**Développer le WIFI territorial : 10 points juridiques à connaître**

Le déploiement d’un réseau WIFI doit être conforme à plusieurs cadres réglementaires distincts : aides d’Etat, code des marchés publics, règles d’utilisation des fréquences, protection des données personnelles, information du public, sécurisation des transmissions et des systèmes d’information.

**1 Application du Code Général des Collectivités Territoriales :**

Les projets ne relèvent pas du déploiement d’infrastructures Très Haut Débit pour des raisons à la fois techniques --il n’est pas possible de garantir à l’usager un débit supérieur à 30 Mbit/s-- et juridiques  car le cadre réglementaire européen tout comme la jurisprudence française n’assimilent pas ce type d’offre de service WIFI à la compétence des collectivités territoriales en matière d’établissement et d’exploitation de réseaux de communications électroniques telle que définie à l’article L. 1425-1 du code général des collectivités territoriales (CGCT). Ces projets relèvent de la compétence des collectivités ou groupements à laquelle concourt le bâtiment ou l’espace public qui sera équipé (développement économique ou touristique, lecture publique, services à la population…). Il s’agit donc d’un service annexe et complémentaire à la fonction principale du bâtiment proposant une offre WIFI, et la collectivité n’est pas astreinte à se déclarer comme opérateur de réseau auprès de l’Arcep.

Lorsque la maîtrise d’ouvrage est intercommunale, le groupement maître d’ouvrage devra attester qu’il agit dans le cadre d’une compétence qu’il détient, soit parce que la loi lui attribue de droit (cf. statuts du groupement), soit parce que ses membres lui ont transféré cette compétence (cf. délibérations des membres transférant leur compétence).

**2 Aides d’Etat**

La Commission européenne a indiqué que la faiblesse des coûts d’équipement WIFI pris en charge sur chaque site plaçait ces investissements publics en dehors du périmètre des aides d’Etat. Cf. décision modificative des règlements européens (UE) n° 1316/2013 et (UE) n° 283/2014 du dispositif « Connecting Europe Facility », points 15 et 16. <http://data.consilium.europa.eu/doc/document/PE-28-2017-INIT/fr/pdf>

**3 Constat de carence**

L’absence de risque au titre des aides d’Etat n’exonère pas le maître d’ouvrage d’effectuer un constat de carence simple d’une offre similaire à celle qui doit être développée : il sera donc nécessaire d’établir une liste des spots WIFI existants à proximité et de vérifier qu’aucun ne propose sur la même aire un service ouvert et gratuit. De plus il sera important que les services proposés soient limités dans le temps (une journée au maximum pour la première inscription, plus limité ensuite). Ceci conduira à bien différencier le service d’un abonnement de communications électroniques. L’ensemble de la démarche permettra d’attester de l’absence de concurrence déloyale.

**4 Application du code des marchés publics**

Les nouveaux seuils publiés au Journal Officiel de l’Union Européenne, s’établissent ainsi :

* Les marchés d'une valeur inférieure à 221 000 € HT peuvent faire l’objet d’une procédure adaptée et d’une mise en concurrence simplifiée (ce qui pourra être le cas pour des projets conçus à l’échelle d’une intercommunalité) ;
* Les marchés d’une valeur inférieure à 25 000 € HT pourront constituer le cas des communes isolées. L'acheteur public a ici pour seule obligation de choisir une offre pertinente, de faire une bonne utilisation des deniers publics et de  ne pas contracter systématiquement avec un même fournisseur lorsqu'il y a plusieurs offres susceptibles de répondre à son besoin.

**5 Utilisation des bandes de fréquences**

Les bandes de fréquence 2400/2483.5 MHz, 5 150/5 250 MHz, 5 250/5 350 MHz et 5470/5725 MHz sont libres d’utilisation, exonérées de redevance et ne nécessitent pas la délivrance d’une autorisation individuelle par l’Autorité de régulation des communications électroniques et des postes (Arcep). Cependant leur usage est assorti de différentes obligations :

* Limitation à des usages en intérieur ou extérieur selon les bandes de fréquence ;
* Limitation de puissance d’émission des antennes ;
* Utilisation de systèmes de sélection de fréquences dynamiques.

Ces dispositions visent notamment à éviter les interférences avec d’autres appareils, notamment des capteurs météo. Les procédures de rappel de l’Arcep sont facturées 450 €, et peuvent conduire à des peines maximum de 30 000 € et 6 mois de prison et 30 000 € d’amende (l’article L39-1 du CPCE).

Il sera donc indiqué d’appliquer les mesures préventives appropriées, y compris concernant l’exposition aux ondes des crèches, maternelles et autres lieux, prévues dans la réglementation.

**6 Sécurité des transmissions  et des systèmes d’information**

L’offre de services WIFI doit être conforme aux recommandations ANSSI données par la note technique du 9 septembre 2013, qui spécifie l’importance d’isoler le réseau d’alimentation des spots WIFI des réseaux de la collectivité et du système d’informationde la collectivité (cf. fiche de synthèse <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-aux-reseaux-wifi/> ).

Les discussions parlementaires en cours autour du « projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité » pourront faire évoluer ce cadre. La recommandation de la Direction Interministérielle du Numérique et des Services d’Information et de Communication consiste à vérifier que les prestataires de services numériques titulaires des marchés publics sont bien informés de ces évolutions et prévoient de pouvoir appliquer au 29 septembre 2018 les règles de sécurité (substantielles, de niveau 2) définies par le règlement européen n°910/2014 du 23 juillet 2014, dit règlement « eIDAS ». Voir à ce propos le document de présentation proposé par l’ANSSI <https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/>

**7 Conservation des données de trafic**

Les responsables des espaces publics (hot-spots wi-fi, cybercafés, employeurs, collectivités) ont l’obligation de conserver les données de trafic. **Il faut un serveur d'authentification qui archive les données de communications pendant un an glissant.** Voir le **décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques** et la fiche d’information et de recommandation de la CNIL du 28 septembre 2010 <https://www.cnil.fr/fr/conservation-des-donnees-de-trafic-hot-spots-wi-fi-cybercafes-employeurs-quelles-obligations>

**8 Information du public**

La Loi Abeille, Loi n° 2015-136 du 9 février 2015 relative à la sobriété, à la transparence, à l'information et à la concertation en matière d'exposition aux ondes électromagnétiques, précise dans son article n°4, alinéa 3 : «Les établissements proposant au public un accès wifi le mentionnent clairement au moyen d'un pictogramme à l'entrée de l'établissement. »

**9 Protection des données personnelles**

Le 25 mai 2018, le règlement général de protection des données, défini à l’échelle européenne et transcrit dans les droits nationaux, sera applicable. De nombreuses formalités auprès de la CNIL vont disparaître. En contrepartie, la responsabilité des organismes sera renforcée. Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

**10 Mobilisation de la Dotation de Soutien à l’Investissement Local**

La mobilisation de la DSIL est prévue sur des projets à caractère numérique, cf. l’article 157 de la loi n° 2017-1837 de finances pour 2018 du 30 Décembre 2017.