Mise en place de points d'accès public à internet - informations et conseils juridiques

Si le déploiement d'un réseau Wi-Fi est techniquement complexe, il est également juridiquement exigeant.

Mairie, médiathèque, musée, etc., vous pouvez souhaiter mettre en place un réseau Wi-Fi (wireless fidelity, fidélité sans fil) pour vos usagers. Répondant à des principes d'ingénieries télécoms et informatiques particulières, les conditions de son déploiement imposent des compétences techniques en architecture de réseaux sans fil.

Le déploiement d'un réseau Wi-Fi public nécessite de respecter certaines exigences juridiques. Il s'agit de savoir si cela vous identifie comme opérateur télécoms. Ensuite, toute connexion au réseau Wi-Fi nécessite, préalablement, de respecter plusieurs principes, jusqu'aux seuils d'exposition régis notamment par la loi 2015-136 (die loi Abeille). Enfin, il existe différentes contraintes légales quant aux données liées aux utilisateurs et à leurs connexions au réseau Wi-Fi. Ne pas respecter toutes ses exigences peut engager directement la responsabilité de toute personne exploitant un réseau Wi-Fi interne ouvert au public.

I- OPÉRATEUR... OU PAS OPÉRATEUR ?

1- La qualité d'opérateur

Selon le ***Code des postes et communications électroniques*** (CPCE, art. L. 32 , 15°), **un opérateur est une « *personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques.* »**

Le même code précise que « *L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques* » nécessitent « *une déclaration préalable auprès de* » l'Arcep (CPCE, art. L. 33-1, I). Toutefois, **l'alinéa suivant libère les exploitants de « *réseaux internes ouverts au public* » de toute obligation de déclaration** auprès de l'Arcep.

2- L'absence de déclaration Arcep

Le déploiement d'**un réseau Wi-Fi localisé à un bâtiment ou une zone réduite** rentre dans cette qualification de « ***réseau interne ouvert au public*** ». Ceci concerne toute structure : *mairies, écoles, médiathèques, cybercafés, immeubles de bureaux, hôtels, etc.* Ils **peuvent implanter et mettre à disposition d'un public un réseau Wi-Fi sans avoir à faire une quelconque « *déclaration préalable* »**. Le mode d'accès au réseau (filaire ou hertzien) autant que le nombre de personnes pouvant se connecter n'a pas d'influence tant que le réseau est et reste localisé. Il faut uniquement que ce public soit restreint et que, en cas de réseau Wi-Fi, les distances d'émissions des ondes ne dépassent pas excessivement les limites de propriété en ce que le réseau doit rester interne.

II- LE RÉSEAU WI-FI, CONDITIONS TECHNIQUES ET CONSIDÉRATIONS JURIDIQUES

Localisé, le réseau Wi-Fi ne peut être implanté qu'en tenant compte de différents éléments techniques (***A***), ce qui permet de le sécuriser partiellement face à ces utilisateurs (***B***).

A- Éléments techniques liés à l'implantation du réseau Wi-Fi

La protection d'un réseau Wi-Fi se pense en termes d'architecture réseau (***1***), de sécurisation logique du réseau (***2***), de blocages d'accès (***3***) et de limitation des seuils d'exposition (***4***).

1. *Architecturer le réseau Wi-Fi*

On ne fait pas ce que l'on veut en matière d'architecture de réseau de communications électroniques. **L'implantation d'un réseau Wi-Fi**, où qu'il se trouve, nécessite d'être pensée. En outre, plus l'endroit concerné sera étendu plus la configuration sera complexe est exigeante. Dès lors, faire appel à un prestataire compétent permettra des gains de temps et des économies d'échelle.

L'idée d'un « *réseau* » implique l'implantation de plusieurs équipements de différents niveaux interdépendants :

*** *hardwares*** : bornes Wi-Fi, antennes, centrale informatique, serveurs, etc. ;

* ***software*** : logiciels de gestion informatique, proxy, pare-feu, gestion de données, etc.

Outre le fait de disposer des bons équipements, il est nécessaire d'implanter au mieux les hotspots (bornes) Wi-Fi pour :

* ***limiter*** le nombre à acheter ;

* ***éviter*** de surcharger le réseau ;

* ***limiter*** les expositions aux ondes hertziennes Wi-Fi.

La loi obligeant à conserver certaines données, il s'agira également de **tenir compte des volumes de données à stocker**, de leurs périodes de péremption et de leurs sécurisations (cf. *partie II-A*).

La sécurisation physique du matériel n'ait pas à négliger. Outre les risques liés aux vols, il faut **empêcher tout accès non autorisé au réseau**. Ceci concerne avant tout les serveurs centraux, lesquels contiennent des données, notamment personnelles.

Dans le choix de la solution il faudra également prévoir une centralisation du paramétrage afin d'éviter des charges de maintenance excessive et rendant l'installation indépendante de l'étendue de la zone à couvrir.

2. *Sécurisation logique du réseau Wi-Fi*

Selon l' article 323-1 du Code pénal , « ***Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni*** *(…).* »

Sans préciser le mode d'accès (physique ou logique), cet article s'avère très large. Il fait appel aux articles 226-17 du même code et 34 de la loi informatique et libertés (cf. *partie III-A-2*).

En dehors de la loi, c'est un réflexe de bon sens que de protéger son matériel informatique pour se prémunir des intrusions, frauduleuses ou non. Les risques d'aspirations de données sont une réalité mais il en est une autre, celles liée aux accès et utilisations malveillantes du réseau Wi-Fi. Il paraît ainsi préférable de sécuriser le réseau pour éviter tout accès risqué, ceci se faisant via des accès par identifiants (cf. *partie II-B*). Les restrictions d'accès sont une meilleure garantie à la protection logique du réseau. Ceci permet également de se prémunir contre les fraudes électroniques, les risques liés au terrorisme, les pratiques illicites sur internet (pédophilie, xénophobie, apologie, diffamation, piratage, etc.), le tout en conformité à la loi Hadopi.

Enfin, l'ANSSI a publié des « *Recommandations de sécurité relatives aux réseaux WiFi* ».

3. *Blocage d'accès*

Si certains des risques cités ci-dessus paraissent plus théoriques que réalistes, l'on ne peut être sûr de rien. En effet, **le comportement de chaque utilisateur du réseau Wi-Fi interne ne peut être contrôlé**. Par exemple, peut-on empêcher un utilisateur d'accomplir des actes de téléchargements illégaux sachant que c'est la responsabilité de l'opérateur local qui sera engagée ?

Il paraît préférable de bloquer l'accès de certains sites internet présentant un risque quelconque pour l'opérateur. Raisonnablement, un blocage ciblé est permis face, par exemple, à des sites de partage de fichiers, de téléchargement illégal et/ou à caractère pornographique, xénophobe ou incitant au terrorisme.

Pour mettre en place ces blocages ciblés, il faut en informer les utilisateurs du réseau. Cette information se fera par une note d'information qui s'affichera en lieu et place du site bloqué. Elle doit également se faire de manière préalable en étant stipulée dans la « ***Charte d'utilisation du réseau Wi-Fi*** » (cf. *partie II-B-2*).

4. *Limitation des seuils d'exposition*

Même s'il s'agit également d'une question polémique, la nocivité des émissions d'ondes électromagnétiques ne doit pas être négligée. Les seuils d'exposition tolérés ont diminués au fil des polémiques et des années. Toutefois certains lieux accueillants du publics sont régis par la loi notamment ceux accueillant des jeunes enfants.

Pour optimiser la captation de signaux des *hotspots Wi-Fi*, il faut les positionner au mieux sur l'espace interne à desservir. Dès lors, l'aide d'un prestataire pour architecturer l'emplacement des bornes n'est pas dénuée du sens. Dans plusieurs crèches et écoles maternelles, des parents ont fait les émissions d'ondes Wi-Fi sous prétexte de principe de précaution au profit de la santé de leurs enfants.

L' OMS a institué des seuils d'exposition , lesquelles doivent être respectés. Concernant la France, les seuils nationaux peuvent être plus restrictifs !

L'association Robins des Toits met à disposition un dossier très complet concernant les dangers du Wi-Fi .

La **loi n° 2015-136 du 9 février 2015** *(dite loi Abeille du nom de la député EEPV Laurence Abeille)* **relative à la sobriété, à la transparence, à l'information et à la concertation en matière d'exposition aux ondes électromagnétiques à l'Article 7** prévoit notamment l'interdiction de l'installation du WiFi en crèches et garderies (mais pas en maternelles) et la désactivation des dispositifs WiFi en primaire en dehors des activités pédagogiques les impliquant. Elle prévoit également de l'information et de la prévention avec l'obligation de signaler par un pictogramme l'existence d'un accès WiFi dans les établissements scolaires.

B- La sécurisation juridique face aux utilisateurs du réseau Wi-Fi

La sécurisation du Wi-Fi n'est pas liée qu'aux risques d'introductions malveillantes, à la loi et aux ondes électromagnétiques. Elle concerne directement les utilisateurs du réseau interne lui-même. Il paraît préférable d'en restreindre les possibilités d'accès (***1***) et de mettre en place une « *Charte d'utilisation du réseau Wi-Fi* » (***2***).

1. *Les restrictions d'accès au réseau Wi-Fi*

Même si cela ne constitue pas une réelle obligation légale, il paraît préférable de restreindre les possibilités d'accès au réseau Wi-Fi en tant que tel. Ainsi, **mettre en place des codes d'accès ou obliger l'utilisateur à s'identifier préalablement** s'avère être une bonne alternative. Cela permet de limiter les risques d'accès frauduleux et de satisfaire à la protection face aux actes non autorisés sur internet : pédopornographie, diffamation, piratage, actes terroristes, etc.

Allant plus loin pour mieux sécuriser et restreindre, on peut imiter la durée de vie de chacun des codes d'accès.

Attention, **la mise en place de codes d'accès conduit inévitablement à la collecte de données à caractère personnelle**. Il faut donc se soumettre à toutes les dispositions de la loi informatique et libertés (cf. *partie III*) : déclaration Cnil, information préalable des utilisateurs, sécurisation des données, effacement, etc.

2. *La mise en place d'une "Charte d'utilisation du réseau Wi-Fi"*

Face aux utilisateurs du réseau Wi-Fi, une bibliothèque, un cybercafé, un musée ou un camping peu mettre en place une « législation de proximité » destinée à encadrer les droits et devoirs de ses utilisateurs. Ce cadrage s'accompli par un document de valeur contractuelle accepté par tout utilisateur du réseau interne. En général dénommé « ***Charte d'utilisation du réseau Wi-Fi*** », il s'agit, pour l'opérateur local, de proposer une convention qui lui permettra de stipuler des réserves de responsabilité face à l'utilisation de son réseau. Cette charte est comparable aux conditions générales d'utilisation (CGU) de tout site ou service internet.

Ainsi, **la Charte d'utilisation du réseau Wi-Fi est un document essentiellement destiné à protéger l'opérateur** face aux utilisations de son réseau par ses clients. Mais pourquoi ? Tout simplement parce que, malgré l'installation de restriction d'accès (codes d'indentification et blocage de sites), on ne peut jamais contrôler le comportement des utilisateurs. **La charte doit stipuler que l'utilisateur n'a pas le droit d'accomplir telle ou telle action ; s'il le fait, il engage directement sa responsabilité !**

Mais la charte doit être acceptée préalablement à l'utilisation effective du réseau. Cette acceptation doit donc avoir lieu dès la première connexion au réseau interne. Cela s'opère à condition que l'utilisateur coche une case indiquant « ***J'accepte la Charte d'utilisation du réseau Wi-Fi.*** » **Cette case doit obligatoirement être un *opt-in***, c'est-à-dire qu'elle ne doit pas être précochée par défaut. **C'est l'utilisateur qui doit volontairement, indépendamment et explicitement cocher cette case d'*opt-in***.

Les différentes stipulations de la charte doivent être adaptées à l'opérateur qui met à disposition le Wi-Fi interne et à ses modes de fonctionnement. Entre autre, peuvent être stipulées l'acceptation de la charte elle-même, les restrictions d'utilisation, les actes interdits et le fait que certaines données à caractère personnel des utilisateurs peuvent être collectées et conservées.

Enfin, il ne faut pas oublier d'**insérer des mentions légale**s au sein de la Charte (Code de la consommation, art. L. 111-2 ; loi CEN, art. 6-III). Vous pouvez trouver une matrice pour mentions légales librement disponible sur le site de l'association AEC.

III- QUANT AUX DONNÉES LIÉES AUX CONNEXIONS WI-FI

Une donnée est le conteneur d'une information, elle est destinée à apporter un renseignement.

Lors de tout accès à internet via un Wi-Fi quelconque, des opérations de collectes, de transferts et d'échanges de données ont lieu. Cela oblige à conserver certaines données (***A***). Lorsqu'il s'agit de données à caractère personnel, les opérations de collecte et de traitement doivent suivre certaines obligations légales (***B***).

A- Collecte et conservation de données

L' article 9 du Code civil énonce que « ***Chacun a droit au respect de sa vie privée.*** » Suivant cette disposition d'ordre public, le Code des postes et des communications électroniques énonce en son article L. 34-1 toutes les **règles juridiques liées aux opérations de collecte et de conservation de données** auxquelles doivent se conformer « *Les personnes qui (…) offrent au public une connexion (…) réseau, y compris à titre gratuit,* » (II, al. 3). Ainsi, ces personnes peuvent « ***conserver certaines données en vue d'assurer la sécurité de leurs réseaux.*** » (IV, in fine).

Certains lieux sont soumis à cette obligation de conservation de données s'ils mettent en place un réseau Wi-Fi interne ouvert à leur clientèle. Il s'agit donc de savoir quelles données sont concernées (***1***), dans quelles conditions elles doivent être conservées (***2***), sans omettre la situation particulières des salariés (***3***) qui peuvent également avoir accès au réseau hertzien interne local.

1. *Les données soumises à conservation*

Il n'est pas nécessaire de conserver tous les types de données. Le Code des postes et communications électroniques liste qu'elles données sont obligatoirement soumises à conservation.

Les articles R. 10-13 et R. 10-14 , IV dudit Code énonce qu'il faut **conserver des données dites de « trafic »** ; c'est-à-dire, en application du l' article R. 10-12 du CPCE , des « *informations (…) susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques (…) et qui sont pertinentes au regard des finalités poursuivies par la loi.* » Les deux articles suivants permettent d'identifier de telles informations.

Ces données de trafic concernent :

* **Art. R. 10-13** , **pour « *les besoins de la recherche, de la constatation et de la poursuite des infractions pénales* »** : « a) *Les informations permettant d'identifier l'utilisateur ;* b) *Les données relatives aux équipements terminaux de communication utilisés ;* c) *Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;* d) *Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;* e) *Les données permettant d'identifier le ou les destinataires de la communication.* »

* **Art. R. 10-14 , IV**, **« *Pour la sécurité des réseaux et des installations* »** :« a) *Les données permettant d'identifier l'origine de la communication ;* b) *Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;* c) *Les données à caractère technique permettant d'identifier le ou les destinataires de la communication ;* d) *Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs.* »

Si l'on constate que la plupart des informations à conserver ont un caractère technique (caractéristiques des terminaux informatiques utilisés, volumétries des communications, connexions aux services), certaines concernent l'identification des utilisateurs. Mais, **qui dit collecte de données d'identification d'une personne physique** – ici l'utilisateur d'un réseau Wi-Fi interne – **dit collecte de données personnelles !** D'ailleurs, cette partie réglementaire du Code des postes et des communications électroniques concerne la protection de la vie privée des personnes.

Pour rappel, **une donnée personnelle est une « *information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement* »** (loi informatique et Libertés du 6 janvier 1978, art. 2, al. 2). Face aux données de trafic à collecter et conserver, cela concerne les informations d'identification des utilisateurs, l'origine de la communication ou les caractéristiques des terminaux utilisés. Par exemple, il en ira ainsi des nom, prénom et coordonnées (adresse, mail, numéro de portable) de l'utilisateur, des identifiants numériques et informatiques de son ordinateur ou smartphone (adresses MAC et IP, numéros constructeurs, etc.), de sa géolocalisation ou encore de navigation sur internet.

Dans le respect de la vie privée des personnes et de la loi informatique et libertés, lesdits utilisateurs doivent être informés de telles opérations de collectes. Cela s'opère par l'acceptation de la charte d'utilisation du réseau Wi-Fi (cf. partie II-B).

Un problème demeure : la collecte de « *données permettant d'identifier le ou les destinataires de la communication.* » (CPCE, art. R. 10-13 , e). En effet, il y a là aussi collecte de données personnelles… mais auprès de personnes n'en étant pas préalablement informées et n'ayant pas accepté cela préalablement. On touche ici une limite à la protection de la vie privée. Cependant, ces collectes suivent des considérations d'ordre public liées à la sécurité du territoire et la protection des personnes (notamment la lutte contre le terrorisme). Une telle finalité permet de passer outre la protection de la vie privée au nom de l'intérêt général. Pour bénéficier d'un minimum de sécurité juridique, il est préférable de stipuler de telles collectes dans la charte d'utilisation du réseau Wi-Fi (cf. *partie II-B*).

Ceci ne doit surtout pas être négligé. Le non-respect de cette obligation de conservation expose les personnes morales à une amende de 375 000 € d'amende (CPCE, art. L. 39-3 ; Code pénal, art. 131-38).

2. *Les conditions de conservation des données*

À compter du jour de la collecte, l'article R. 10-13 du CPCE, III oblige à **conserver toutes ces informations pendant « *un an* »**. Sans plus de précisions, aucune période maximale ne semble exigée. Donc, au-delà de ces douze mois, la loi informatique et libertés s'applique. De manière générale, son article 6 énonce que les données personnelles collectées doivent être « *conservées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.* » C'est donc la « *finalité* » de la conservation qui prime ; au regard du CPCE, il s'agit ici « *de la recherche, de la constatation et de la poursuite des infractions pénales* ». Ainsi, si un an est le minimum légal, il semble préférable de ne pas aller au-delà de deux années.

Plus claire, l'article R. 10-14 dispose que la durée de conservation ne doit pas excéder « *trois mois* ».

Passées ces périodes, les données collectées ne peuvent être conservées que si elles ont fait l'objet d'une anonymisation (loi IL, art. 39-II, dernier al.).

Dans ses aspects techniques et numériques, la conservation des données de trafic doit être sécurisée. Outre l'utilisation de codes d'accès sécurisés, le matériel sur lesquelles elles sont conservées doit être sécurisé et protégé. Si l'opérateur interne les conserve chez lui sur un disque dur, il devra le tenir sous clé et éviter tout accès physique. Il paraît tout de même plus simple et efficace de faire appel à un prestataire hébergeur, lequel a de très fortes obligations de sécurisation physique et logique des données qu'il héberge.

3. *Quant aux salariés de l'opérateur Wi-Fi interne*

Cas à part, les salariés peuvent eux aussi être utilisateurs, à titre professionnel et/ou personnel, du réseau Wi-Fi interne à disposition.

Selon l'article L. 1222-4 du Code du travail, toute collecte d'« *information concernant personnellement un salarié (…) par un dispositif quelconque [doit être] porté préalablement à sa connaissance.* » L'indifférence face au dispositif de collecte fait que la collecte de données via réseau Wi-Fi interne est concernée. Ce porté à connaissance peut s'accomplir de différentes façons :

- par affichage et lettre d'information auprès des salariés ;

- par un avenant au contrat de travail, cet avenant devant expressément et personnellement être signé par l'employeur et chaque employé ;

- par une clause particulière au sein de tout nouveau contrat de travail établi après installation du dispositif de collecte via Wi-Fi interne.

Enfin, dans le cadre de l'article L. 2323-32, alinéa 3 du Code du travail, la « *mise en œuvre dans l'entreprise* » d'un Wi-Fi conduit à des collectes de données relatives aux employés. Cela permet à l'employeur d'exercer « *un contrôle de l'activité des salariés.* » Ceci impose d'en informer « *préalablement* » le comité d'entreprise.

B- Obligations légales face aux données collectées

Sous conditions, la loi oblige à rendre disponibles les données collectées, même si celles-ci sont des données personnelles (***1***), dans le cadre de procédures judiciaires (***2***).

1. *Face aux données personnelles*

Concernant les données personnelles, toute opération de collecte nécessite de constituer un fichier contenant de telles données. Dans le cadre de l'article 25-I de la loi informatique et libertés, ce fichier doit obligatoirement faire l'objet d'**une déclaration auprès de la Commission nationale informatique et libertés** (***Cnil***). Seul le fait d'opérer des collectes doit être déclaré. Donc, les données collectées doivent rester strictement confidentielles et ne surtout pas être déclarées, même face à la Cnil. Par dérogation prévue au III du même article, la présence d'un **Correspondant Informatique et Libertés** (***CIL***) apporte une dispense aux obligations de déclaration. En effet, le Cil est une sorte de garant des données personnel car il est « *chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la* » loi informatique et libertés.

En son article 34, cette loi oblige à « *prendre toute précautions utiles (…) pour préserver la sécurité des données et, notamment, empêcher (…) que des tiers non autorisés y aient accès.* ». Cette obligation est rappelée à l'article 226-17 du Code pénal.

Plus généralement, en lien aux dispositions pénales énoncées par la loi informatiques et libertés (art. 50 à 52), ce sont les articles 226-16 à 226-24 du Code pénal qui répriment les « mauvais » comportements face aux données à caractère personnel. À ce titre, l'article 226-16 puni « *Le fait (…) de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'ai été respectées les formalités préalables à leur mise en œuvre* ».

2. *Face aux procédures judiciaires*

Les autorités judiciaires (services de police ou de gendarmerie et tribunaux) **sont habilitées à demander et obtenir communications des données collectées**. Cette habilitation **s'étend également aux données personnelles**. Cette communication est obligatoirement demandée dans le cadre d'une

réquisition judiciaire. Elle poursuit des objectifs de lutte contre les fraudes électroniques, contre le terrorisme, contre les pratiques illicites sur internet (activités pédophiles, xénophobie, apologies, diffamation, piratages, etc.) et en conformité à la loi Hadopi.

En dehors des juridictions privées, une réquisition administrative peut être ordonnée pour communiquer les données collectées (CPCE, art. L. 34-1-1) dans un but de prévention et de lutte contre le terrorisme.

Au vu de tous les points cités plus haut et de tous les questionnements qu'ils induisent, le service informatique du SIAGEP reste à votre disposition pour tout renseignement complémentaire et conseil dans la mise en œuvre d'un tel projet.