnes habilitées pourront demander la communication de ces données : autorités judiciaires en cas de réquisition par exemple.

La CNIL considère néanmoins que **les entreprises et les administrations** qui fournissent un accès Internet à leurs seuls employés ou agents ne se retrouvent pas concernées par l'obligation de conservation. Cependant, un employeur peut mettre en place un dispositif de surveillance quant à l'activité de ses salariés dès que certaines garanties sont respectées, telles que l'information des intéressés quant à la mise en œuvre du système et la déclaration du dispositif auprès de la CNIL.

Quelles sont les informations à conserver ?

Seules les **informations techniques** c'est-à-dire qu'il ne s'agit pas du contenu des communications échangées ou des informations consultées doivent être conservées. Leur périmètre est défini strictement. Il s'agit :

- Des informations quant à **l'identification de l'utilisateur** (ex : adresses IP) ;
- Des informations quant **aux équipements terminaux de communication** utilisés ;
- De la date, l'heure et la durée de chaque communication** ;
- Des services complémentaires utilisés ou demandés ainsi que leurs fournisseurs** ;
- Des informations identifiant le ou les destinataires de la communication (spécialement pour les activités de téléphonie)** ;
- Des données identifiant **l'origine et la localisation de la communication**.

Une durée fixe d'un an est assignée à la conservation de ces données relatives au trafic et ce lorsqu'il s'agit de la recherche, de la constatation et de la poursuite des infractions. Cette durée ne peut être réduite et court dès l'enregistrement des données.

A noter : des contrôles sont régulièrement effectués par la Commission Nationale de Contrôle des Interceptions de Sécurité quant aux opérations de communications techniques. En cas de non respect de ces dispositions l'opérateur Wifi peut encourir jusqu'à 5 ans d'emprisonnement et 300 000 Euros d'amende.

Quid de la sécurité des réseaux et installations

Pour **la sécurité des réseaux et installations**, les opérateurs ont également la possibilité de conserver :

- Les données permettant d'identifier l'origine de la communication ;
- Les caractéristiques techniques ainsi que la date, l'heure et la durée de chaque communication ;
- Les données à caractère technique permettant d'identifier le ou les destinataires de la communication ;
- Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs.

Pour ce qui est de la durée de conservation de ces données, elle est laissée à la discrétion des opérateurs en fonction de leurs besoins, mais elle ne peut être définitive et **ne peut excéder 3 mois**.

Doit-on créer un fichier nominatif ?

Les opérateurs Wifi ne sont nullement obligés de relever et de conserver l'identité des utilisateurs désireux de se connecter et par là même de créer un fichier nominatif. Si l'opérateur décide de ne conserver que **les seules données techniques** de connexion, il n'a **aucune obligation déclarative auprès de la CNIL**. En revanche, **s'il fait le choix de procéder à l'identification préalable des utilisateurs**, en leur faisant remplir une fiche d'inscription par exemple, il est soumis à une **déclaration normale auprès de la CNIL**.

Quels sont les risques à contrer ?

- Téléchargements illégaux, en relation avec l'HADOPI ;
- Activité pédophile ;
- Propos diffamatoires, xénophobes ... ;
- Piratages.

Par Sandra Lys, juriste stagiaire AEC