CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DE MARTINIQUE

CONCOURS INTERNE
DE TECHNICIEN PRINCIPAL TERRITORIAL DE 2e CLASSE
SESSION 2016

Jeudi 14 avril 2016

EPREUVE D'ETUDE DE CAS

SPECIALITE : INGENIERIE, INFORMATIQUE ET SYSTEMES D'INFORMATION

ÉPREUVE D'ADMISSIBILITÉ :

Etude de cas portant sur la spécialité au titre de laquelle le candidat concourt.

Durée : 4 heures
Coefficient : 1

A LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni votre numéro de convocation, ni signature ou paraphe.
- Aucune référence (nom de collectivité, nom de personne, ...) **autre que celles figurant le cas échéant sur le sujet ou dans le dossier** ne doit apparaître dans votre copie.
- Seul l'usage d'un stylo à encre soit noire, soit bleue est autorisé (bille non effaçable, plume ou feutre). L'utilisation d'une autre couleur, pour écrire ou pour souligner, sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.
- L'utilisation d'une calculatrice de fonctionnement autonome et sans imprimante est autorisée.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 21 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

- Vous préciserez le numéro de la question et le cas échéant de la sous-question auxquelles vous répondrez.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas...

Vous êtes technicien principal territorial de 2ème classe dans la commune de Techniville, qui compte près de 50 000 habitants.

Directement rattaché au Directeur général des services, vous avez en charge la gestion des infrastructures et du parc informatique. Vous encadrez deux autres techniciens qui vous aident dans cette mission.

Afin d'apporter un service supplémentaire à ces usagers, le Maire de votre commune souhaite équiper la bibliothèque d'un réseau Wifi gratuit.

A l'aide des documents ci-joints et de vos connaissances, vous répondrez aux questions suivantes :

QUESTION N°01 (6 Points)

Décrivez la démarche de gestion de projet que vous allez adopter en identifiant les différents acteurs et leurs rôles respectifs.

QUESTION N°02 (6 Points)

Dans une note, détaillez les mesures que vous prendrez afin de garantir la conformité aux exigences juridiques, à la sécurisation du réseau et à la protection des visiteurs.

QUESTION N°03 (4 Points)

3A. Décrivez les différentes normes Wifi de façon à comparer leurs performances.

3B. Quelles sont les normes les mieux adaptées à une bibliothèque ? Justifiez.

3C. Malgré les données théoriques de portée des antennes Wifi, le réseau Wifi de la bibliothèque municipale présente de nombreuses zones non couvertes.

- ✓ Quelles peuvent en être les raisons ?
- ✓ Comment cela aurait-il pu être évité ?

QUESTION N°04 (4 Points)

Détaillez les mesures techniques que vous prendrez afin de garantir l'accessibilité et la facilité de connexion au réseau Wifi.

Liste des documents :

DOCUMENT N°01 : « Comment déployer un bon réseau Wifi pour un évènement ».
www.journaldunet.com le 27/10/14 par Virgile Juhan (2 pages).

DOCUMENT N°02 : « Les risques juridiques et économiques du Wifi gratuit ».
www.lesechos.fr le 31/01/2008 par Frédéric Salat-Baroux (1 page).

DOCUMENT N°03 : « Mise en place de points d'accès public à internet – informations et conseils juridiques ».
AEC Agence Aquitaine du numérique le 05/03/2015 par Cédric Favre. (6 pages).

DOCUMENT N°04 : « Wifi territorial ».
wifi.va-solutions.fr - 2016 (1 page).

DOCUMENT N°05 : « Wifi public urbain ».
Communauté d'Agglomération du Pays Ajaccien (2 pages).

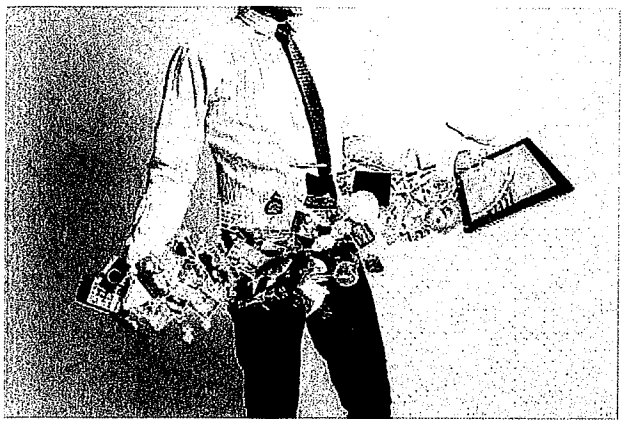
DOCUMENT N°06 : « Accès Internet en bibliothèque : ce qu'exige vraiment la loi ».
www.scinfolex.com le 26 mars 2010 par calimaq (4 pages).

DOCUMENT N°07 : « Paris Wifi : Conformité réglementaire ».
www.api-site-cdn.paris.fr (2 pages).

DOCUMENT N°01

Comment déployer un bon réseau Wifi pour un événement

www.journaldunet.com le 27/10/14 par Virgile Juhan.



Peut-on garantir de bonnes connexions Wifi lors de n'importe quel événement ? Est-ce seulement une question de norme ou de bande de fréquence ? Décryptage, avec un spécialiste.

Pour une conférence, un événement, un salon... il est appréciable de bénéficier d'un réseau Wifi robuste et performant. Mais c'est hélas bien rarement le cas ! Comment mettre en place un bon réseau Wifi, performant, aujourd'hui, à l'heure où chacun a son smartphone, parfois avec un ordinateur portable en plus, et aime tweeter un événement en direct ou regarder à tout moment la dernière vidéo qui buzze sur les réseaux sociaux ? Un contexte aussi où, techniquement, plusieurs normes Wifi cohabitent et font parler d'elles (IEEE 802.11ac ou 802.11n notamment), tout comme différentes bandes de fréquence (2,4 ou 5 GHz)... Quoi choisir, comment s'y retrouver, et qu'est-ce qu'il faut utiliser pour mettre en place un réseau Wifi efficace ?

S'adapter aux inconvénients

Premier défrichage : à chaque norme, ses avantages et inconvénients. Idem pour les deux bandes de fréquences 2,4 ou 5 GHz. Avec la bande des 5 GHz, de nombreuses interférences sont évitées, et la bande passante disponible est plus importante qu'avec celle des 2,4 Ghz. Mais elle a aussi a une portée moins grande, et tous les périphériques ne sont pas compatibles. Or, la norme IEEE 802.11ac n'utilise que la bande de fréquence des 5 Ghz.

"On préconise donc d'utiliser les deux bandes, 5 Ghz et 2,4 GHz. L'idéal, aujourd'hui, dans ce contexte, c'est que chaque point d'accès propose trois 'radios' différentes : deux en 802.11n, sur 2,4 et 5 Ghz, et une en 802.11ac sur les 5 Ghz", explique Jean-Louis Tillet, Senior Sales Business Development Manager chez Cisco. En outre, avec un bon matériel, selon ce spécialiste, une borne peut servir jusqu'à 400 appareils. Et de telles bornes peuvent être disposées tous les 10 ou 20 mètres. Après, selon la jauge (un stade, un centre de convention, ou une petite salle pour une conférence), le matériel peut différer, et le maillage aussi. Sachant qu'évidement, les utilisateurs se partagent la bande passante : dix utilisateurs simultanés sur un point d'accès à 860 Mo/s auront donc 86 Mo/s de bande passante.

La pratique plus que la théorie

Mais attention, tient tout de suite à préciser le spécialiste de Cisco, il s'agit là de chiffres très théoriques. " En général concernant les déploiements de réseau Wifi pour un événement, rien ne vaut la pratique, qui peut être bien différente de la théorie... C'est pour cela qu'un audit du lieu, en amont, est nécessaire : bien s'adapter à l'environnement est capital", martèle Jean-Louis Tillet.

"Un réseau Wifi, ce n'est pas que du réseau, mais aussi de la radio"

En outre, rappelle cet expert, lors de cet audit en amont, il faut aussi prévoir que le réseau Wifi ne se comportera pas de la même façon dans le lieu vide qu'une fois les personnes à l'intérieur. Pourquoi ? Car nous sommes faits d'eau. Or, les réseaux Wifi sont sensibles à l'eau. C'est d'ailleurs ce qui a pu poser problèmes à des entrepôts de bouteilles d'eau qui voulaient s'équiper de réseau Wifi pour leurs opérations de logistique...

Et bien d'autres interférences sont susceptibles de dégrader le réseau Wifi, qui peut aussi être affecté par la qualité de l'air, ou le Bluetooth, entre autres. C'est d'ailleurs aussi pour cela que surveiller et gérer la performance du réseau en direct, via un contrôleur dédié, peut aussi réguler les performances et améliorer la qualité du signal. "Un réseau Wifi ce n'est pas que du réseau, mais aussi de la radio", rappelle l'employé de Cisco.

Coûts et ROI d'un bon réseau Wifi

Sur le papier, cela a donc l'air simple. Peut-être cher, mais simple. A écouter l'expert de Cisco, garantir un bon wifi, même à un public très connecté, serait donc toujours possible. Mais comment se fait-il alors que sur tant d'événements, même les plus connus de l'informatique, le réseau Wifi soit si mauvais ?

"Souvent, les lieux sont équipés de vieux produits", avance l'employé de Cisco, qui donne aussi une autre piste d'explication, aussi convaincante : il n'est pas toujours précisé dans le contrat de location de la salle que lieu doit disposer d'un bon réseau Wifi... C'est aussi, évidemment, parce que déployer de bons réseaux est souvent considéré comme un trop gros investissement, sans ROI. Mais cela pourrait évoluer. "Des centres d'exposition pourraient mieux monétiser les informations recueillies par le réseau Wifi", pense par exemple Jean-Louis Tillet. Et une entreprise peut sponsoriser un réseau, et voir son nom apparaitre, sur l'événement ou sur une page de connexion. Sans oublier qu'un événement ayant un bon réseau Wifi générera sans doute un plus grand nombre de tweets ou de contenus postés en direct sur les réseaux sociaux, et bénéficiera donc d'une meilleure promotion. Des leviers de ROI qui pourraient aider des événements à déployer de meilleurs réseaux Wifi à l'avenir... Et certains en ont bien besoin.

DOCUMENT N°02

Les risques juridiques et économiques du Wi-Fi gratuit

www.lesechos.fr le 31/01/2008 par Frédéric Salat-Baroux

La volonté de certaines collectivités publiques, notamment des communes, de fournir des accès Wi-Fi gratuits à leurs administrés ou usagers de passage, si séduisante qu'elle puisse être de premier abord, pose un certain nombre de questions juridiques lourdes. Et cela tant au regard des conditions d'intervention des collectivités territoriales en matière de communications électroniques qu'en matière de concurrence.

L'intervention publique peut revêtir plusieurs formes. La première consiste à mettre à la disposition d'un opérateur de communications électroniques une partie du domaine public (jardins, places, bibliothèques...) afin que ce dernier y installe ses équipements, à partir desquels les consommateurs pourront accéder gratuitement à Internet.

Cette mise à disposition revêt la forme d'une autorisation d'occupation du domaine public, qui doit s'inscrire dans le respect des règles de concurrence. Si l'on considère les espaces publics concernés comme des facilités essentielles, au sens du droit de la concurrence, la personne publique devra offrir un accès à cette ressource, de façon ouverte et non discriminatoire, aux opérateurs en faisant la demande. Par ailleurs, le Conseil de la concurrence se réservera la faculté de vérifier la motivation d'une éventuelle exclusivité. Cette occupation se doit également d'être payante et tenir compte des avantages procurés au titulaire de l'autorisation (1). En tout état de cause, le choix du ou des opérateurs doit s'accompagner d'une procédure de publicité. Ce premier mode d'intervention permet à tous les opérateurs qui le souhaitent d'offrir un service supplémentaire à leurs abonnés, et ce, sans ajouter un autre coût pour l'utilisateur final.

Fracture numérique

La collectivité peut également vouloir, comme c'est le cas avec le Wi-Fi gratuit, financer intégralement le service rendu, en proposant des offres apparemment gratuites aux consommateurs. Or la compétence des collectivités territoriales en matière de communications électroniques est fixée par l'article L 1425-1 du Code général des collectivités territoriales. Cet article pose des principes généraux d'objectivité, de transparence, de non-discrimination et de proportionnalité de leur intervention. Surtout, la collectivité qui souhaite fournir le service aux consommateurs, doit, avant de lancer son projet, faire la preuve d'une insuffisance d'initiative privée (2) de la part des opérateurs. En effet, le législateur a entendu limiter l'autorisation d'intervention des collectivités territoriales en ce domaine à ce seul cas. Les travaux parlementaires montrent qu'il s'agissait ainsi d'agir pour résorber la fracture numérique, pallier l'absence d'opérateurs privés dans certaines zones, essentiellement rurales, sans pour autant *« fausser le jeu de la concurrence, à la fois entre le secteur privé et le secteur public et entre les opérateurs privés ».*

En détournant l'article L 1425-1 de son objet, et faute de respecter la condition de l'insuffisance d'initiative privée, l'intervention de la collectivité devrait être regardée par les tribunaux comme privée de base légale. C'est notamment la raison pour laquelle, dans un souci d'éviter des distorsions de concurrence, la Commission européenne a récemment demandé à la municipalité de Prague de modifier son projet de réseau sans fil, qui devait permettre de fournir au public un accès gratuit à Internet.

Au-delà de la légalité très contestable des procédures d'installation de Wi-Fi gratuit, c'est l'équilibre économique de ce marché qui risque de se trouver fragilisé. En effet, le choix par les collectivités locales de fournir des accès gratuits peut avoir pour conséquence de détourner une partie de la clientèle des opérateurs dès lors que les consommateurs seront tentés de résilier leur abonnement payant, pour profiter de la gratuité du service offerte par le débordement naturel des ondes Wi-Fi au delà des espaces publics. Le risque existe alors d'empêcher le libre jeu de la concurrence entre les opérateurs. Et, comme toujours, quand la libre concurrence est contrariée, c'est l'innovation qui en pâtit et, à l'arrivée, le service aux usagers.

Ces risques sont d'autant plus inutiles que les opérateurs sont prêts à offrir ce service à leurs clients et que, s'agissant du Wi-Fi gratuit des communes, ce service a néanmoins un coût. Si le Wi-Fi est gratuit pour l'usager, il ne l'est pas pour le contribuable.

(1) Art 2125-1 et suivant du Code général de la propriété des personnes publiques. (2) Art L 1425-1 alinéa 2 « Dans les mêmes conditions qu'à l'alinéa précédent, les collectivités territoriales et leurs groupements ne peuvent fournir des services de communications électroniques aux utilisateurs finals qu'après avoir constaté une insuffisance d'initiatives privées propres à satisfaire les besoins des utilisateurs finals et en avoir informé l'Autorité de régulation des communications électroniques. Les interventions des collectivités s'effectuent dans les conditions objectives, transparentes, non discriminatoires et proportionnées. L'insuffisance d'initiatives privées est constatée par un appel d'offres déclaré infructueux ayant visé à satisfaire les besoins concernés des utilisateurs finals en services de communications électroniques. » (*) Avocat à la cour, Weil, Gotshal & Manges.

DOCUMENT N°03

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

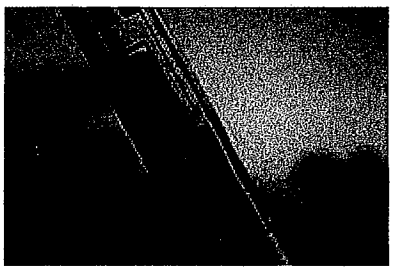
AEC Agence Aquitaine du numérique le 05/03/2015 par Cédric Favre

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

Cybercafé, bibliothèque, musée, camping, etc., tout professionnel du secteur culturel peut souhaiter mettre en place un réseau Wi-Fi (wireless fidelity, fidélité sans fil) pour sa clientèle. 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 le professionnel du tourisme est ou non identifié en tant qu'opérateur télécoms (***I***). Ensuite, toute connexion au réseau Wi-Fi nécessite, préalablement, de respecter plusieurs principes (***II***). Enfin, il existe différentes contraintes légales quant aux données liées aux utilisateurs et à leurs connexions au réseau Wi-Fi (***III***). 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 : ***cybercafés, immeubles de bureaux, hôtels, bibliothèques, 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 connecté 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

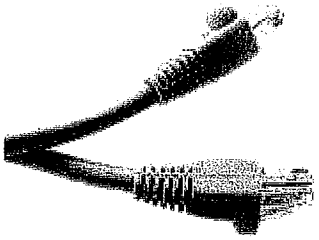
Localisé, le réseau Wi-Fi ne peut être implanté qu'en tenant compte de différents éléments techniques (***A***), ce qui permet de le sécuriser partiellement face à ces utilisateurs (***B***).

A- Eléments 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 étalé malgré sa localisation, par exemple un musée ou un camping, 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.



câbles de connexion

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

* ***hardwares*** : hotspots, antennes, centrale informatique, mitigeurs, serveurs, etc. ;
* ***software*** : logiciels de gestion informatique, pare-feu, gestion de données, etc.

Outre le fait de disposer des bons équipements, il est nécessaire d'implanter au mieux les hotspots 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.

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 interne. Commercialement parlant, il n'est pas envisageable de bloquer un grand nombre de sites. Raisonnablement, un blocage ciblé est permis face, par exemple, à des sites de partage de fichiers, de téléchargement illégal et/ou à caractère pornographique.

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. **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 .

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 interne** (bibliothèque, musée, camping, etc.) 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*.**

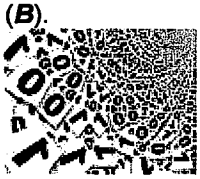
Les différentes stipulations de la charte doivent être adaptées à l'opérateur qui met à disposition le Wi-Fi interne et à ses modes de fonctionnement. Entre autre, peuvent être stipulées l'acceptation de la charte elle-même, les restrictions d'utilisation, les actes interdits et le fait que certaines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

Enfin, il ne faut pas oublier d'**insérer des mentions légales** 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 , elle est 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 CPCE 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).

Un hôtel, une bibliothèque ou un musée sont notamment 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 CPCE 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 IL, 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*

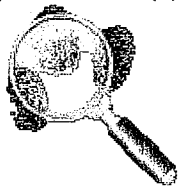
Cas à part, les salariés peuvent eux aussi être utilisateurs, à titre professionnel et/ou personnel, du réseau Wi-Fi interne à disposition.

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 a 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.

DOCUMENT N°04

Wifi Territorial

wifi.va-solutions.fr – 2016.

Une zone wifi étendue avec, pour l'usager et les gestionnaires, une facilité d'accès et d'utilisation déconcertante.

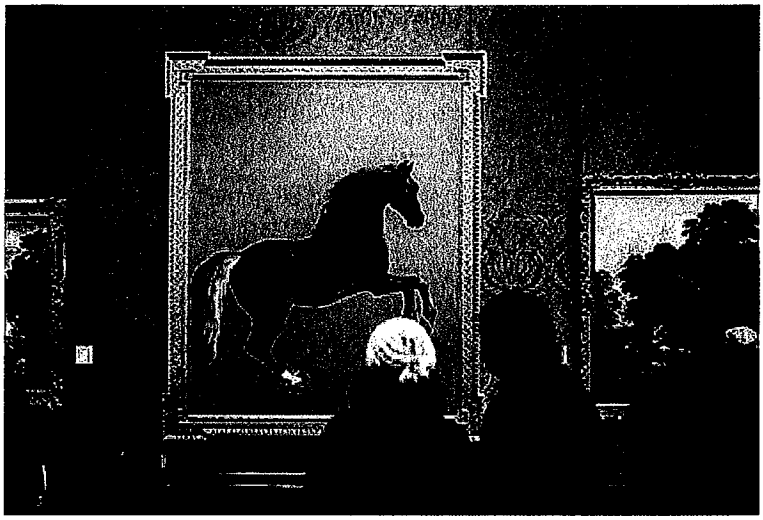
Le WiFi territorial vous permettra d'homogénéiser la communication à l'échelle régionale, voire nationale.

Optez pour une stratégie de communication cohérente où les statistiques récoltées vous permettront d'améliorer et d'adapter au mieux vos futures offres.

6 Français sur 10 partent en vacances avec un ordinateur ou un Smartphone pour surfer sur internet ou envoyer des e-mails et les touristes utilisent de plus en plus leurs tablettes à l'extérieur.

L'utilisateur, en plus de bénéficier d'un service simple et performant, bénéficiera d'une relation privilégiée avec les acteurs du territoire.

Une seule authentification utilisateur sur tout un territoire grâce à un maillage Hot-spots efficace.



Les étapes de la mise en place d'un WiFi territorial :

1. Repérage des zones touristiques,
2. Installation de Hot-spots intérieurs ou extérieurs,
3. Déploiement de l'équipement urbain et phase de test,
4. Communication (de ce service gratuit) auprès des touristes et des adhérents,
5. Optimisation de la solution.

Un processus simple, unique et automatique partout.

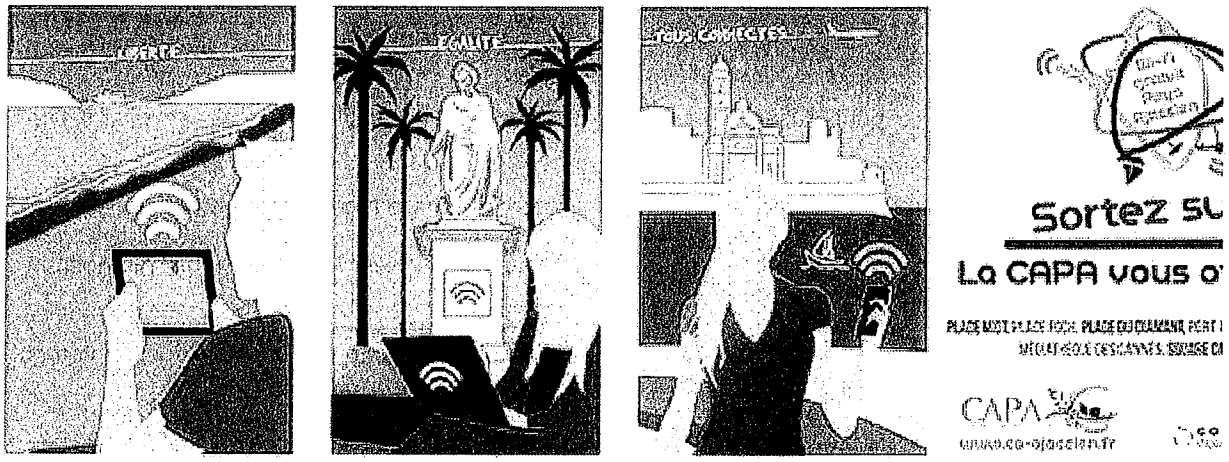
Faites profiter de cette possibilité à vos clients.

Un outil de statistique performant

Une solution parfaitement adaptée aux offices de tourisme !

- Une simplification d'accès au WiFi pour les usagers.
- Pas de redondance d'identification,
- Pour les offices : un réseau unifié, un gain de temps, une gestion réduite et un territoire couvert.
- Une première connexion sur un site adéquat
- Déplacez-vous où vous le souhaitez
- Vos appareils se reconnaitront automatiquement aux sites WiFi disponibles

DOCUMENT N°05

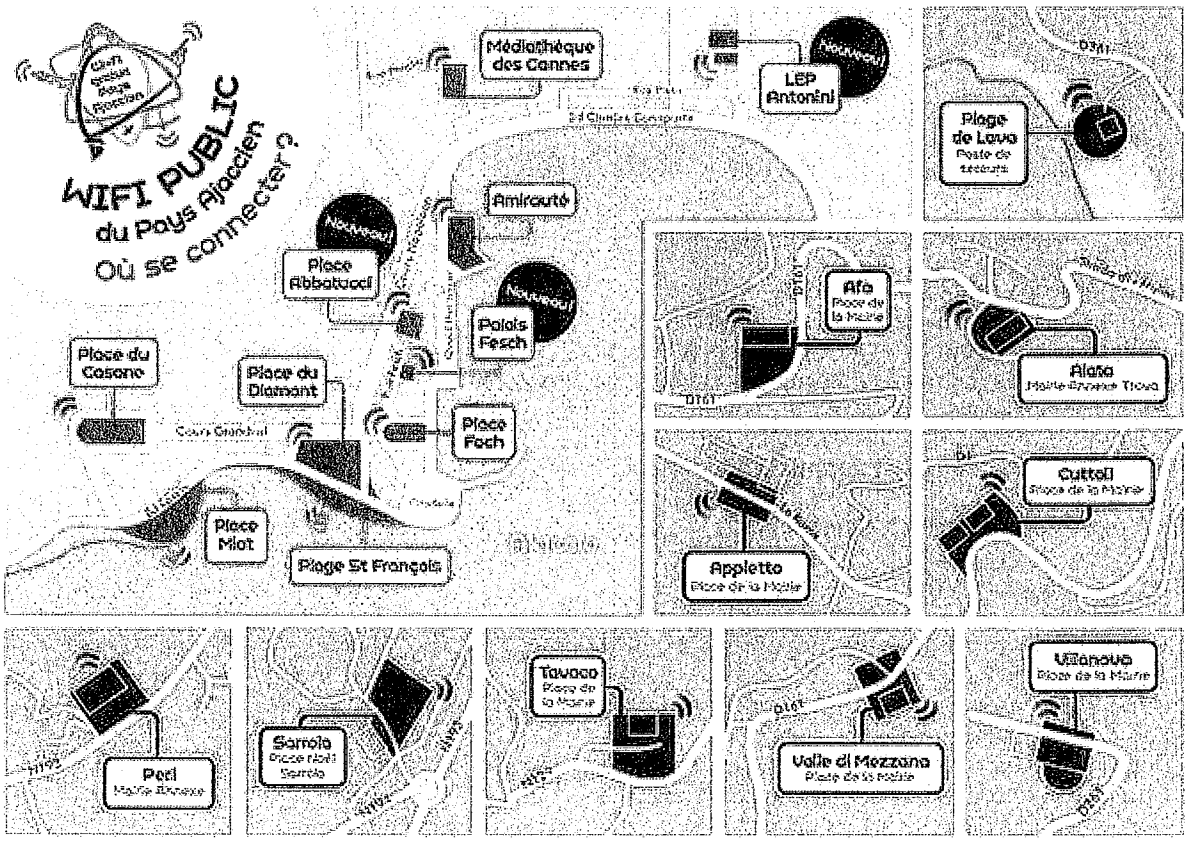


Wifi public urbain

Communauté d'Agglomération du Pays Ajaccien

La Communauté d'Agglomération du Pays Ajaccien offre à ses habitants, aux visiteurs et aux touristes, un service gratuit de wifi public. Accessible facilement sur smartphone, tablette ou ordinateur portable, la connexion est proposée sur huit sites du territoire et en cours d'extension aux neuf autres communes de la CAPA.

Le Wi-Fi public du Pays Ajaccien est un service mis en place par la Communauté d'agglomération du Pays Ajaccien (CAPA) dans le cadre de sa stratégie « Territoire Numérique ». Depuis le 18 juin 2013, cette réalisation sans précédent sur le territoire insulaire, permet aux habitants, visiteurs ou touristes de se connecter gratuitement, sans fil et en haut débit, à Internet.



Accompagner le développement du numérique mobile

Avec cette initiative la CAPA innove en répondant aux enjeux de réduction de la fracture numérique et aux besoins de mobilité de chacun. En cours d'extension dans les coeurs des 9 villages de la communauté d'agglomération, la connexion à Internet gratuite est possible à AJaccio sur la Place Miot, la Place Foch, la Place du Diamant, le Port de l'Amirauté, la Place du Casone, la Médiathèque des Cannes, le LEP Jules Antonini.

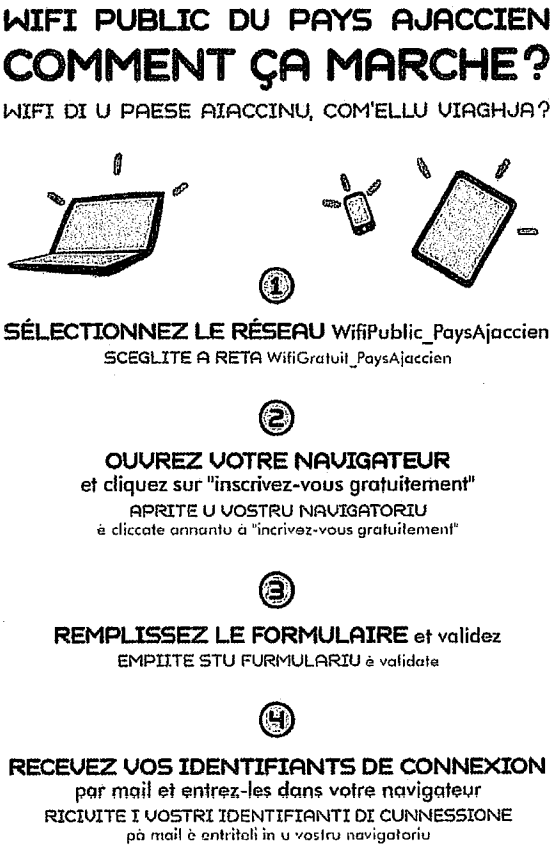
La CAPA dispose également d'une solution wifi mobile pour apporter sa technologie dans des zones non couvertes par l'infrastructure fixe.

Deux objectifs distincts sont poursuivis avec le déploiement de ce Wifi public :

- Offrir un nouveau service aux usagers
- Réduire la fracture numérique et permettre à tous d'accéder à internet
- Rendre la ville intelligente et améliorer l'information des habitants et des touristes

Surf en toute liberté

Lors de sa première connexion, l'usager devra créer un compte personnel selon une procédure simple et classique. Il pourra ensuite surfer pour accéderen plein air, au web, aux vidéos, aux mails...



Intégration réussie dans le paysage

De taille réduite (20 cm sur 10), les antennes ont été installées autour des sites. Des mesures de rayonnement électromagnétique réalisées à la demande de la CAPA par un bureau d'étude agréé par l'A.N.F.R. (Agence Nationale des Fréquences), ont donné des résultats d'émission maximale largement inférieurs aux normes nationales d'exposition au public.

DOCUMENT N°06

Accès Internet en bibliothèque : ce qu'exige vraiment la loi

www.scinfolex.com le 26 mars 2010 par calimaq

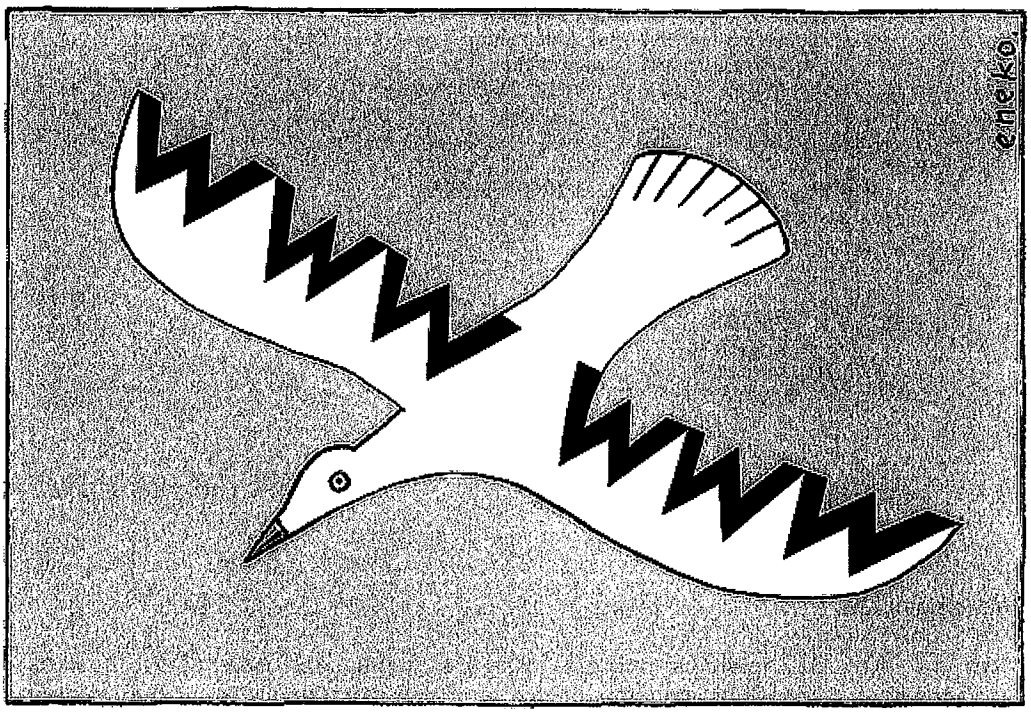
L'IABD (Interassociation Archives Bibliothèques Documentation) publie aujourd'hui une mise au point, concernant la teneur et l'étendue des obligations légales qui pèsent sur les services d'archives, de bibliothèques et de documentation lorsqu'ils offrent sur place des accès Internet à leurs usagers. L'information a été relayée sur Bibliobsession, Paralipomènes et sur le site de l'ADBS.

Le sujet est complexe et sensible, car il confronte les professionnels de l'information à un choix difficile. Donner accès à Internet constitue aujourd'hui pour les services d'archives, de bibliothèques et de documentation un aspect essentiel de leurs missions ; mais leur responsabilité est susceptible, à divers degrés, d'être engagée du fait d'agissements délictueux qui seraient commis à partir de ces connexions par leurs usagers.

Entre la liberté de l'usager et la responsabilité de l'établissement, il faut trouver un équilibre, qui est d'autant plus difficile à déterminer que les textes applicables sont nombreux (Code des postes et communications électroniques, loi LCEN de 2004, loi anti-terroriste de 2006, loi Hadopi de 2009, etc.) et leurs dispositions délicates à interpréter. Demander aux utilisateurs de s'identifier lorsqu'ils se connectent à Internet ; mettre en place des filtres pour bloquer l'accès à certains sites ; neutraliser certaines fonctionnalités comme le téléchargement ou l'usage des clés USB : autant de pratiques qui ont cours dans nos établissements, sans que l'on sache si elles sont réellement exigées par les textes de loi.

La question est d'autant plus importante que depuis l'été 2009, l'accès à Internet n'est pas seulement un service rendu à l'usager, mais l'exercice d'une liberté fondamentale, explicitement consacrée par le Conseil constitutionnel à l'occasion de sa censure de la première loi Hadopi :

« [...] aux termes de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 : « La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi » ; qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services. »



Fragile, si fragile... la liberté d'accès à Internet. (En defensa de internet.
Par tonymadrid photography. CC-BY-NC-ND. Source : Flickr)

Il peut être tentant pour les bibliothèques, archives et centres de documentation de mettre en place des mécanismes de contrôle qui leur permettront de limiter les risques de voir leur responsabilité engagée. Mais il faut bien avoir conscience que si ces dispositifs vont au-delà de ce que la loi exige, ils auront pour effet de restreindre volontairement l'exercice d'une liberté fondamentale des citoyens, garantie par la Constitution.

La mise au point de l'IABD passe en revue les textes pour délimiter avec précision le champ de ces obligations légales. Il ressort de l'analyse que si les bibliothèques, archives et centres de documentation sont bien obligés de conserver pendant un an les données de connexion (loi anti-terroriste de 2006), **il n'est nullement exigé, ni de recueillir l'identité des personnes qui accèdent à Internet, ni de mettre en place a priori des moyens de sécurisation des connexions tels que des systèmes de filtrage.**

Les textes préservent donc le droit des usagers à utiliser Internet librement, sans avoir à donner leur identité et à conserver leur anonymat lors de leur usage des connexions.

L'accès public à Internet est une liberté protégée, mais hélas menacée. Lors du débat de la loi Hadopi, il avait été un temps proposé par le ministère de la Culture de mettre en place un « portail blanc » pour brider les accès publics wifi et les restreindre à une liste prédéterminée de sites « propres ». Un tel système aurait pu être appliqué dans les parcs ou les mairies, mais aussi dans les bibliothèques et autres services similaires offrant des accès wifi à leurs usagers. Face à cette menace d'atteinte à la liberté d'accès à l'information, l'IABD avait déjà réagi par le biais d'une déclaration. Le projet de portail blanc a finalement été abandonné lors de l'examen au Parlement de la loi, mais j'ai eu l'occasion d'essayer de montrer dans un billet précédent comment la loi Hadopi était susceptible d'aggraver la responsabilité pesant sur les bibliothèques du fait de l'usage des connexions Internet qu'elles offrent à leurs usagers.

Lors du dernier congrès de l'ABF, un atelier avait été organisé sur le thème « L'autonomie de l'usager versus la responsabilité du bibliothécaire » auquel j'avais participé. Il en était ressorti qu'au-delà de la question légale, les modalités de l'accès à Internet relèvent d'un choix professionnel qui revêt une forte dimension éthique. Pour que la liberté de l'usager puisse exister, le bibliothécaire doit nécessairement accepter d'assumer une part incompressible de responsabilité.

Aux Etats-Unis, les bibliothécaires ont subi (et subissent encore) les conséquences du Patriot Act, qui les obligent à communiquer aux autorités des données personnelles sensibles de leurs usagers.

Il n'y a pas (encore) de Patriot Act en France, mais bien souvent, il reste plus facile de se connecter à Internet depuis un Mac Do qu'à partir de la bibliothèque de son quartier.

Si les services de bibliothèques, d'archives et de documentation veulent pleinement jouer un rôle d'espace public dans la cité, ils doivent aborder de front ces questions.

Ci-dessous le texte complet de la mise au point de l'IABD.
****

Offrir un accès à l'internet dans une bibliothèque, un service d'archives ou d'information : Les conditions juridiques

Entre les missions des bibliothèques, des services d'archives et d'information, et les obligations légales, quelle est la frontière entre un service ouvert à tous et le respect de la loi ? Comment interpréter les mesures préconisées ou imposées par le législateur, et les concilier avec la tradition d'un accès le plus large possible à l'information et à la connaissance ? Y a-t-il un espace d'interprétation propice à la sauvegarde des libertés ? Partageons-nous une posture professionnelle respectueuse du droit mais aussi des intérêts des usagers ?

Quelles obligations légales ?

· Conserver les logs de connexion ?

Internet peut être libre et gratuit pour le public ; les établissements ne sont pas tenus de recueillir l'identité des personnes à qui ils proposent un accès à l'internet ; l'usager peut même utiliser un pseudo pour se connecter et avoir accès à ses espaces personnels. En revanche, on doit pouvoir identifier l'ordinateur à l'origine de l'usage illicite par une adresse IP fixe.

La seule obligation qui s'impose aux bibliothèques, aux services d'archives et d'information (ou aux organismes dont ils relèvent) est de remettre, lors d'une réquisition judiciaire ou administrative, selon les cas, les logs de connexion (note 1) et toutes les informations qu'ils détiennent (note 2). Ces informations seront recoupées par les services chargés de l'enquête pour retrouver la personne à l'origine de l'infraction. L'antériorité exigible pour les données est d'un an.

· Sécuriser les postes ?

La loi n'impose pas que l'on filtre les accès à l'internet des ordinateurs mis à la disposition du public (note 3). Installer des filtres pour bloquer certains sites susceptibles d'être pénalement répréhensibles ne permettrait que de limiter sa responsabilité en cas de réquisition judiciaire, c'est-à-dire seulement après avoir reçu une lettre recommandée enjoignant l'abonné de sécuriser son poste.

En revanche, le fait de munir de filtres les ordinateurs proposés au public limite de manière arbitraire l'accès à l'internet, alors que cet accès constitue une liberté publique consacrée par le Conseil constitutionnel [5].

· Remettre des informations nominatives ?

C'est une obligation qui ne s'impose, au titre de la loi Hadopi, qu'aux organisations qui opèrent en tant que FAI (les services informatiques des universités, par exemple). Il incombe, en effet, aux FAI de fournir aux personnes chargées de l'enquête les informations détaillées dans le décret du 5 mars 2010, dont certaines sont nominatives (note 4).

Le poids de chartes et des règlements

Chartes et règlements intérieurs permettent d'informer le public des bibliothèques sur les usages interdits, sur la surveillance dont ils peuvent faire l'objet et sur l'existence éventuelle de filtres.

D'autres documents destinés aux bibliothécaires leur rappellent le contrôle qu'il convient d'exercer et leur obligation de mettre fin à tout usage de l'internet qui serait manifestement illicite (contrefaçon, cyberpédopornographie, activités terroristes, etc.). L'enquête permettra d'évaluer, en fonction d'un contexte, la diligence du personnel.

Nulle obligation d'identifier les personnes ni même de filtrer les accès à l'internet

En cas de réquisition, les bibliothèques, les services d'archives et d'information abonnés à des FAI doivent remettre aux enquêteurs les logs de connexion et toute autre information habituellement recueillie.
Il leur est recommandé de remettre aussi les chartes communiquées aux usagers et les informations destinées aux personnels.

Que disent les textes ?

La loi anti-terroriste

L'obligation de conserver pendant un an les données de connexion, imposée aux fournisseurs d'accès Internet (FAI) par la loi anti-terroriste du 23 janvier 2006 [1], est étendue à tous ceux qui offrent un accès à l'internet à leur public.

Comme l'indique le Forum des droits sur l'internet [7], la conservation des logs peut se faire de trois manières différentes : en utilisant localement des unités de stockage dédiées associées à un routeur mis en place pour assurer la répartition du trafic interne entre les différents postes ; en confiant cette obligation au FAI auprès duquel on a acheté des abonnements à plusieurs adresses IP publiques correspondant au nombre de postes ; en confiant l'enregistrement à un tiers prestataire de services.

La loi Hadopi

La loi dite Hadopi [3] dissocie les obligations des FAI de celles des titulaires d'un abonnement à l'internet. La responsabilité d'une bibliothèque, d'un service d'archives ou d'information titulaire de plusieurs abonnements auprès d'un FAI n'est engagée pour les usages illicites réalisés à partir des ordinateurs connectés au réseau mis à la disposition du public que si les postes n'ont pas été sécurisés, après en avoir reçu l'injonction écrite de la Haute Autorité pour la diffusion des œuvres et la protection des droits d'auteur sur Internet (Hadopi).

Qu'en conclure ?

Ni la loi anti-terroriste, ni la loi Hadopi n'obligent ces établissements à identifier les utilisateurs des ordinateurs mis à leur disposition, ni à conserver des informations nominatives pour les remettre lors d'une enquête diligentée par un juge au titre de la loi Hadopi, ou d'une personnalité qualifiée placée auprès du ministre de l'Intérieur au titre de la loi anti-terroriste, ni même à filtrer à titre préventif les accès à l'internet.

Le respect des usages traditionnellement admis dans les bibliothèques, services d'archives et d'information reste compatible avec les obligations juridiques qui leur sont imposées, dès lors que les professionnels appliquent la loi, toute la loi, rien que la loi.

Textes

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

2. Décret 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques. Sur le site Légifrance.

3. Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet. Sur le site Légifrance.

4. Décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet ». Sur le site Légifrance.

5. Décision n° 2009-590 DC du 22 octobre 2009. Loi relative à la protection pénale de la propriété littéraire et artistique sur internet. Sur le site du Conseil constitutionnel.

Recommandations – Déclarations

6. Offrir un accès public à l'internet : Des responsabilités aux multiples implications. Déclaration de l'IABD, 10 mars 2009. Sur le site de l'IABD.

7. Les lieux d'accès public à l'internet. Recommandation du Forum des droits sur l'internet, 28 décembre 2007. Sur le site du Forum des droits sur l'internet.

8. Non au portail blanc. Déclaration de l'IABD du 6 mars 2009. Sur le site de l'IABD.

DOCUMENT N°07

Paris Wi-Fi : Conformité réglementaire

www.api-site-cdn.paris.fr

Un cadre strict et rigoureux

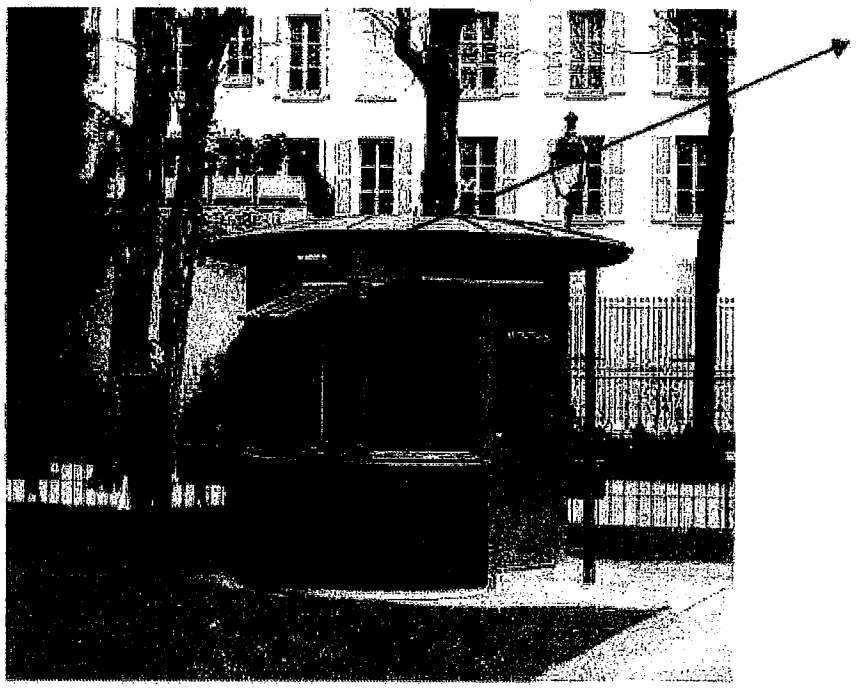
Pour être mis en vente sur le marché européen et obtenir le marquage CE, les équipements WiFi doivent être conformes à la directive européenne 1999/5/CE du 9 mars 1999 et respecter les limites d'exposition fixées par la recommandation européenne 1999/519/CE du 12 juillet 1999. Cette dernière a été transposée en droit français par le Décret N° 2002-775 du 3 mai 2002 *« relatif aux valeurs limites d'exposition du public aux champs électromagnétiques émis par les équipements utilisés dans les réseaux de télécommunication ou par les installations radioélectriques »*.

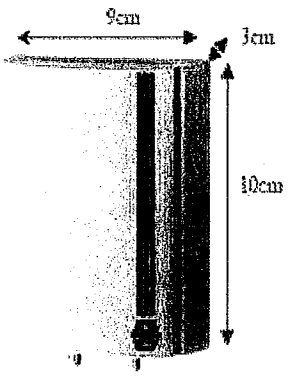
Afin de vérifier leur conformité, les équipements du service Paris WiFi ont été testés selon la norme européenne EN50385:2002 *« Norme de produit pour la démonstration de la conformité des stations de base radio et des stations terminales fixes pour les radio télécommunications avec les restrictions de base et avec les niveaux de référence relatifs à l'exposition de l'homme aux champs électromagnétiques)* ».

Les bornes d'accès à l'Internet du service Paris WiFi sont conformes aux limites d'exposition en vigueur.

Focus

Les antennes des bornes d'accès à l'internet du service Paris WiFi sont généralement installées hors de portée du public. **Les caractéristiques techniques des équipements du service Paris WiFi sont identiques à celles des bornes utilisées par les particuliers.**





Les limites

La conformité au décret 2002-775 est évaluée selon la norme européenne EN 50385. Cette vérification de la conformité au décret est réalisée en considérant le corps humain en contact avec l'antenne et à puissance d'émission maximale. Dans ce cas, la limite d'exposition à ne pas dépasser est de 2 watts par kilogramme (W/kg) dans la tête et le tronc et de 4 W/kg dans les membres : il s'agit du Débit d'Absorption

Spécifique ou DAS qui représente la puissance électromagnétique absorbée par unité de masse de tissu et rend donc directement compte de l'exposition du corps.

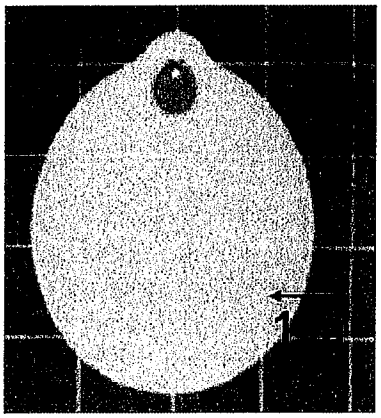
Exposition des personnes

Des valeurs inférieures aux limites

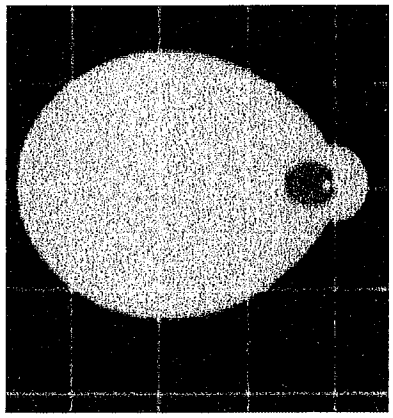
Les normes internationales donnent la possibilité de mesurer l'exposition des personnes en terme de champ électrique exprimé en volts par mètre (V/m), grandeur physique plus facilement mesurable que les watts par kilogramme. Dans le cas des bornes WiFi, la limite à ne pas dépasser est de 61 V/m.

Des simulations ont été réalisées pour évaluer l'exposition du public à proximité des bornes utilisées par le service Paris WiFi. En conditions classiques d'utilisation, le niveau d'exposition des personnes reste inférieur à 61 V/m.

Les figures ci-dessous donnent un exemple de la répartition du champ électrique dans un plan vertical et un plan horizontal en face d'une antenne typique : **au-delà de 3 ou 4 mètres, on voit que le champ électrique est inférieur à 1% de cette limite.**

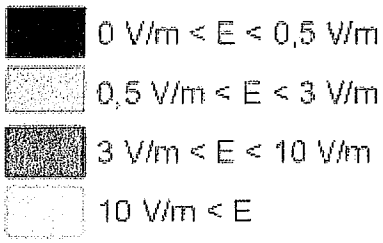


Champ électromagnétique (E)
dans le plan vertical - **1m/carreau**



Champ électromagnétique (E)
dans le plan horizontal - **1m/carreau**

Exemple de niveau du champ électromagnétique produit par des émetteurs WiFi utilisés par le service Paris WiFi



De même, les valeurs de DAS mesurées au contact sont inférieures à la limite de 2 W/kg. En effet, en considérant le corps humain en contact avec l'antenne et à puissance d'émission maximale de la borne WiFi, le DAS est de l'ordre de 0,1 à 1 W/kg selon les installations.