Wi-fi et responsabilité

Laure-Anne CORNELIE

DESS droit du numérique et des nouvelles technologies
Universités Paris I – Paris XI
Mémoire sous la direction de Maître Olivier ITEANU

Septembre 2003

Contact : laure-anne.cornelie@wanadoo.fr

A mes parents et à Olivier MARSET

Remerciements à Olivier MARSET qui, par ses remarques judicieuses et ses explications techniques, est à l'origine de mon intérêt pour le sujet, à Erwan pour le spamming et aux personnes qui m'ont encouragée.

Plan

Introduction

La libéralisation des télécommunications amorcée en 1990[1] avait pour objectif de faciliter l'entrée sur le marché de nouveaux opérateurs et de faire perdre à l'opérateur historique sa position dominante. La réglementation adoptée sur le fondement des prescriptions communautaires, est une émanation des principes du droit de la concurrence. Elle applique des théories telles que la transparence dans la fixation des prix et l'accès aux facilités essentielles pour parvenir à l'exercice d'une parfaite concurrence dans l'intérêt des usagers. Le droit d'accès aux facilités essentielles a notamment pris la forme du dégroupage de la boucle locale[2], offrant aux opérateurs entrants la possibilité d'utiliser le réseau local existant de l'opérateur historique et de desservir directement leurs abonnés.

L'ouverture du marché des télécommunications a également pour intérêt de générer une émulation à la création de technologies innovantes, proposant des solutions alternatives de supports de télécommunication et d'offres de services.

Les offres de services au public se sont enrichies de nouvelles prestations, des solutions ont été expérimentées pour la couverture téléphonique de zones rurales ou enclavées. Ainsi, des expériences ont été menées sur l'utilisation du spectre hertzien dans les collectivités rurales comme solution alternative au réseau filaire.

L'utilisation de la ressource hertzienne a par ailleurs permis l'apparition de nouveaux moyens de communication. Il s'est agi dans un premier temps de la téléphonie mobile qui a connu un rapide succès[3]. La technologie GPRS utilisée par la téléphonie mobile offrait aux professionnels la possibilité de transmettre des données vocales et écrites par le vecteur hertzien.

Le déploiement du réseau filaire fut cependant plus rapide que le réseau hertzien qui n'offrait pas de services comparables. Le succès et la popularité d'Internet furent utilisés pour donner un nouveau souffle à la téléphonie mobile. Il s'est agi de permettre l'accès au contenu de la toile par l'UMTS ou mobile de troisième génération. Cette technologie a suscité bien des espoirs quant à l'accès à Internet mobile via le téléphone portable de l'abonné.

Le projet qui s'annonçait d'envergure a subi plusieurs reports. Les efforts déployés pour sa mise en œuvre ne laissaient pas prévoir l'arrivée de technologies alternatives, développées sur la base d'architecture réseau électrique et offrant une meilleure ergonomie que le

[1] Loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications et loi n° 90-568 du 2 juillet 1990 relative à l'organisation du service public de la poste et des télécommunications qui transforme France Télécom en exploitant public.
[2] La boucle locale est un ensemble de liens filaires ou radioélectriques existant entre le poste de l'abonné et le commutateur d'abonnés auxquels il est rattaché. La boucle locale est ainsi la partie du réseau qui permet à un opérateur d'accéder directement à l'abonné.
[3] En sept ans, de fin 1994 à 2001, le taux d'équipements mobiles est passé de 1,3% à 61,6%, cf. <http://www.art-telecom.fr>.

téléphone portable. Ces technologies ont connu une rapide généralisation. Ceci a été une justification supplémentaire au report du plan de déploiement de l'UMTS.

Dans le cadre des réseaux locaux radioélectriques (RLR ou RLAN[4]), composés d'ordinateurs et d'autres périphériques, deux normes ont été élaborées, l'une utilisant la bande de fréquences de 2,4 GHz et l'autre la bande de 5 GHz. Le nom wi-fi est souvent indifféremment utilisé pour désigner l'un ou l'autre de ces labels ou les matériels ayant reçu la certification de compatibilité avec la norme.

Ces technologies ont permis d'établir des réseaux de petite portée sans fil (*wireless*), en remplaçant donc le câblage par le vecteur hertzien, raccordés à un intranet ou à Internet à distance, à haut débit. L'innovation tient également au fait que ces technologies intègrent des systèmes de sécurité permettant de pallier les fragilités inhérentes à la radioélectricité (*Fidelity*).

Le label wi-fi a été élaboré par l'*Institute of Electrical and Electronics Engineers* (IEEE), sur le standard de la norme IEEE 802.11 (ISO/IEC 8802-11). C'est un standard qui décrit les caractéristiques d'un réseau local sans fil (ou *wireless local area network* WLAN). Il est possible de relier des périphériques à une liaison haut débit (11 Mb/s) sur un rayon de dix à cinquante mètres en intérieur et de plusieurs centaines de mètres en extérieur. Pour ce faire, l'ordinateur portable, l'assistant personnel ou le téléphone équipé d'une carte réseau, se connecte à un point d'accès ou borne d'accès au réseau.

La norme 802.11 définit les couches basses du modèle OSI[5] pour une liaison sans fil utilisant des ondes électromagnétiques. Ces couches sont la couche physique permettant le codage de l'information, la couche de liaison de données constituée de deux sous-couches, l'une contrôlant la liaison logique (*logical link control* ou LLC) et l'autre contrôlant l'accès au support (*media access control* ou MAC).

La norme initiale 802.11 a évolué et il en existe aujourd'hui plusieurs déclinaisons présentant des débits et applications différents. On se dirige vers la norme 802.11x qui offrirait des moyens complémentaires en matière de chiffrement des données.

Il est possible d'échanger des données jusqu'à 54Mb/s dès lors que les ordinateurs sont équipés d'une carte wi-fi les reliant entre eux ou/et à une borne radioélectrique d'accès à Internet.

---

[4] RLAN pour Radio Local Area Network.

[5] OSI signifie Open system interconnection ou interconnexion de systèmes ouverts. C'est un standard permettant de gérer la communication entre ordinateurs de réseau comportant 7 couches : une couche physique qui définit la façon dont les données sont converties en signaux numériques, une couche liaison de données qui définit l'interface avec la carte réseau, une couche réseau qui permet de gérer les adresses et le routage des données, une couche transport qui est chargée du transport des données et de la gestion des erreurs, une couche session qui contrôle le dialogue entre les machines, une couche présentation qui définit le format des données, et une couche application qui assure l'interface avec les applications.

Le wi-fi se généralise car il présente divers intérêts économiques et sociaux. Les équipements wi-fi utilisent des bandes qui ont dans la plupart des pays été libéralisées et qui sont dédiées à l'expérimentation industrielle, scientifique et médicale. Ceci permet la fabrication de matériels, à prix abordable par des particuliers[6].

L'avantage de la ressource hertzienne est de supprimer le câblage, évitant ainsi d'investir dans des infrastructures filaires onéreuses. Cet intérêt doit être apprécié en corollaire avec la politique sociale visant à réduire la fracture numérique entre les citoyens. Il est très vite apparu que le wi-fi pouvait, au-delà des utilisations domestiques, donner accès à l'Internet haut débit aux habitants des collectivités rurales. Il n'est plus nécessaire d'installer dans chaque foyer une prise téléphonique reliant l'abonné au réseau filaire. Dorénavant, il suffit qu'un opérateur connecté au réseau filaire installe des bornes radioélectriques offrant une connexion à son réseau pour que les habitants d'une collectivité bénéficient des services de la société de l'information.

Pour les collectivités locales où le périmètre à couvrir est important, le réseau radioélectrique est composé d'une parabole satellite et de bornes qui relaient les signaux captés par la parabole vers les antennes domestiques.

Par ailleurs, le wi-fi s'inscrit également dans le cadre d'une politique de développement économique urbain. Les relations d'affaires peuvent être réalisées en tout lieu via Internet grâce à l'installation de points d'accès dans les lieux de passage public ou *hotspots*.

Le wi-fi a connu un rapide engouement aux Etats-Unis. Selon une étude du *Yankee Group*,[7], il y avait 3020 *hotspots* en 2002 et 12080 en 2003. La contagion s'est propagée en Europe où 5000 *hotspots* étaient dénombrés par *IDC Gartner* en février 2003, contre 840 en 2002.[8]

La France n'a pas résisté à la vague wi-fi. Depuis la décision de l'ART du 7 novembre 2002 permettant l'installation de bornes wi-fi,[9] le nombre de *hotspots* a augmenté,[10] permettant l'accès au haut débit dans les gares, les hôtels et aéroports.

Le wi-fi est une illustration de la convergence des vecteurs de communication comme le constate la directive européenne " cadre" du 7 mars 2002.[11] Il entre ainsi dans la nouvelle

---

[6] Sur le site <http://fr.kelkoo.com>, il était possible de trouver au début du mois de septembre 2003 des cartes PCMCIA à partir de 45 €, des bornes d'accès à 130 € et des routeurs de point d'accès à 162 €.

[7] Etude de juillet 2003, parue le 1er septembre 2003 dans le Journal du Net : *Le marché du Wi-Fi,* <http://www.journaldunet.com/>.

[8] Etude d'IDC Gartner de février 2003 parue dans le Journal du net du 9 juillet 2003.

[9] Décision n° 02-1031 du 7 novembre 2002 adoptant les lignes directrices de l'ART relatives à l'expérimentation de réseaux ouverts au public utilisant la technologie RLAN.

[10] En mai 2003, il y avait en région Ile-de France plus d'une soixantaine de hotspots répertoriés après enquête du Journal du net cf. : <http://www.journaldunet.com/dossiers/wifi/annuairewifiidf.shtml>.

[11] Directive 2002-21 CE du parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques JOCE L 108/33, 24 mars 2002.

nomenclature des réseaux de communications électroniques. L'article 2-a de la directive qualifie de réseau de communications électroniques :

" *les systèmes de transmission et, le cas échéant, les équipements de communication ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires (...) les réseaux terrestres fixes et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux (...)* ".

Les réseaux utilisant la norme wi-fi répondent aux critères de cette qualification étant donné qu'il s'agit de systèmes de transmission permettant par voie hertzienne et le cas échéant satellitaires, la transmission de données et l'accès au haut débit.

Les espoirs sont donc réels et tous les arguments militent en faveur de la généralisation du wi-fi. Cependant en France, il y a plusieurs freins au développement du wi-fi.

Il y a d'une part des freins techniques.

Sur le territoire national, la bande de fréquence 5 GHz n'est pas totalement libéralisée. Dans deux décisions en date du 3 décembre 2002, l'ART a limité l'utilisation des réseaux radioélectriques en intérieur sur la bande de fréquences 5150-5350 MHz et a interdit toute émission sur la bande 5470-5725 MHz.[12] Cette interdiction a pour " *but d'assurer la compatibilité avec les projets de réseaux satellites du service mobile par satellite ainsi qu'avec les systèmes radar existant dans la bande* ".

Ce sont des raisons similaires qui faisaient obstacle à la libéralisation totale de la bande de fréquences 2,4 GHz dans certains départements. En effet, bien qu'étant une bande de fréquences internationalement libre de droit, la France bénéficiait de la part de l'Union internationale des télécommunications (UIT) d'une exception fondée sur l'intérêt de la Défense nationale. Les fréquences 2450-2500 MHz ont ainsi été utilisées et le sont encore pour les radars et pour le lancement de fusées Crotale.

Ce régime d'exception accordé à la France au sein des Nations Unies a été l'une des causes de la lenteur de déploiement des réseaux wi-fi dans certains départements pour lesquels l'établissement en vue de la fourniture de services au public était soumis à autorisation. Mais depuis les décisions 03-908 et 03-909[13], le régime s'est assoupli et se rapproche des

[12] Décision n° 02-1091 attribuant des fréquences aux installations radioélectriques dans la bande 5150-5350 MHz et décision n° 02-1092 fixant les conditions d'utilisations radioélectriques dans la bande 5150-5350 MHz datées du 3 décembre 2002.

[13] Décision de l'ART n° 03-908 du 22 juillet 2003, modifiant la décision n° 2002-1009 de l'ART en date du 31 octobre 2002, attribuant des fréquences aux installations radioélectriques dans la bande 2400-2483,5 MHz. Décision de l'ART n° 03-909 du 22 juillet 2003 portant modification de la décision n° 2002-1031 de l'ART en date du 7 novembre 2002 portant l'adoption des lignes directrices relatives à l'expérimentation de réseaux ouverts au public utilisant la technologie RLAN.

prescriptions européennes posées par la Conférence européenne des administrations postales et des télécommunications.[14] Il tend à s'inscrire dans le cadre des directives européennes " paquet télécom " du 7 mars 2002[15] qui n'étaient pas transposées au 24 juillet 2003, mais dont certaines de leurs dispositions sont d'effet direct.

Il existe également un frein juridique au déploiement des RLR wi-fi dans les collectivités rurales. L'article L 1511-6 du code général de collectivités locales, modifié par la loi du 17 juillet 2001,[16] n'autorise pas les collectivités locales à exercer les activités d'opérateur au sens de l'article L 32, 12° du CPT. Elles peuvent cependant bâtir des infrastructures de télécommunications. En effet, cette disposition, justifiée par la préservation de l'initiative privée, organise une procédure de consultation publique destinée à recenser les besoins des opérateurs ou utilisateurs pour la création d'infrastructures de télécommunications.

Certains considèrent pourtant qu'il s'agit d'un régime qui ne tient pas compte des limites que peut présenter l'initiative privée ignorante de l'altruisme et de l'intérêt public. Cet article ne se préoccupe pas de la participation des zones rurales à la politique de développement des télécommunications. L'offre d'accès à haut débit par le biais du wi-fi dans les collectivités se trouve ainsi ralentie, ce au moins jusqu'à l'adoption de la loi sur la confiance dans l'économie numérique. En effet, depuis la modification du projet de loi par le Sénat, il est prévu de permettre aux collectivités territoriales et à leurs groupements d'établir des réseaux de télécommunications ouverts au public et d'offrir des services de télécommunications lorsqu'il y a une insuffisance d'initiatives privées, sous réserve du respect du droit de la concurrence.[17]

Un autre argument juridique fondé sur la constatation des limites du droit face aux nouvelles technologies est avancé. Etant une nouvelle technique de communication, le wi-fi présenterait des situations de fait nouvelles qui ne sauraient être appréhendées par les mécanismes juridiques existant. Il y aurait des vides juridiques engendrés par les spécificités inhérentes à cette technologie. La norme utilise les ondes radioélectriques qui sont par nature peu sécurisées. Elle permet de surcroît l'accès au réseau Internet, " espace de non droit " du fait de sa dimension planétaire. Le wi-fi se révèle alors être un moyen idéal de commission d'infractions. Leurs auteurs ne verraient pas leur responsabilité engagée étant donné l'inadaptation du droit à la matière.

---

[14] CEPT ; organisme créé en 1959 entre des Etats européens, en vue de la concertation et de la coopération en matière commerciale, de la coordination du spectre et de régulation technique et normative. Elle est à l'origine de l'European Telecommunications Standards Institute chargée de la standardisation.

[15] Directive 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion dite " accès " ; directive 2002/20/CE relative à l'autorisation de réseaux et de services de communications électroniques dite " autorisation " ; directive relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques 2002/21/CE dite " cadre " ; directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques dite " service universel ".

[16] L n° 2001-624 du 17 juillet 2001 portant diverses dispositions d'ordre social, éducatif et culturel article 19, JO 18 juillet 2001.

[17] Projet de loi pour la confiance dans l'économie numérique adopté par le Sénat le 25 juin 2003 ; pour consultation cf. e.g : <http://senat.fr/dossierleg/pjl02-195.html>.

Ces réflexions sont identiques à celles qui ont été tenues au début du développement de l'Internet. Or, le droit a rappelé avec force qu'il n'était pas nécessaire de recourir à des régimes juridiques nouveaux[18]. Les mécanismes existant se sont adaptés sans difficultés à Internet. Il en est ainsi par exemple des dispositions relatives à la diffamation et autres délits de presse issus de la loi, pourtant ancienne, du 29 juillet 1881. On peut également citer les principes du respect de la vie privée et des correspondances s'appliquant au courrier électronique, ou enfin l'ensemble des traités internationaux relatifs au droit international de la vente et partant, aux contrats de vente à distance en ligne.[19]

Il en ressort que l'Internet n'a pas généré de comportements délictueux nouveaux mais n'est qu'un moyen nouveau de commission d'infraction.
Qu'en est-il pour le wi-fi ? Cette technologie permet-elle à ses acteurs d'échapper à leur responsabilité ?

Le wi-fi est un système de communication électronique qui a pour originalité de réunir des modes de télécommunication existants. Il réalise la convergence entre le vecteur hertzien et le haut débit.

L'emploi de la technologie hertzienne n'est pas nouveau. Très tôt il a été question de réglementer au sein des Nations Unies cette ressource rare en vue de son utilisation optimale par l'ensemble des pays. L'UIT a dressé un tableau d'utilisation des fréquences organisant la répartition des fréquences et les régimes d'autorisation auxquels elles étaient soumises. L'adoption de ce règlement par les Etats membres a institué un régime juridique précis encadré par des mécanismes d'engagement de responsabilité.

L'accès au haut débit que facilite le wi-fi est en réalité un accès à Internet par l'utilisation de la technologie du xDSL. Or, comme Internet n'est pas un espace sans droit, les règles qui régissent Internet trouvent également à s'appliquer au wi-fi.

Les divers acteurs du wi-fi ne sont pas livrés à eux-mêmes. L'opérateur du réseau radioélectrique ouvert au public, installateur des bornes et des points d'accès, sera soumis au droit des télécommunications pour les aspects tenant à l'installation du réseau et à certaines dispositions du droit des télécommunications régissant le droit des contrats. Ainsi par exemple, dans l'hypothèse où l'opérateur du réseau radioélectrique est une autre personne que l'opérateur du réseau de données haut débit, des conventions d'interconnexion devront être signées en considération des exigences essentielles.

---

[18] TGI Paris, ordonnance de référé 22 mai 2000, Affaire Yahoo!, Communication, commerce électronique septembre 2000, commentaire n°92 ; Juriscom.net : <http://www.juriscom.net/jpt/visu.php?ID=300>.
[19] Convention des Nations Unies sur les contrats de vente internationale de marchandises dite Convention de Vienne du 11 avril 1980, publiée en France par un décret du 22 décembre 1987, et la Convention de La Haye de détermination des conflits de loi en matières de ventes internationales du 15 janvier 1955, entrée en vigueur en France le 1er septembre 1964.

Par ailleurs, l'opérateur du réseau radioélectrique devra nouer une relation contractuelle avec le fournisseur d'accès à Internet s'il n'exerce pas lui-même cette activité.

Dans les lieux de passage public, le gestionnaire du point d'accès à Internet devra d'une part établir un contrat d'accès à Internet avec un fournisseur d'accès et d'autre part, un contrat de prestation de service avec l'utilisateur qui veut se connecter à sa borne.

Une autre architecture contractuelle peut être envisagée lorsque le gestionnaire du site relie une borne à un réseau d'accès radioélectrique à Internet. Dans ce cas, l'opérateur du réseau est un fournisseur d'accès offrant un service d'accès à Internet régi par le droit des contrats.

Il reste l'utilisateur final qui peut se retrouver dans trois situations différentes.

L'utilisateur peut accéder au haut débit par le biais d'un point d'accès public. Le service peut être payant ou gratuit.

L'utilisation du wi-fi peut être interne, pour le partage d'une connexion haut débit filaire par tous les membres de la famille ou les employés d'un bureau.

Un autre exemple de semi-mobilité peut être donné pour ce qui est de la desserte de régions rurales. L'accès au haut débit se fait par le biais d'un contrat passé entre l'opérateur du réseau radioélectrique qui fournit l'accès à Internet à l'ensemble d'une commune.

Ces différents aspects contractuels issus de la typologie des acteurs seront peu ou prou abordés. Seront mises en lumières les questions pratiques qui se présentent en matière de wi-fi et les solutions juridiques qui peuvent y répondre, mais dont la méconnaissance fait dire qu'il y a vide juridique.

Pour certaines de ces questions, des solutions juridiques ont d'ores et déjà été édictées par le législateur ou par l'Autorité de régulation elle-même. Elles touchent aux réseaux radioélectriques de télécommunications utilisant la norme 802.11.

D'autres questions sont, elles, relatives aux données transmises par le réseau. Ces données peuvent être issues du réseau radioélectrique mais aussi du réseau à haut débit. Dans l'un ou l'autre cas, elles peuvent être source de responsabilité.

Il en ressort que le wi-fi peut faire naître la responsabilité de ses acteurs en tant que réseau radioélectrique de télécommunication (chapitre I) et à cause du contenu qui y transite (chapitre II).

Chapitre 1- Le réseau en tant que contenant, source de responsabilité

L'installation d'un réseau radioélectrique de télécommunications est soumise à des prescriptions strictes afin de garantir la qualité des télécommunications, ainsi qu'une bonne gestion du spectre hertzien **(I)**. Ces exigences sont maintenues au cours de l'utilisation du réseau **(II)**.

Section 1 - L'ignorance des conditions d'établissement d'un réseau local radioélectrique sur la bande de fréquences 2,4GHz.

Les réseaux radioélectriques sont soumis à des conditions plus ou moins strictes d'établissement. Celles s'appliquant aux RLAN sont peu contraignantes depuis la loi du 27 juillet 1996 en faveur des technologies de communications innovantes,[20] mais elles doivent pour autant être présentées (§ 1). La puissance d'émission du réseau et la bande hertzienne de transmission sont en revanche des éléments techniques qui sont fonction de la typologie du réseau (§ 2). Les équipements composant ce dernier doivent s'y conformer (§ 3).

§ 1. Les conditions générales d'établissement d'un réseau local wi-fi

Les conditions d'établissement d'un RLAN ont évolué et ne font plus l'objet de contrôle par l'ART (A). L'utilisateur du réseau doit cependant garantir le respect d'exigences techniques dans l'hypothèse où les communications transmises par le futur réseau emprunteront un réseau ouvert au public (B).

A. L'évolution des conditions d'établissement d'un RLR

Sous l'ancien régime, l'établissement d'un RLAN wi-fi nécessitait ou non l'octroi d'une licence individuelle (1). Le régime actuel issu de la directive communautaire " autorisation " facilite l'établissement des RLAN wi-fi qui ne requiert qu'une déclaration (2).

1. L'ancien régime de l'octroi d'une licence d'établissement en fonction de la typologie du réseau

En raison de la rareté de la ressource hertzienne, l'établissement d'un réseau radioélectrique est soumis à autorisation qu'il soit ouvert au public ou indépendant. Cependant, dans ce dernier cas, l'article L 33-3 réservait les hypothèses où le réseau radioélectrique était de faible portée et celle où il n'utilisait pas de fréquences spécifiquement assignées à son utilisateur. Aucune licence n'était nécessaire, mais l'utilisateur avait à se conformer aux prescriptions posées par l'ART.

Les dispositions prises concernant le wi-fi illustraient ce régime.

[20] Loi nº 96-659 du 26 juillet 1996 art. 6 Journal Officiel du 27 juillet 1996.

a. La nécessité d'une licence d'établissement pour les RLR ouverts au public

Aux termes de l'article L 33-1 du CPT, les RLAN établis pour la fourniture au public de services de télécommunication, devaient obtenir une autorisation préalable du ministre chargé des télécommunications, après instruction du dossier par l'Autorité de régulation. Selon cet article, le maintien de la licence accordée pour une durée de 15 ans est soumis à l'application d'exigences contenues dans un cahier des charges.

Les premiers RALAN wi-fi ouverts au public ont bénéficié d'une licence délivrée à titre expérimental. Les réseaux expérimentaux dépendent de l'article L 33-1 alinéa 4 qui limite l'autorisation à une durée inférieure à quinze années. Les premières licences expérimentales ont été accordées gratuitement par l'ART, pour une durée de 18 mois renouvelables.[21]

L'ouverture d'une procédure d'octroi de licence peut être introduite par toute personne physique ou morale présentant les qualités pour l'exercice de l'activité d'opérateur. Appliquée aux RLAN, la procédure suivait une forme simplifiée, dans l'esprit du futur régime d'autorisation générale instauré par les directives " paquet télécom ". Ainsi, dès lors que le dossier de demande d'établissement d'un RLAN était complet, l'ART le transmettait au ministère de la Défense. Ce dernier vérifiait la localisation du projet par rapport aux sites et équipements militaires.

L'application d'un régime libéral n'écartait pas l'exigence de l'octroi d'une licence expérimentale préalablement à l'établissement du réseau. A défaut, l'opérateur s'exposait à une sanction pénale de six mois d'emprisonnement et de 75 000 euros d'amende.

Les réseaux pour lesquels une licence avait été octroyée émettaient avec une puissance de 100 mW sur toute la bande de fréquences 2400 et 2483,5 GHz, à l'extérieur comme à l'intérieur de bâtiments. Des liens fixes point à point pouvaient être établis pour les besoins de ces réseaux dans la bande 2,4 GHz ou dans des bandes de fréquences spécifiques. Dans ce dernier cas, la demande de licence suivait une procédure spécifique[22].

Le futur régime simplifié n'a pas influencé que la procédure d'octroi de licence. Il était visible au niveau de l'installation d'équipement lui-même. Ainsi, le raccordement d'une borne d'accès à un réseau ouvert au public ne nécessitait aucune autorisation, que ce raccordement soit réalisé par le titulaire de la licence d'établissement du réseau ouvert au public ou par un tiers désireux d'installer un *hotspot*.

L'installation de *hotspots* consiste en la fourniture de services d'accès à un réseau ouvert au public dans des lieux de passage public en vue de partager un même accès haut débit.

---

[21] La première autorisation d'expérimentation a été accordée par un arrêté en date du 27 février 2003 à M. Zablocki sur le territoire de l'île de Ré (JO du 25 mars 2003 p 5290).

[22] La procédure à suivre était celle de demande d'installation d'un réseau sur la bande de fréquences 3,5 GHz. Actuellement, une société intéressée par la boucle locale radio doit tout d'abord déposer à l'Autorité un dossier de licence.

La fourniture d'un tel service peut ne nécessiter que l'installation de bornes d'accès sans équipements plus lourds. C'est pour cela qu'aucune licence n'était nécessaire.

En revanche, lorsqu'une personne souhaitait établir un nouveau réseau d'accès ayant pour objet de relier les bornes radioélectriques entre elles ou d'utiliser un réseau privé existant, une autorisation s'imposait. En effet, le fait de relier des bornes radioélectriques d'accès consiste à établir un nouveau réseau ouvert au public.

De même, l'utilisation RLAN privé existant pour la fourniture de service au public nécessitait l'octroi d'une licence. En effet, ceci était justifié par le raisonnement suivant lequel l'ouverture au public d'un réseau privé revient à modifier la destination de ce réseau en réseau ouvert au public. Or, un exploitant de réseau indépendant ne peut conférer à son réseau le caractère de réseau ouvert au public sans autorisation préalable délivrée dans les conditions prévues à l'article L 33-1. A défaut, l'exploitant est sanctionné dans les conditions prévues aux articles L 36-11 et L 39.[23] Ces dispositions valaient pour les RLAN indépendants et une licence d'expérimentation de dix-huit mois devait être sollicitée auprès de l'ART.

b. La conformité des RLR wi-fi indépendants aux prescriptions de l'ART

L'installation d'un réseau indépendant sur la bande de fréquences 2,4 GHz était libre, la bande de fréquences 2,4 GHz n'étant pas assignée à un utilisateur. Mais l'utilisateur devait se conformer aux prescriptions de l'ART posées dans les décisions n° 02-1008 et n° 02-1009 de l'ART.[24]

Selon ces décisions, aucune demande de licence n'était requise pour les réseaux indépendants émettant à l'intérieur. *A contrario*, une autorisation était nécessaire pour les réseaux émettant à l'extérieur. A défaut, l'établissement d'un tel réseau était sanctionné de six mois d'emprisonnement et de 30 000 euros d'amende. L'application de la sanction pénale était précédée d'une injonction faite en vue de la désinstallation du réseau.

La notification adressée à une association pour le développement des réseaux sans fils dans les collectivités locales illustre la fermeté de l'Agence nationale des fréquences et de l'ART dans l'application de ces dispositions. Il s'agissait en l'espèce d'une association qui avait installé un réseau radioélectrique dans la commune de Mane située dans les Alpes du sud. Ce réseau qui émettait en extérieur, permettait d'accéder au réseau haut débit. Après un mois de fonctionnement, l'association s'est vue notifier par l'ANF une injonction de désinstallation du réseau sous peine de sanctions pénales.[25]

---

[23] Cf. article L 33-2 alinéa 5.

[24] Cf. décisions de L'ART du 31 octobre 2001, n° 02-1008 et n° 02-1009, ainsi que l'arrêté du ministre délégué à l'industrie en date du 23 décembre 2002 homologuant la décision n°02-1006, publié au JO 19 janvier 2003 p.1188.

[25] Cf . e.g.: <http://pw.lesmanos.com/news.php>.

2. Le nouveau régime de la déclaration

Le projet de loi de transposition des directives communautaires du 7 mars 2002, dites " paquet télécom "[26], prévoit en son article 6 de modifier l'article L 33-1 actuel en introduisant un régime de simple déclaration préalable à l'ART.

Ce régime est en vigueur depuis le 25 juillet 2003, car il s'agit d'une disposition d'effet direct de la directive " autorisation " 2002/20/CE.

a. Le régime de la déclaration pour l'établissement des RLR ouverts au public.

Le futur article L 33-1 disposera que, l'établissement d'un réseau ouvert au public et la fourniture au public de services de communications électroniques sont libres, sous réserve d'une déclaration préalable auprès de l'ART.

Les opérateurs de RLAN ouverts au public bénéficient d'ores et déjà de ce régime et doivent uniquement, depuis le 25 juillet 2003, date d'entrée en vigueur de certains effets des directives " paquet télécom ", déclarer l'installation du réseau. La déclaration adressée à l'ART, contient des éléments d'identification de l'opérateur tels que son siège social, son numéro d'immatriculation au RCS, un extrait Kbis et les coordonnées d'un correspondant dans l'hypothèse où il y a des liaisons. La déclaration présente une description du projet, en indiquant la zone couverte et la date de lancement. Pour les études prospectives de l'ART, l'opérateur peut préciser le montant des investissements et ses éventuels partenariats avec des collectivités locales.

De même que sous l'ancien régime, les RLAN ouverts au public, raccordés à des RLAN existants étaient établis sans licence, de même aujourd'hui ils n'ont pas à être déclarés.

Les RLAN wi-fi ouverts au public sont toujours établis à titre expérimental et ce jusqu'à la fin de l'année 2004,[27] et les expérimentations en cours se poursuivent.

b. Les RLR indépendants

L'établissement d'un réseau privé wi-fi devient libre. Aucune formalité n'est requise auprès de l'ART, qu'il y ait ou non raccordement à un réseau ouvert au public.

Le non-respect de l'obligation de destination a beaucoup moins de conséquence car leur changement de statut les fait tomber dans le régime de la déclaration et non de la licence obligatoire. Cependant cette déclaration est nécessaire et les opérateurs devront se soumettre aux obligations faites aux réseaux ouverts au public en matière de confidentialité des correspondances.[28]

---

[26] Projet de loi n° 1055, adopté en Conseil des ministres le 31 juillet 2003.
[27] Cf. les lignes directrices du 25 juillet 2003 sur *L'évolution du régime d'autorisation pour les RLAN à compter du 25 juillet 2003.*
[28] Article L 33-1 et article 6 du projet de loi sur la communication électronique daté du 31 juillet 2003.

L'article 9 de l'avant projet de loi introduisait une nouvelle notion de " *réseaux ouverts au public interne* ", sans en donner de définition. Ceci donnait lieu à interrogation sur la nature de ces réseaux qui, comme les RLAN indépendants, auraient été exemptés de déclaration.

Dans l'article 6 du projet de loi adopté le 31 juillet 2003, il est question de " *réseaux internes ouverts au public* ". Ces réseaux suivent le régime des réseaux indépendants. L'inversion des adjectifs laisse à penser qu'il s'agit de réseaux indépendants permettant à plusieurs groupes fermés d'utilisateurs de communiquer. L'ART tendait à considérer que ces réseaux étaient en réalité des réseaux ouverts au public. Le nouvel alinéa de l'article L 33-1 les ferait échapper à l'obligation de déclaration préalable et aux sanctions y afférentes.

Il serait même possible selon cet article d'éviter à un réseau privé, dont la destination a été modifiée, de procéder à toute déclaration, dès lors que les communications qu'il permet sont réservées à un groupe fermé.

Le nouveau régime permettra sans conteste de faciliter l'établissement de réseaux radioélectriques.

B. L'ignorance des dispositions relatives au droit d'accès au réseau

Afin d'encourager le développement des télécommunications, l'établissement de nouveaux réseaux est facilité par la possibilité d'avoir accès à des infrastructures existantes. Ceci a pour but d'éviter que les nouveaux opérateurs aient à investir dans des équipements onéreux tout en leur permettant d'entreprendre librement des projets liés au marché des télécommunications. Il s'agit d'une facilité essentielle au sens du droit de la concurrence définie par la directive européenne " accès " du 7 mars 2002 comme, " *la mise à la disposition d'une autre entreprise, dans des conditions biens définies et de manière exclusive ou non exclusive, de ressources et/ou de services en vue de la fourniture de services de communications électroniques* ".[29] La directive poursuit qu'il s'agit notamment d'un accès à des éléments de réseaux et à des ressources associées et éventuellement la connexion des équipements par des moyens fixes ou non tels que la boucle locale, l'accès à des infrastructures physiques et l'accès aux systèmes logiciels.

L'accès au réseau existant constitue un droit s'exerçant dans le cadre d'un contrat passé entre l'opérateur et le nouvel entrant, dans le respect des exigences essentielles. Tous les contrats portant sur l'accès doivent être conclus dans le respect des conditions d'objectivité, de transparence et d'absence de discrimination.

[29] Directive 2002-19 CE du Parlement européen et du Conseil relative à l'accès aux réseaux de communications électroniques et aux ressources associés, ainsi qu'à leur interconnexion, article 2-a JOCE L 108/7 du 24 avril 2002.

Deux cadres principaux se présentent. Il peut soit s'agir d'un contrat d'interconnexion, soit d'un contrat d'accès à la boucle locale.

Dans la législation actuelle, l'interconnexion est un service réciproque d'accès aux réseaux entre deux opérateurs de réseaux ouverts au public. La prestation d'interconnexion peut n'être qu'unilatérale lorsqu'elle est offerte à un fournisseur de service au public.

Cette convention est signée dans l'intérêt des utilisateurs qui peuvent ainsi, grâce à l'interconnexion, communiquer entre eux quel que soit le réseau auquel ils sont raccordés ou quel que soit le service qu'ils utilisent.[30]

Cependant, le projet de loi sur la communication électronique limite l'interconnexion à la seule prestation réciproque entre opérateurs de réseaux ouverts au public, et parle d'accès lorsqu'il s'agit de l'autorisation faite par l'opérateur du réseau ouvert au public à un fournisseur de services de communications électroniques.[31]

Les conventions d'interconnexion sont soumises à l'ART qui vérifie qu'elles sont passées dans des conditions de nature à préserver la concurrence et les dispositions réglementaires.

Avant la mise en œuvre effective de l'interconnexion, les interfaces doivent faire l'objet d'essais définis et réalisés conjointement par les deux opérateurs concernés. Dans le cas où les essais d'interconnexion ne s'effectueraient pas dans des conditions techniques et dans des délais normaux, l'une ou l'autre des parties peut saisir l'ART. Les interfaces d'interconnexion doivent bien sûr être conformes aux spécifications techniques adoptées et publiées par l'ART en vue de garantir les exigences essentielles et la qualité de bout en bout.

Les conventions d'interconnexion sont des conventions de droit privé[32] qui, en cas de litiges, sont soumises aux principes du droit général des contrats. L'ART est compétente lorsque les parties optent pour l'arbitrage.

Le droit d'accès inclut également l'accès à boucle locale radioélectrique (ou BRL), communément appelé " dégroupage ". Ceci consiste à ouvrir aux nouveaux opérateurs l'accès au réseau radioélectrique local de l'opérateur historique pour desservir directement leurs abonnés.

Certains réseaux indépendants peuvent également être connectés à un réseau ouvert au public. Les parties concluent une convention qui a pour nature un contrat de location d'une capacité de transmission, régi par le droit privé.

L'article R 9 du CPT définit la liaison louée comme " *la mise à disposition par l'exploitant public d'un contrat de location d'une capacité de transmission, entre des points de*

[30] Cf. Article L 32, 9° CPT.
[31] Cf. Article 2 du projet de loi.
[32] Articles L34-8 et D 99-6 du CPT.

terminaison déterminés du réseau public au profit d'un utilisateur à l'exclusion de toute commutation contrôlée par cet utilisateur ". Ceci exclut le multipoint et la commutation.

Pour l'installation de RLAN dans des lieux de passage public, on peut identifier le raccordement de bornes à un réseau radioélectrique ouvert au public comme l'exercice du droit d'accès. L'opérateur du réseau ouvert au public offre au gestionnaire du site une facilité pour le déploiement de son activité.

Un réseau indépendant radioélectrique n'est pas redevable d'un service d'accès à l'égard d'un autre réseau indépendant. Ceci reviendrait à modifier la nature du réseau privé en réseau ouvert au public. Malgré l'assouplissement du régime d'établissement, les conséquences pour l'utilisateur privé sont réelles car le défaut de déclaration préalable constitue un délit.[33] Par ailleurs, les gestionnaires des RLAN ouverts au public ont des obligations relatives à la fourniture du service universel et à la confidentialité des correspondances. L'utilisateur d'un réseau indépendant wi-fi ou le gestionnaire d'un *hotspot* privé, ne peut donc être contraint d'offrir un accès à son réseau, par exemple pour faciliter l'itinérance.

La généralisation du droit d'accès au réseau a permis d'offrir aux usagers un service d'itinérance ou de " *roaming* ". Ce service, qui a d'abord été offert en matière de téléphonie mobile, garantit à l'utilisateur d'accéder au meilleur réseau disponible quel que soit l'endroit où il se trouve, y compris à l'étranger, et ce sans jamais couper la communication.

En matière de réseau utilisant la technologie wi-fi, il n'y a pas à la charge des opérateurs d'obligation d'itinérance à l'égard des utilisateurs du réseau. Ils sont libres de proposer ou non cette prestation en passant des accords commerciaux avec les opérateurs ou avec des fournisseurs d'accès. L'ART estime que ceci vaut également dans les communes rurales, où les premiers réseaux wi-fi sont installés à titre expérimental dans le cadre du développement de la boucle locale, aucune obligation d'itinérance n'existe.

Les conditions générales d'installation de réseaux radioélectriques ayant été envisagées, il convient de rentrer plus dans les détails des exigences tenant à la puissance d'émission de ces réseaux.

§ 2. Les conditions particulières d'établissement : la localisation du réseau et la puissance d'émission

L'ART a fixé, dans sa décision n° 02-1008 et dans ses lignes directrices[34], les conditions d'utilisation des fréquences sur la bande 2,4 GHz. L'émission d'un RLR wi-fi sur la bande

[33] Article 19 du projet de loi sur la communication électronique.
[34] Cf. décisions n°02-1008 et 02-1009 du 31 octobre 2002, et les Lignes directrices relatives à l'expérimentation de réseaux ouverts au public utilisant la technologie RLAN adoptées par le 7 novembre 2002 par la décision n°02-1031.

de fréquences 2,4 GHz dépendait de sa localisation (A). Ce régime est abrogé depuis la décision de l'ART du 22 juillet 2003 (B).

A. L'ancien régime de la localisation géographique

Certains départements étaient ou non libéralisés.

1. Les départements libéralisés

Les réseaux ouverts au public ayant obtenu une licence d'autorisation du ministre des télécommunications pouvaient émettre en intérieur ou en extérieur sur la bande 2,4 GHz ou sur des bandes de fréquences spécifiques utilisant une puissance isotrope rayonnée de 100 mW.

Pour l'installation d'un réseau radioélectrique indépendant, l'utilisateur devait tenir compte de la situation géographique du réseau et du périmètre d'émission déterminé par la puissance d'émission. Selon le réglage de la puissance d'émission, le réseau diffuse ou non en extérieur. Or, c'était la situation géographique qui déterminait s'il était possible d'installer un réseau émettant à l'extérieur d'un bâtiment.

L'utilisateur devait se reporter à la liste des départements dressée par l'ART, dans lesquels il était possible d'utiliser un réseau radioélectrique émettant en intérieur comme en extérieur. Cette liste, présentée le 3 février 2003 par l'Autorité de régulation, traduisait les dernières avancées en matière de libéralisation telles que décrites par le communiqué de presse de l'ART en date du 7 novembre 2002.[35] Elle a permis d'introduire 20 nouveaux départements.

Dans les départements libéralisés, anciennement au nombre de 58, il était possible d'utiliser un réseau local radioélectrique à l'intérieur des bâtiments avec une puissance isotrope rayonnée équivalente (PIRE) maximale de 100mW sur toute la bande de fréquences 2400-2483,5 MHz.

Ainsi, pour des installations radioélectriques émettant sur la bande de fréquences 2400-2446.5 MHz avec une PIRE maximale de 10 mW ou sur la bande de fréquences 2446,5-2483,5 MHz avec une puissance rayonnée inférieure ou égale à 100 mW utilisées à l'intérieur des bâtiments, le principe était celui de la liberté d'établissement.

Dans ces mêmes départements, pour une émission en extérieur, il fallait distinguer selon que la transmission avait lieu sur les fréquences 2400-2454 MHz ou sur les fréquences 2454-2483 MHz. Lorsque la transmission était faite sur les fréquences 2400-2454 MHz, la puissance maximale autorisée était de 100mW. Pour les communications transmises à l'aide des fréquences 2454-2483 MHz, la puissance maximale autorisée était de 10mW.

[35] Cf. communiqué de presse du 3 février 2003, <http://www.art-telecom.fr/>.

Plus clairement, dans ces 58 départements libéralisés, il était possible d'émettre à l'intérieur et à l'extérieur en utilisant la sous-bande 2400-2454 MHz avec une PIRE inférieure à 100mW, ceci, sans demander d'autorisation.

2. Les départements non libéralisés

Dans les départements non libéralisés en raison de la présence d'équipements militaires, l'utilisation de la bande de fréquence 2400-2446,5 MHz n'était pas autorisée à l'extérieur des bâtiments.

Une précision doit être faite. L'utilisation des fréquences 2400-2483,5 pour une PIRE limitée à 100 mW n'était pas totalement proscrite. Il fallait uniquement adresser une demande en vue de l'utilisation de ces fréquences pour la puissance indiquée. Cette demande pouvait être dans certains cas acceptée si l'installation ne gênait pas d'équipements militaires.

Inversement, il pouvait y avoir des exceptions d'établissements de réseaux sur la bande de fréquences 2400-2454 MHz dans l'un des 58 départements libéralisés. L'octroi de licence avait lieu au cas pas cas et le régime n'était pas parfaitement homogène.

Seuls quelques départements d'Outre mer étaient entièrement libéralisés.[36]

Des travaux de concertation ont été menés entre l'ART et le ministère de la Défense afin d'ouvrir totalement la bande 2400-2483,5 MHz avec une PIRE de 100 mW en intérieur et en extérieur à tous les départements.

B. La décision n° 03-908 de l'ART du 22 juillet 2003

Avec le nouveau régime, les seuls éléments à analyser pour l'établissement d'un RLAN concernent les sous-bandes de fréquences et la puissance d'émission des équipements.

La décision n° 03-908 abroge la décision n°02-1009 et libéralise l'ensemble des départements de l'Hexagone.

Comme auparavant, la bande de fréquences 2400-2483,5 MHz est dévolue à l'émission de signaux à une PIRE maximale de 100 mW, à l'intérieur des bâtiments. Sur la bande de fréquences 2400-2454 MHz, l'émission de communications est possible avec une PIRE de 100 mW. Sur la bande de fréquences 2454-2483,5 MHz, l'émission est limitée à une PIRE de 10 mW.

Les possibilités de brouillage des équipements militaires existent encore. C'est pour cela que les équipements utilisés doivent être conformes avec la réglementation nationale afin de respecter la PIRE.

[36] Il s'agissait de la Guadeloupe, de la Martinique, de Saint-Pierre et Miquelon et de Mayotte.

§ 3. La conformité des équipements à la réglementation nationale

La réglementation nationale se réfère à la norme ETSI à laquelle doivent se conformer les appareils reliés au réseau.

A. La normalisation des terminaux et bornes wi-fi à la norme ETSI

Bien que leur fourniture ait été libéralisée, les équipements terminaux de télécommunications font l'objet d'un contrôle de conformité. Ce contrôle est justifié par la nécessité de préserver les exigences essentielles nécessaires à la liberté de communication.
Sont concernés par ce contrôle de conformité, les équipements terminaux destinés à être connectés à un réseau ouvert au public, qu'il s'agisse d'une connexion directe ou indirecte. Il faut que ces équipements permettent par leur connexion au réseau ouvert au public, la transmission, le traitement ou la réception de l'information.

La connexion est indirecte lorsqu'elle s'effectue par le biais d'un autre réseau ou d'un autre terminal connecté au réseau ouvert au public. La plupart des équipements de communication sont concernés par la procédure de conformité, parmi lesquels les équipements terminaux radioélectriques.

L'attestation de conformité délivrée par un organisme désigné par l'ART vise à garantir que les équipements terminaux répondent à des spécificités permettant leur bon fonctionnement sans perturber les réseaux et les services.

Ces spécifications sont des exigences que des règlements techniques mettent en œuvre sous la forme de paramètres permettant d'évaluer la conformité de chaque type d'équipement aux exigences essentielles. Les attestations données par chaque autorité nationale sont reconnues mutuellement sur le territoire de l'Union Européenne lorsqu'elles sont délivrées par rapport à des normes européennes harmonisées.

En matière d'équipements utilisés pour la transmission de données sur la bande de fréquences de 2,4GHz, la conformité aux spécifications techniques se fait par comparaison aux normes définies par l'Institut Européen des normes de Télécommunication (ETSI). Pour l'élaboration de la liste de normes en vigueur dans l'Union Européenne, l'ETSI tient compte des normes internationales existantes afin de permettre un haut développement des réseaux de télécommunications européens.

La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local radioélectrique. Cette norme a été adoptée en considération du standard 802.11 élaboré par la " *Wireless Ethernet compatibility alliance* ".

Le nom " wi-fi " correspond à la certification donnée par la *Wireless Ethernet Compatibility Alliance* aux appareils utilisant la norme 802.11. Cet organisme est chargé

de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. A son niveau, l'ETSI promeut également le développement de la conformité des tests de spécification au standard 802.11 afin d'assurer l'interopérabilité des équipements et produits par les fabricants. Le test de spécification inclut à la fois un test radioélectrique et un test du protocole. Les tests de spécification sont menés conjointement par l'ETSI et par un consortium des plus grandes entreprises de technologies de communication afin d'affiner et d'améliorer le standard.

B. La procédure de conformité

La procédure d'attestation de conformité applicable en France s'inscrit désormais dans le cadre de la directive du Parlement européen et du Conseil du 9 mars 1999[37] transposée par l'ordonnance du 25 juillet 2001.[38]

Cette ordonnance a conduit à modifier l'article L 34-9 du code des postes et télécommunications relatif aux procédures d'évaluation de conformité des équipements terminaux.

Désormais la procédure d'agrément *a priori* des terminaux est substituée par une procédure *a posteriori*. Sont concernés par ces dispositions les modems, les cartes de connexion, les bornes radioélectriques. Ces équipements peuvent être mis librement sur le marché lorsqu'ils ont fait l'objet d'une évaluation interne dans les locaux de l'équipementier ou après avis d'un organisme notifié. L'attestation de conformité peut être retirée dès lors que les produits du fabricant ne respectent plus les spécificités techniques et réglementaires.

La conformité aux exigences essentielles définies par le droit communautaire, telles que la sécurité des usagers, le risque d'interférence, la protection des réseaux, l'utilisation optimale du spectre, est présumée acquise lorsque le fabricant déclare le terminal conforme aux normes européennes harmonisées.

La suppression de la procédure d'attestation de conformité *a priori* implique que le fabricant indique sur l'emballage des équipements concernés les quatre précisions suivantes : la destination d'usage, c'est-à-dire les réseaux et les pays pour lesquels l'équipement est utilisable, le marquage CE, le numéro d'organisme notifié (le cas échéant) et une signalétique d'avertissement dans le cas où il s'agit de fréquences non harmonisées.

Pour les équipements hertziens, l'attestation de conformité est délivrée après avis de l'Agence nationale des fréquences.

---

[37] Directive 1999/5/ CE relative aux équipements hertziens et aux équipements terminaux de télécommunications et à la reconnaissance mutuelle de leur conformité dite " RTTE ", 9 mars 1999, JOCE 7 avril 1999, n°91, p. 10.

[38] Ordonnance n° 2001-670 du 25 juillet 2001 portant adaptation au droit communautaire du code de la propriété intellectuelle et du code des postes et télécommunications, JO 28 juillet 2001, p 12132.

Une illustration peut être donnée concernant la signalétique d'avertissement dans le cas où il s'agit d'une fréquence non harmonisée. En France, où la bande de fréquences 2,4GHz n'est pas totalement libéralisée, le constructeur anglais qui livre sur le territoire national du matériel wi-fi avec la carte pré-installée doit décrire la procédure à suivre pour permettre l'utilisation de son matériel par un client français dans les conditions respectant la réglementation. Autrement, il s'expose aux sanctions de l'article L 39-1 du code des postes et télécommunications. Selon les dispositions de cet article, le fabricant qui met sur le marché un équipement qui n'a pas fait l'objet d'une procédure d'attestation de conformité ou/et qui ne décrit pas les caractéristiques du produit nécessaires à l'information de l'acheteur, commet un délit passible de six mois d'emprisonnement et de 30 000 euros d'amende.

Hormis ces normes techniques et réglementaires prises au niveau national, il existe des spécifications relatives aux interfaces des réseaux ouverts au public. Pour permettre à tout fabricant de fournir des équipements interopérables avec les interfaces du réseau ouvert au public, l'opérateur doit publier des spécifications suffisamment détaillées pour faciliter la conception de terminaux capables d'utiliser tous les services fournis par l'interface correspondante.

La modification des interfaces techniques au cours de l'exploitation du réseau, doit faire l'objet d'une publication afin de permettre aux usagers d'avoir des équipements adaptés à l'utilisation du réseau.

Section 2 - L'engagement de la responsabilité due à la négligence dans l'utilisation du réseau

L'utilisation de tout réseau suppose que certaines précautions soient prises pour garantir son fonctionnement. Une liste non exhaustive des attitudes contraires à l'utilisation du réseau lui-même (§ 1) et contraires à une gestion optimale de la ressource hertzienne pour les réseaux radioélectriques et plus particulièrement ceux émettant sur la bande de fréquences 2,4 GHz (§ 2), peut être dressée.

§ 1. Négligence quant à l'utilisation du réseau *stricto sensu*

Pour assurer l'utilisation optimale du réseau, les opérateurs et les utilisateurs doivent conserver la destination initiale du réseau (A), et se conformer aux impératifs d'intérêts publics visant à préserver son intégrité (B).

A. L'obligation de maintenir la destination du réseau

L'exigence de maintien de la destination du réseau concerne les réseaux radioélectriques indépendants. Sont visés les réseaux internes qui sont entièrement établis sur une même

propriété et n'empruntant pas le domaine public hertzien, et les réseaux à usage privé ou partagé.[39]

Il y a usage privé lorsque le réseau est réservé à l'usage exclusif de la personne physique ou morale qui l'établit. L'usage est qualifié de partagé lorsque l'usage du réseau est réservé à un groupe fermé d'utilisateurs (GFU) composé de personnes physiques ou morales qui échangent des communications internes au sein de ce groupe.[40]

A priori, cependant, seuls les réseaux indépendants empruntant le domaine public hertzien présentent des risques quant à la perte de leur destination. En effet, un réseau indépendant peut être connecté à un réseau ouvert au public filaire ou hertzien contrairement au réseau interne. Cette facilité est accordée après demande faite par l'utilisateur qui doit assurer que la connexion ne permettra pas l'échange de communications entre des personnes autres que celles auxquelles l'usage du réseau est réservé.

Lorsque le réseau indépendant offre la possibilité d'établir des communications entre des personnes autres que celles auxquelles l'usage du réseau est réservé, le réseau perd sa qualification de réseau indépendant pour celle de réseau ouvert au public. L'alinéa 5 de l'article L 33-2, dispose en effet " *qu'un exploitant de réseau ne peut conférer à son réseau le caractère de réseau ouvert au public* ".

Outre la mise en demeure de désinstaller le réseau, l'exploitant s'expose à des sanctions pénales de l'article L 39, 1°.

Comme il a été exposé, l'installation d'un réseau ouvert au public requérait l'octroi d'une licence préalable délivrée par l'ART dans les conditions de l'article L 33-1, mais n'est aujourd'hui soumise qu'à une déclaration préalable.

En matière de réseaux radioélectriques émettant sur la bande de fréquence 2,4 GHz, l'ART a spécifié que l'utilisation d'un réseau privé existant pour relier de bornes RLAN entre elles revient à transformer ce réseau en réseau ouvert au public. Ceci s'explique par le fait que le professionnel qui procède à une telle opération établit un nouveau maillage, à partir du réseau privé, pour permettre l'accès au réseau filaire.

Peut-on faire un parallèle avec le particulier qui installe une borne wi-fi émettant en extérieur en vue de partager son accès haut débit et considérer qu'il change la destination de son réseau privé ?

---

[39] Article L 32, 4°.

[40] L'ART milite en faveur de l'abandon de cette distinction qui, bien qu'ayant été reprise dans le projet de loi sur les communications électroniques, n'a plus lieu d'être. En effet, la distinction était faite afin de soumettre les réseaux à usage partagé à déclaration et au paiement de redevances. Mais le futur cadre réglementaire met fin à cette obligation de déclaration.

Selon le collège de l'ART, un tel raisonnement ne peut être tenu car un réseau constitue un maillage composé d'un ensemble de ressources de télécommunications.[41] Un simple particulier ne peut posséder à lui seul tous ces équipements. Par ailleurs, l'émission en extérieur n'implique pas une connexion au réseau ouvert au public hertzien.

Cette réponse peut cependant être contestée car le particulier est bien un maillon du réseau filaire ouvert au public et permet d'établir un lien entre ce réseau et le réseau hertzien lorsqu'il offre au public l'accès à sa connexion Internet.

De manière plus évidente, l'association wi-fiste de quartier, dont les adhérents offrent le partage de leur accès haut débit, peut être assimilée à un opérateur de réseau ouvert au public dès lors que cet accès a lieu sans identifiant de connexion et n'est pas réservé à ses membres.

Une autre hypothèse peut être envisagée dans le cadre d'un réseau communautaire permettant d'accéder à Internet. Le réseau est sécurisé et seuls les membres peuvent y accéder par un dispositif d'indentification.

Pour la connexion établie au niveau du réseau radioélectrique, il y a bien un réseau indépendant constitué par un groupe fermé d'utilisateurs.[42] Cependant, ces utilisateurs peuvent avoir accès au réseau filaire ouvert au public et communiquer avec des personnes non membres du réseau indépendant. Il est tentant de dire qu'un tel réseau est ouvert au public car il permet d'échanger des communications avec des personnes non membres du réseau communautaire.

Dans tous ces cas de figure, il est possible de soutenir qu'il y a bien un réseau hertzien ouvert au public. Il n'y a pas lieu en effet d'établir de distinction entre la nature du réseau auquel il est possible d'accéder par le biais d'un réseau radioélectrique.

Cette qualification peut être étayée par un argument de fait. Dès lors que, l'émission en extérieur est consciente et volontaire, il y a fourniture de service au public. Or l'article L 32, 3° qualifie de réseau ouvert au public " *tout réseau de télécommunication établi ou utilisé pour la fourniture au public de services de télécommunications*. "

L'ART n'a pas traité ce point. Elle se contente de renvoyer au contrat de fourniture d'accès à Internet passé avec le FAI. Cette position pourrait être justifiée par la volonté de développer l'installation de réseaux radioélectriques permettant l'accès au haut débit.

Sous l'ancien régime, ce raisonnement avait pour conséquence de faire dépendre l'établissement du réseau d'une autorisation préalable aux risques de sanctions pénales de l'article L 39-1 du CPT. Aujourd'hui, l'opérateur doit effectuer une déclaration. Ce régime

[41] Commutateurs, liens de transmission filaires et hertziens.
[42] Il doit être précisé que les réseaux indépendants " multi-GFU " sont considérés par l'ART comme des réseaux ouverts au public ; cf. e.g. avis n°03-552 de L'ART du 29 avril 2003 sur le projet de loi sur les communications électroniques.

est assoupli, mais l'absence de déclaration expose toujours à des sanctions pénales. La déclaration d'établissement d'un RLAN ouvert au public est une formalité impérative sanctionnée d'un an d'emprisonnement et de 75 000 euros d'amende.[43] Par ailleurs, l'opérateur doit respecter les obligations qui incombent à tout gestionnaire de réseaux ouverts au public notamment, les garanties de confidentialité et d'intégrité des communications.

La position de l'ART est louable et elle se situe dans l'esprit d'assouplissement du droit des télécommunications tel que le prévoit le projet de loi sur la communication électronique. Une position plus précise devrait être prise, d'une part, pour protéger les particuliers, et d'autre part, pour que l'accès au haut débit ait lieu par le développement de l'installation des bornes d'accès à Internet dans les lieux de passage public et s'intègre dans le cadre d'une politique de développement économique.

B. Les impératifs d'intérêt public : le maintien de l'intégrité du réseau

L'exigence de conservation de l'intégrité du réseau s'impose à l'opérateur exploitant du réseau, mais également aux opérateurs avec lesquels il a conclu une convention d'interconnexion, et avec les abonnés.

Lorsqu'une interconnexion avec un tiers porte gravement atteinte au bon fonctionnement du réseau de l'opérateur, ce dernier, après vérification technique de son réseau, en informe l'ART. Celle-ci peut autoriser, si cela est nécessaire, la suspension de l'interconnexion après en avoir informé les parties. Des conditions sont fixées pour rétablir le réseau.

Le réseau peut également être endommagé du fait de l'usager.

La libéralisation du marché des équipements terminaux a eu pour contrepartie de rendre responsable l'usager qui utilise un matériel non agréé connecté à un réseau ouvert au public. L'utilisateur supporte à l'égard de l'exploitant du réseau toutes les conséquences financières liées à l'utilisation d'un matériel non conforme.[44] Cette responsabilité de l'usager a été confirmée par une réponse écrite d'un sénateur concernant les cas de piratage de lignes téléphoniques portant sur des postes sans fil non agréés :

" *Les cas de " piratage " de lignes téléphoniques auxquels il est fait allusion portent exclusivement sur des postes sans fil non agrées dépourvus de code de sécurité. Or l'article L 34-9 de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications stipule que les " équipements terminaux sont fournis librement " et que " lorsqu'ils sont destinés à être connectés à un réseau ouvert au public, ils doivent faire l'objet d'un agrément délivré par le ministre chargé des télécommunications ". Par*

[43] Article 19 du projet de loi modifiant l'article 39.
[44] TI Paris, 7 janvier 1993 Delaunay c/ France Télécom, RJ P&T1993, n° 31.

ailleurs, le décret n° 92-116 du 4 février 1992 interdit la vente et l'utilisation de matériels non agréés ".[45]

Par analogie, on peut appliquer cette jurisprudence à l'hypothèse où un utilisateur s'équipe de matériels wi-fi non conformes aux spécificités nationales relatives à la puissance et à l'utilisation des fréquences, et qu'il commet des dommages sur un réseau ouvert au public filaire ou hertzien. Dans un tel cas, l'ART peut sans préjudice d'éventuelles sanctions pénales prévues à l'article L.39-1 du code des postes et télécommunications, demander à l'opérateur du réseau auquel sont irrégulièrement connectés ces terminaux, de suspendre la fourniture du service à l'utilisateur des équipements concernés. Ceci *a fortiori* lorsque les équipements ont occasionné un dommage grave ou des perturbations radioélectriques, ou une atteinte à son fonctionnement.

Il peut arriver que des terminaux ayant fait l'objet d'une procédure d'évaluation de conformité causent des dommages au réseau ouvert au public. Dans ce cas, il est mis en œuvre une procédure de notification de l'opérateur à l'ART, puis de l'ART à l'utilisateur, afin qu'il soit mis fin aux perturbations dans un délai déterminé. Si à l'expiration de ce délai l'utilisateur ne s'est pas conformé à la mise en demeure, sur demande de l'ART, l'opérateur suspend la fourniture du service qui utilise les terminaux à l'origine des perturbations.

Lorsque le dommage causé est très grave, l'opérateur peut prendre l'initiative de déconnecter les terminaux de l'utilisateur sans délai et en informe l'ART.

Ces mesures sont imposées par le respect des exigences essentielles. Dans l'énumération de l'article L 32, 12° du code des postes et télécommunications, il est fait mention de " *la protection des réseaux et notamment des échanges d'informations de commande et de gestion qui y sont associés* ".

Ceci est justifié par le fait que le réseau est le vecteur de la communication et que toute atteinte portée à son intégrité rejaillit sur la liberté fondamentale de communication des abonnés.

L'acquéreur du matériel défectueux pourra se retourner contre le fabricant des équipements sur le fondement des articles 1386-1 et 1386-2 du code civil.[46]

Hormis la préservation de l'intégrité, l'utilisation du vecteur de communication doit " *garantir dans l'intérêt général la santé publique et la sécurité des personnes* ". La préservation de cette garantie peut, en matière de réseaux radioélectriques, être réalisée par une gestion optimale des fréquences.

---

[45] Réponses ministérielles à questions écrites Rép. Min. à QE, JO Sénat Q. 29 mars 1993, p.601s.

[46] Loi n°98-389 du 19 mai 1998 de transposition de la directive CE n°85/374 du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, et réglementaires et administratives des Etats membres en matière de responsabilité du fait des produits défectueux.

§ 2. Négligence dans l'utilisation optimale des fréquences

La ressource hertzienne impose que l'on prenne des précautions relatives à la santé publique et à l'intégrité des personnes (A) et à la qualité d'émission des autres appareils radioélectriques (B).

A. La protection de l'intégrité des personnes

Les antennes wi-fi rayonnent avec une puissance maximale de 100mW, très inférieure par exemple aux antennes GSM dont la puissance, elle-même relativement faible par rapport à d'autres sources d'émission radioélectrique, est de l'ordre de quelques dizaines de watts.

Il y a donc peu d'inquiétude pour ce qui est des risques du wi-fi sur la santé publique. Cependant, il faut rester vigilant et respecter les valeurs limites que ne doivent pas dépasser les champs électromagnétiques émis par les équipements utilisés dans les réseaux de télécommunications.

Par ailleurs, il faut veiller à ce que les bornes et antennes soient installées de manière à ne causer aucun préjudice physique corporel de nature à engager la responsabilité de leur propriétaire sur la base des articles 1382 et 1384 alinéa 1 du code civil sans exclure d'éventuelles sanctions prises par l'Autorité au titre de l'article L 36-11. Très souvent les antennes radioélectriques sont placées sur des toits en hauteur. Une fixation artisanale pourrait faciliter la chute de l'antenne sur un passant.

L'article 1384, alinéa 1 du code civil pose une présomption simple de responsabilité du fait des choses. Cependant, les conditions des trois causes exonératoires de responsabilité sont difficiles à réunir. Il faut que le gardien de la chose prouve "*qu'il a été mis dans l'impossibilité d'éviter le dommage sous l'effet d'une cause étrangère qui ne lui est pas imputable*".[47] Est qualifiée de cause étrangère l'événement imprévisible, irrésistible et extérieur au gardien de la chose. L'imprévisibilité et l'irrésistibilité rendent l'événement inévitable. L'extériorité est le caractère qui rend l'événement insurmontable car étranger à la chose elle-même et au gardien. Trois exemples recouvrent ces conditions cumulatives. Ce sont, la force majeure, la faute ou le fait de la victime et enfin la faute ou le fait d'un tiers.

Appliqués à l'exemple proposé, aucun des critères n'est réuni étant donné que l'installation artisanale est faite par le propriétaire ou pour son compte.

La responsabilité pénale du propriétaire peut également être recherchée pour manquement à une obligation de sécurité imposée par la loi ayant causé directement le dommage.[48] En l'espèce, l'obligation de sécurité est contenue dans les dispositions de l'article L 32 du CPT qui inclut parmi les exigences essentielles, la santé et la sécurité des personnes. Il est

[47] Voir par exemple Civ. 2ème 24 mars 1984, Bull. civ. II, n°70.
[48] Article 121-3 alinéa 3 du code pénal.

cependant plus fréquent que le propriétaire d'équipements radioélectriques de faible puissance soit responsable des perturbations causées à d'autres appareils.

B. Les risques de brouillages des fréquences

Les ondes radioélectriques sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut être aisément brouillé par une émission radioélectrique ayant une fréquence proche de celle utilisée dans le réseau sans fil. Un four à micro-ondes peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

Il s'est ainsi avéré nécessaire de régir le spectre hertzien au niveau international au sein de l'Union internationale des télécommunications (UIT, organe des Nations Unies). L'UIT a élaboré un règlement de radiocommunication qui a pour visée de permettre l'accès équitable au spectre hertzien, de prévenir et résoudre les cas de brouillage et de permettre une exploitation efficace des services de radiocommunication.

Les Etats membres sont chargés au niveau national de mettre en œuvre cette réglementation. En France, l'utilisation du spectre hertzien est régie par le tableau national de répartition des bandes de fréquence (TNRBF) élaboré par l'Agence nationale des fréquences qui met en œuvre le règlement de l'UIT. Le TNRBF organise un régime d'autorisation et un régime d'utilisation de plein droit des bandes de fréquences.

La bande de fréquences 2400-2483,5 MHz fait partie des bandes dont l'utilisation est libre pour certains appareils radioélectriques. Cette bande a été libéralisée dans de nombreux pays car elle est utilisée pour des applications industrielles, scientifiques et médicales autres que de radiocommunications[49]. Ceci a permis de développer des équipements grand public à faible coût pour l'établissement de réseaux locaux à l'intérieur des bâtiments.Ces équipements ont par la suite été développés pour permettre le déploiement de réseaux radioélectriques émettant en extérieur.

En France, malgré le régime d'utilisation de plein droit de la bande 2,4 GHZ, des conditions d'utilisation ont été fixées par l'ART dans les décisions n° 02-1008 et n° 02-1009. Ces décisions visaient à limiter la puissance d'émission des appareils afin d'éviter des brouillages avec les autres utilisations qui sont mises en œuvre sur cette bande de fréquences et sur les bandes voisines. En effet, dans les fréquences utilisables de plein droit, le nombre d'utilisateurs et leur position géographique est totalement libre. Si ces utilisateurs sont très nombreux, il y a des risques d'interférences mutuelles.

Or, l'article L 39-1, 2° incrimine le fait " *de perturber, en utilisant une fréquence, un équipement ou une installation radioélectrique, dans des conditions non conformes aux dispositions de l'article L 34-9 ou sans posséder l'autorisation prévue à l'article L 89 ou en dehors des conditions réglementaires générales prévues à l'article L 33-3, les émissions*

[49] Comme exemple d'application ISM il y a les appareils domestiques ménagers tels le four micro-ondes.

hertziennes d'un service autorisé, sans préjudice de l'application de l'article 78 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication ".

L'un des reproches fait à l'association *Provence Wireless*, concernait le brouillage d'équipements radioélectriques.[50] Ceci a conduit à l'injonction de désinstaller le réseau.

La décision n° 02-1008 l'ART spécifie de surcroît à l'article 3 que, " *les installations radioélectriques visées par la présente décision fonctionnent sur une base de non brouillage et sans garantie de protection* ". Par conséquent, l'utilisateur ne doit pas occasionner de gêne à d'autres utilisateurs autorisés. Par exemple, l'utilisateur ne doit pas perturber les radars de la Défense nationale qui sont installés sur les fréquences 2450-2500 MHz.

Par ailleurs, la garantie de non-brouillage induit que l'utilisateur ne bénéficie pas de la garantie de disponibilité des fréquences. Ainsi, il peut lui être demandé de désinstaller ses bornes et équipements wi-fi.

L'acquéreur de bonne foi dispose, lorsqu'il apparaît immédiatement après la vente que la borne est trop puissante, d'une garantie des vices cachés qui rendent l'équipement impropre à l'usage auquel il était convenu, prévue à l'article 1641 du code civil. Les vices qui sont garantis ne sont que ceux qui ne sont pas apparents au moment de l'achat. Ceci est le cas de la puissance d'émission hertzienne d'une antenne, si le vendeur ne procède à aucun test en magasin.

Le contenu circulant sur le réseau peut également être source de responsabilité.

[50] Mane est un village de 1300 habitants situé à Forcalquier dans les Alpes du Sud (04). Des équipements militaires doivent sans doute être présents dans ce département qui n'est pas compris dans la liste des 58 départements libéralisés.

Chapitre II - Le contenu transitant sur le réseau source de responsabilité

Les RLAN permettent la transmission de contenus destinés à la correspondance privée ou publique, un même réseau pouvant réunir ces deux types de données. Les opérateurs ont des obligations garantissant l'intégrité des données, afin de préserver la liberté de communication. Ceci est particulièrement visible pour la correspondance privée, que le législateur protège contre tout risque d'atteintes. Or, en matière de wi-fi, ces atteintes sont exacerbées à cause de la vulnérabilité de la norme qui facilité l'accès aux données transmises par les ondes radioélectriques (section 1).

Concernant la correspondance publique, il est tentant de procéder pour les données de cette nature comme la jurisprudence l'a fait pour les données circulant sur le réseau Internet. Cependant, la nouvelle notion de " *communication électronique* " et les réticences de l'Autorité de régulation conduisent à rechercher un régime au contenu de la correspondance publique transmis sur les réseaux wi-fi (section 2).

Section 1 – Wi-fi et accès aux correspondances privées

La norme wi-fi illustre les risques que représentent les systèmes de communications à l'égard de la vie privée des personnes. En effet, cette nouvelle norme de télécommunications utilise un réseau radioélectrique. Or, de tels réseaux sont par défaut non sécurisés et les communications transmises sont aisément captables et altérables par brouillage. La norme 802.11 présente certes des garanties par rapport aux autres réseaux sans fil mais elle reste vulnérable (§ 1). La vulnérabilité est un frein au développement du wi-fi pour les communications privées.

Elle facilite en effet les atteintes qui peuvent être portées aux personnes et aux systèmes de télécommunications (§ 2).

Des solutions existent néanmoins en amont et en aval sous la forme de mesures techniques de protection et de mécanismes juridiques de responsabilité (§ 3).

§ 1. Exposé des failles techniques du wi-fi

Le réseau wi-fi est vulnérable car étant un réseau radioélectrique, il ne permet d'assurer ni la confidentialité des communications, ni l'authentification, ni l'intégrité des données.

A. L'absence de confidentialité

Etant basé sur un protocole d'émission radioélectrique, le wi-fi propage une émission vers tous les récepteurs qui sont aux alentours. Les informations émises peuvent ainsi être captées par un tiers muni d'un récepteur et d'une antenne placés dans le volume d'émission.

Ce type d'attaque qualifiée de " *parking lot attack* " permet à un pirate équipé d'une carte IEEE 802.11b de se connecter au réseau intranet d'une entreprise ou d'un particulier en stationnant à proximité des lieux.

En effet, le plus souvent, la portée d'émission dépasse plus ou moins largement les locaux dans lesquels est placée l'antenne d'émission.

De plus, ce périmètre peut-être mal configuré par défaut, et le réseau sera visible de l'extérieur des bâtiments.

B. La faiblesse de l'authentification et du contrôle d'accès

La fragilité du wi-fi s'illustre dans la faiblesse du protocole WEP permettant l'authentification des clients (1) et assurant l'accès au réseau (2).

1. La faiblesse de l'authentification

Le WEP, pour ***Wired Equivalent Privacy***, est un protocole chargé du chiffrement des trames 802.11 à l'aide de l'algorithme RC4 qui utilise des clés de 40 ou 104 bits. Ses faiblesses se situent au niveau du chiffrement des clés dont la gestion est lourde.

a. La rigidité de la clé de chiffrement générée par le protocole WEP

Le flux de données échangées entre des machines utilisant le protocole 802.11 est non encrypté. La trame composée par ses données contient trois groupes d'éléments parmi lesquels un code appelé " *cyclic redundancy code* " ou CRC. Ce code de quatre octets permet d'assurer l'intégrité des informations.

L'intégrité des données est préservée, cependant, elles ne sont pas chiffrées mais en clair.

Le principe du WEP consiste à définir dans un premier temps une clé secrète qui est déclarée au niveau du point d'accès et des clients. La clé sert à créer un nombre pseudo-aléatoire d'une longueur égale à la longueur de la trame. Chaque transmission de donnée est ainsi chiffrée en utilisant le nombre pseudo-aléatoire.

Pourtant, il est aisé de retrouver la clé de chiffrement à l'aide de logiciels présents sur Internet permettant de générer des clés aléatoires, parce que la clé de session partagée par toutes les stations est statique. C'est-à-dire que pour déployer un grand nombre de stations wi-fi il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications.

b. La lourdeur de la gestion des clés

Il se pose également le problème de la gestion des clés. Une seule et même clé est partagée par tous les utilisateurs. Cette clé est stockée sur un équipement mobile (fichier ou

adaptateur) qui est exposé. Si un utilisateur la perd, il faut la remplacer par une autre sur tous les équipements, ce qui est contraignant.

Les risques sont d'autant plus importants qu'il est possible d'installer des points d'accès à l'intérieur d'un périmètre protégé, à l'insu de l'administrateur du réseau filaire. Ainsi, à l'intérieur d'une entreprise, un employé malveillant peut brancher un point d'accès sur une prise réseau pour rendre publiques les communications du réseau.[51]

2. La faiblesse du contrôle d'accès

Il y a deux moyens de contrôler l'accès à un réseau wi-fi, soit on utilise un identifiant (SSID[52]), soit par l'adresse MAC.

a. L'absence de confidentialité de l'identifiant SSID

S'agissant de l'identifiant, il n'est pas en principe chiffré lors de la transmission des trames. Non seulement il est laissé à la valeur par défaut du constructeur mais, de surcroît, il est annoncé à chaque connexion aux points d'accès.

En effet, lors de l'entrée d'une station dans une cellule, cette dernière diffuse sur chaque canal une requête de sondage *(probe request*) contenant l'ESSID[53] pour lequel elle est configurée, ainsi que les débits que son adaptateur supporte. Si aucun ESSID n'est configuré, la station écoute le réseau à la recherche d'un SSID parce que chaque point d'accès diffuse régulièrement une trame balise (*beacon*) donnant les informations sur son BSSID[54] ses caractéristiques et son ESSID qui est diffusé par défaut.

Selon les explications de Pascal Urien,[55] le processus d'authentification a lieu de la manière suivante : un point d'accès (AP) émet périodiquement une trame. Une station qui désire rejoindre le réseau émet une demande d'entrée accordée par le point d'accès.

Après cette opération, la station s'authentifie auprès du réseau grâce à un scénario en quatre étapes :

- la station transmet une requête d'authentification (*authentification request*),
- le point d'accès produit un challenge (*authentification challenge*) de 128 octets en clair,
- la station encode les 128 octets à l'aide d'une trame WEP (*authentification response*) associée à un champ IV de 24 bits et une clé d'identification de 2 bits et enfin,

[51] Cf. en ce sens Christian Claveleira, ingénieur au Comité réseaux des Universités in *Sécurité informatique,* n° 40 juin 2002, <http://www.cnrs.fr/Infosecu/num40-sansFond.pdf>.
[52] SSID abréviation de Service Set Identifier.
[53] ESSID abréviation de Extend Service Set Identifier.
[54] BSSID abréviation de Basic service set identifier.
[55] Interview de Pascal Urien (Schlumberger Sema) mené par Robert Longeon du journal du CNRS *Sécurité informatique,* juin 2002 n°40, <http://www.cnrs.fr/Infosecu/num40-sansFond.pdf >.

- le point d'accès notifie l'échec ou la réussite de l'opération (*authentification result*).

Un utilisateur mal intentionné qui écoute le réseau peut obtenir le SSID lui permettant ainsi un accès au réseau. En effet, il est aisé de déduire du message en clair et du message chiffré les 128 premiers octets de la clé générés à partir du vecteur IV et de la clé d'identification.

De plus, l'interprétation du SSID sur le réseau est souvent facilitée par le fait que le SSID porte le nom du service ou de l'organisme utilisateur du réseau.

Il est donc aisé d'obtenir l'ESSID d'une cellule en restant à l'écoute du réseau.

c. La production de fausses adresses MAC

Le contrôle d'accès peut également se faire par adresse MAC, c'est-à-dire par identification de la carte d'accès wi-fi du poste mobile.[56] La carte d'accès ou adaptateur est une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Ce contrôle peut être cumulé avec la vérification de l'identifiant.

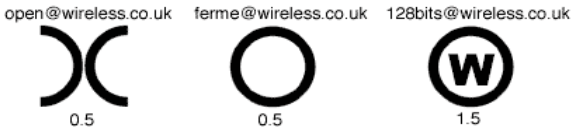
L'administrateur peut établir une liste de contrôle (liste ACL) d'accès énumérant les adresses physiques des cartes wi-fi autorisées à accéder au réseau. Mais ce contrôle est également facilement contournable car la plupart des adaptateurs permettent de modifier leur adresse. Par ailleurs il est fastidieux d'établir une liste de contrôle d'accès dans les grandes entreprises.

La pratique du *war-driving* et du *war-Xing* ou *war-crossing* est ainsi apparue aux Etats-Unis. Il s'agit, à l'aide d'un ordinateur portable équipé d'une carte réseau sans fils, de repérer parmi ces réseaux ceux qui ne sont pas sécurisés. Ceci a pour première visée d'établir une cartographie des points d'accès à Internet[57] afin de bénéficier gratuitement d'accès au réseau filaire. Cette pratique qui à l'origine n'était pas motivée par de mauvaises intentions, bénéficie néanmoins aux pirates. Ces derniers peuvent par exemple, par le biais du réseau filaire d'une entreprise, accéder à Internet afin de mener des attaques.

---

[56] En anglais, *wireless adapters* ou *network interface control* noté NIC.

[57] Pour rendre visible la présence d'un réseau radioélectrique les adeptes ont utilisé des symboles dessinés à la craie sur le trottoir (*war chalking*) permettant d'indiquer la nature du réseau. Il y a trois symboles : deux demi-cercles dos à dos désignent un réseau ouvert offrant un accès à Internet, un cercle désigne un réseau sans fil sans accès à Internet et un W encerclé signale un réseau correctement sécurisé. Au dessus du symbole sont inscrits, l'identifiant du nœud ou le moyen de contacter son propriétaire et en dessous, la bande passante utilisée. Cette pratique londonienne a été importée en France sous le nom de craie-fiti (cf e.g <http://www.wifi-montauban.net>).



Etant donné qu'il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise installatrice du réseau wi-fi peut voir sa responsabilité engagée au titre de l'attaque.

Le standard 802.11 intègre certes un mécanisme de chiffrement des données, le WEP (*wired equivalent privacy*) censé rendre le réseau plus sûr que les autres réseaux sans fils. Pourtant, celui-ci reste vulnérable.

C. L'intégrité des informations

Le protocole 802.11 intègre un code de 4 octets (*cyclic redundancy code*) censé assurer l'intégrité des données. Cependant, le ou exclusif (octets à octets) de deux trames de même longueur est associé à un CRC obtenu par un ou exclusif des deux autres CRC. A partir d'une trame en clair et de son CRC, il est donc possible de modifier une trame chiffrée tout en recalculant un CRC correct. Le protocole n'assure nullement l'intégrité des données.

D. La disponibilité des services, les dénis de service

La sensibilité au brouillage est une autre vulnérabilité induite par la technologie des réseaux sans fil. Elle peut entraîner un déni de service des équipements du réseau, voire la destruction de ces équipements dans le cas de bruit généré artificiellement.

La norme 802.11 est basée sur le protocole CSMA pour *Carrier Sense Multiple Access with Collision Avoidance*. Ce protocole, par similitude au protocole utilisé sur les réseaux filaires,[58] met en place un mécanisme d'esquive de collision à l'aide d'un principe d'accusé réception réciproque entre la station émettrice et le récepteur. L'accès au réseau est subordonné à l'absence d'émission par une station tierce.[59]

Une fois la connexion établie, la station doit s'associer au point d'accès afin de pouvoir lui envoyer des paquets de données.

Un pirate maîtrisant les conditions d'accès et d'association peut demander la " désassociation " de la station en envoyant des informations afin de perturber volontairement le fonctionnement du réseau sans fil.

Une autre forme d'indisponibilité des services est envisageable en provoquant un engorgement du réseau, par l'envoi d'un grand nombre de donnés à une machine afin de la surcharger et provoquer ainsi l'encombrement du réseau à distance.

---

[58] Sur un réseau filaire avant d'émettre un message la machine vérifie qu'aucun message n'est en train d'être émis par une autre machine. Auquel cas elle attend avant d'émettre. Ceci est permis grâce au protocole CSMA/CD pour *carrier sense multiple access with collision detect*.

[59] Ceci résout l'inconvénient des réseaux sans fil sur lesquels les stations communiquant avec un récepteur ne s'entendent pas à cause de leur portée d'émission. La station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé *DIFS* pour *Distributed Inter Frame Space*), alors la station peut émettre.

Le dernier risque tient plus à l'essor de cette technologie qu'à la technologie elle-même. Il concerne la méconnaissance des utilisateurs vis-à-vis de leur équipement. Par exemple, Windows XP intègre par défaut la gestion des cartes sans fil, si l'ordinateur portable d'un utilisateur possède un équipement sans fil alors, cet ordinateur sera par défaut prêt à communiquer sur le réseau.

§ 2. Exposé des trois garanties de la liberté de communication

Parce que la correspondance est une composante de la personnalité en ce qu'elle permet la vie relationnelle, des principes ont été érigés afin de garantir la liberté de communication.

Le respect de ces principes est soit mis à la charge des seuls professionnels exerçant une activité de télécommunications, c'est le cas des nécessaires neutralité et sécurité (A, B) des réseaux, soit cette obligation est générale et s'impose à tous. Il s'agit du devoir de respect du secret des correspondances (C).

A. La neutralité du réseau

L'obligation de neutralité mise à la charge des opérateurs leur interdit de faire une distinction entre le contenu des messages véhiculés. Ils doivent à ce titre effectuer la transmission de tous les messages. Ce principe est contenu dans l'article L 32-1 II 5° du code des postes et télécommunications qui confie au ministre des télécommunications et à l'ART le soin de veiller au respect du " *principe de neutralité au regard du contenu des messages transmis* ". La notion de " *messages transmis* " s'entend de tous messages privés ou transmis au public. En matière de wi-fi, cette obligation ne sera assumée que par les opérateurs de réseaux ouverts au public sur lesquels transitent des données émises provenant de réseaux ouverts au public ou de réseaux indépendants. Mais le principe de neutralité n'a pas vocation à s'appliquer aux opérateurs de réseaux indépendants. Ces derniers ne sont pas destinés à permettre des communications entre des personnes n'appartenant pas au groupe fermé d'utilisateurs. En revanche, l'obligation de garantir l'accès aux données vaut pour tout type de réseau.

B. La garantie de sécurité d'accès aux données

L'accès aux données est sûr lorsque le réseau et les systèmes de traitement de ces données sont sécurisés.

1. L'obligation de sécuriser le réseau

Parmi les exigences essentielles, l'article L 32, 12° impose à l'opérateur d'assurer " *la protection des réseaux et notamment des échanges d'informations de commande et de gestion qui y sont associés* ".

L'opérateur doit à ce titre se conformer aux prescriptions techniques en matière de sécurité édictées par l'ART. Un contrôle est exercé par l'ART qui peut demander la communication des dispositifs de sécurité mis en œuvre par l'opérateur.

Les dispositifs de sécurisation du réseau doivent non seulement exister au moment de l'établissement du réseau, mais l'opérateur doit également s'assurer de leur efficacité tout au long de l'exploitation du réseau eu égard aux avancées techniques. Cette obligation est doublée d'une obligation d'information et de conseil vis-à-vis des utilisateurs. En effet, l'opérateur doit d'une part, informer ses clients des services existant pour renforcer la sécurisation des communications et d'autre part, informer ses clients des risques particuliers de violation de la sécurité du réseau et des moyens éventuels d'y remédier.

La garantie de sécurité du réseau est un gage de l'exploitation du réseau lui-même car les usagers sont assurés que les données qui y circulent conserveront leur intégrité.

L'exposé de ce principe devrait rassurer les acteurs des RLAN. Cependant, dans les faits cette obligation ne joue pas pleinement car l'ART semble considérer que l'obligation de sécurité, bien qu'étant une composante des exigences essentielles, n'est qu'un but à atteindre. Les exigences essentielles n'ont pas pour objet premier de se rapporter à la sécurisation des réseaux de télécommunication. Sans pour autant être exonératrice, cette interprétation a pour conséquence d'alléger les exigences de sécurité mises à la charge des opérateurs. Nombreux sont ceux qui s'en affranchissent par le biais des dispositions contractuelles. Ceci n'est pas en faveur du développement des RLAN.

2. La sécurisation du traitement des données

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,[60] impose également en matière de traitement d'informations nominatives une obligation de sécurité qui vient parfaire l'obligation de déclaration préalable à la CNIL. L'une et l'autre de ces obligations ont pour but de garantir le respect de la vie privée. L'obligation de sécurité dans le traitement des informations vise plus précisément à assurer la confidentialité des données à caractère personnel. Ainsi, l'article 29 de la loi dispose que :

[60] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O. 7 janvier 1978 ; Foruminternet.org, <http://www.foruminternet.org/documents/lois/lire.phtml?id=10>.

" *Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés* ".

Il s'agit d'une obligation générale de sécurité à la charge de toute personne responsable d'un traitement informatique de fichiers nominatifs.

La CNIL a adopté une recommandation le 21 juillet 1981, où elle précise à l'intention des maîtres de fichiers, le degré d'efficacité des mesures de sécurité physiques comme logiques. Ces mesures de sécurité doivent préserver l'intégrité de l'information et être capables de résister aux atteintes accidentelles ou volontaires[61].

Les atteintes volontaires qui sont les préoccupations essentielles en matière de réseau hertzien sont " *celles qui visent à la destruction totale ou partielle des installations, celles qui ont pour objet le vol ou l'altération des logiciels, le détournement, l'altération ou la destruction d'informations.* "

Les recommandations de la CNIL n'ont aucune valeur contraignante, cependant, les maîtres de fichiers sont invités à renouveler les mesures de sécurité afin qu'elles soient en conformité avec les évolutions techniques.

Dans un communiqué en date du 14 mars 2003, la CNIL a émis des réserves relatives à l'utilisation des équipements et réseaux wi-fi pour le traitement des informations. Elle recommande aux utilisateurs et aux professionnels la mise en œuvre de mesures de sécurité préalablement à toute installation et utilisation du réseau wi-fi pour prévenir les atteintes qui pourraient être portées au secret des correspondances.[62]

C. Le secret des correspondances

Depuis la loi du 10 juillet 1991[63] qui correspond à une mise en forme de la jurisprudence de la Cour européenne des droits de l'homme,[64] le principe du secret des correspondances englobe la correspondance postale comme la correspondance émise par la voie des télécommunications dès lors qu'elle est privée. Le caractère privé de la correspondance suppose deux conditions cumulatives. Il faut d'une part que le message émis soit exclusivement destiné à une ou plusieurs personnes déterminées et individualisées.

---

[61] Délibération n°81-094 du 21 juillet 1981 portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes informatiques, JO 24-25 août 1981.

[62] <http://www.cnil.fr/thematic/index.htm>.

[63] Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

[64] Arrêt Klass du 6 septembre 1978 relatif aux interceptions des correspondances pour sécurité et les arrêts Krusling et Huvig du 24 avril 1990 pour les interceptions ordonnées par l'autorité judiciaire.

Lorsqu'il y a plusieurs destinataires, ces personnes doivent être liées par une communauté d'intérêt. D'autre part, il faut que le contenu du message témoigne du lien qui unit l'émetteur avec le ou les destinataires.

La question s'est posée de savoir si le courrier électronique pouvait être qualifié de correspondance privée. Le tribunal correctionnel de Paris, dans un jugement du 2 novembre 2000, a répondu par l'affirmative en considérant que l'envoi de messages électroniques de personne à personne constitue de la correspondance privée, protégée par la loi dès lors que le contenu qu'elle véhicule est exclusivement destiné à une personne déterminée.[65] La loi du 10 juillet 1990 s'applique à tout type de correspondance privée de la vie courante ou relative aux affaires, et quel que soit le mode de communication.

Il existe deux situations dans lesquelles le réseau radioélectrique permet d'échanger de la correspondance privée. Soit la correspondance a lieu directement entre deux ou plusieurs ordinateurs mobiles qui se transmettent des données par le biais des ondes radioélectriques en se connectant les uns aux autres. On parle d'architecture *ad hoc*. Soit la correspondance est indirecte, et elle prend la forme de courrier et de données échangées par Internet. L'utilisation de l'une ou l'autre de ces situations peut se faire aussi bien dans le cadre professionnel que privé.

Pour qu'un tiers puisse prendre connaissance de leur contenu, il faut qu'il soit dans l'alternative de la préservation des intérêts de l'Etat et de la commission rogatoire dans le cadre d'une enquête judiciaire. Il s'agit d'exceptions strictes.

Un tiers à la correspondance peut cependant être tenté de contrôler le contenu des messages transmis. Cette situation se retrouve particulièrement dans le cadre des relations de travail. Il en va ainsi par exemple de l'employeur qui a limité l'usage de la messagerie à des fins professionnelles et qui souhaite s'assurer du respect de l'interdiction, ou bien encore de l'employeur qui a des doutes sur la fidélité de son salarié.

La jurisprudence s'est prononcée sur le contrôle de l'usage de la messagerie électronique dans l'entreprise. La transparence et la proportionnalité sont les deux principes directeurs auxquels est subordonnée la surveillance du salarié par l'employeur.

La surveillance est admise lorsqu'elle respecte les principes cumulatifs posés par le code du travail. L'article L 121-8 prévoit qu'aucune information concernant personnellement le salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance. L'article L 432-1 et L 432-2 du même code soumet à information et consultation préalable du comité d'entreprise tout projet de mise en œuvre de moyens et techniques permettant de contrôler l'activité des salariés. L'ensemble de ces dispositifs doit être pris sans restreindre de manière injustifiée et non proportionnée les droits des personnes et les libertés individuelles et collectives (article L 120-2 du code du travail). A défaut, les preuves collectées contre le salarié ne peuvent être produites dans une action en

[65] TGI de Paris, 17ème chambre correctionnelle, 2 novembre 2000, *JCPE* 2002, chronique n°36, observations Bruguière et Vivant.

justice, et de surcroît, l'employeur se rend coupable d'atteinte au secret des correspondances et à la vie privée.

Après plusieurs hésitations doctrinales et jurisprudentielles, c'est ainsi qu'en a décidé la Cour de cassation dans l'arrêt Nikon du 2 octobre 2001.[66]

Il est cependant admis que l'administrateur chargé du fonctionnement et de la sécurité du réseau, puisse avoir accès aux messageries et à leur contenu pour prévenir des attaques. Cependant, il ne peut divulguer le contenu des messages.

Le wi-fi permettant la transmission de messages électroniques via Internet, les solutions élaborées viennent à s'appliquer.

Une autre forme de contrôle des correspondances est imaginable sur le réseau radioélectrique interne à l'entreprise. L'employeur peut installer un ordinateur " contremaître " chargé de veiller sur les tâches des salariés et les messages transmis en architecture *ad hoc*, en se réservant la possibilité de prendre connaissance du contenu des messages transmis.

Ici encore, l'installation d'un tel dispositif doit se faire dans le respect des dispositions réglementaires pour que les preuves constituées contre le salarié soient recevables en justice.

§ 3. Les solutions techniques et juridiques de consolidation du réseau

Face aux risques que présente la norme wi-fi et aux nécessités de garantir la vie privée, il est nécessaire de déployer des solutions techniques de protection (A). Le droit reste cependant prêt à intervenir lorsque ces solutions révèlent leur limite (B).

---

[66] C. cass. 2 octobre 2001: " *Vu l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, l'article 9 du Code civil, l'article 9 du nouveau Code de procédure civile et l'article L. 120-2 du Code du travail ; Attendu que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ; Attendu que pour décider que le licenciement de M. Onof était justifié par une faute grave, la cour d'appel a notamment retenu que le salarié avait entretenu pendant ses heures de travail une activité parallèle ; qu'elle s'est fondée pour établir ce comportement sur le contenu de messages émis et reçus par le salarié, que l'employeur avait découverts en consultant l'ordinateur mis à la disposition de M. Onof par la société et comportant un fichier intitulé " personnel " ; Qu'en statuant ainsi, la cour d'appel a violé les textes susvisés* ". Dalloz 2001 jurisprudence p. 148 note P-Y. Gautier

A. Les mesures préventives de protection : les dispositifs techniques

Le degré de sécurisation du réseau dépendra de l'utilisation qui est faite du réseau. Si elle est limitée à la consultation d'Internet ou à la visualisation de films, il n'est pas surprenant que l'utilisateur tolère que quiconque ait accès aux données transmises. Et même s'il effectue des achats électroniques, ces transactions étant protégées par la technologie SSL (*secure socket layer*), il y a peu de risque.

Cependant, lorsque les données transmises sont confidentielles du fait de relations professionnelles (2) ou si l'utilisateur particulier (1) désire simplement une sécurité supplémentaire, diverses techniques peuvent être implémentées, ceci en attendant la future norme 802.11x censée résoudre les failles actuelles (3).

1. Les protections domestiques : la reconfiguration du protocole

Comme premières mesures de protection d'un réseau wi-fi domestique ou d'une petite entreprise, on peut d'une part supprimer la configuration par défaut des points d'accès au réseau. Comme il a été exposé, les bornes d'accès sont configurées par défaut de manière à diffuser en permanence l'identifiant de connexion. Cet identifiant est souvent au nom de l'organisme administrant le réseau.

Il est donc nécessaire de modifier la clé WEP et l'identifiant réseau SSID installé par défaut. Il faut également désactiver la fonction qui consiste à l'envoi régulier de la trame balise (*beacon*). Il est possible de régler la puissance d'émission du pont (AP) au minimum nécessaire bien que ceci n'offre que peu de garantie pour empêcher l'écoute du réseau à distance.

On peut enfin à ce stade utiliser une clé de chiffrement de 64 ou 128 bits.

Pour passer à un autre niveau de protection, il est prudent d'associer le protocole WEP à des moyens techniques supplémentaires car, tel qu'il a été présenté précédemment, il utilise des clés fixes et il n'y a pas d'architecture d'authentification et de distribution des clés de session.

Pour remédier à cette faiblesse, il est par exemple possible de mettre en place un réseau privé virtuel (RPV) imposant l'authentification de l'utilisateur sur le réseau. Il s'agit d'une solution à laquelle les professionnels ont recours.

2. Les protections dans le cadre professionnel

En raison des différences tenant à la valeur économique des intérêts en jeu dans le cadre des activités des entreprises, les données circulant sur les RLAN professionnels sont protégées par des processus plus complexes tels que des dispositifs d'authentification avec le RPV ou d'identification.

a. Les dispositifs d'authentification

La couche RPV intègre des dispositifs d'authentification et de chiffrement entre les points d'accès et le réseau. Le RPV a pour avantage de fonctionner avec le réseau filaire en place. Ce processus permet de se réserver une partie du réseau public (Internet ou autre serveur) le temps de la transmission entre la station et le point d'accès. De surcroît, un code de cryptage est utilisé pour le transfert des données. Les données qui sont émises en retour sont également cryptées afin d'empêcher leur interception.

Le RPV est approprié aux communications professionnelles émises par exemple depuis des aéroports ou des hôtels, ou par des employés travaillant à domicile. De même pour prévenir les attaques contre un réseau fermé d'entreprise.

Dans les locaux de l'entreprise, il est toujours possible d'attribuer à un visiteur qui a besoin d'accéder à Internet ou de consulter son courrier électronique, un identifiant lui permettant cet accès. Cependant, l'accès à Internet par le biais du réseau wi-fi sera limité aux seules personnes authentifiées ayant une identification.

On peut compléter cette protection en installant des pare-feux ou *firewalls* afin de rendre le réseau invisible à l'extérieur. Par ailleurs, ils permettent d'empêcher les intrusions dans le système et dans les fichiers. Les pare-feux contrôlent et régulent le flot de données à l'intérieur et à l'extérieur des ordinateurs du réseau filaire et du réseau sans fil. Ils peuvent être mis en place pour intercepter, pour analyser et arrêter un virus émis par un hacker.

Comme le RPV, les pare-feux présentent divers niveaux de protection selon la technologie mise en œuvre.

b. Les processus d'identification

Beaucoup d'entreprises utilisent RADIUS (*remote access dial-up user service*), processus qui accorde l'accès au réseau uniquement aux utilisateurs dont le nom et le mot de passe sont reconnus. Pour accéder à un fichier ou au réseau, l'utilisateur devra signaler son nom et son identifiant. Le serveur vérifie que l'utilisateur a bien un compte et, auquel cas, il vérifie qu'il s'agit bien du mot de passe qui lui est attribué. Une fois ces vérifications faites, l'accès au réseau est ouvert.

RADIUS peut être programmé pour offrir des classes d'accès différentes en fonction de l'utilisateur. Ainsi une personne ne pourra disposer que d'Internet, une autre bénéficiera d'Internet et du courrier électronique et une autre enfin pourra accéder à Internet, au courrier électronique et aux fichiers.

On peut protéger le réseau radioélectrique par l'installation du processus Kerberos. Ce processus d'authentification créé par le *Massachusetts Institut of technologies* (MIT) est basé sur la distribution de clés. Il permet à deux entités de communiquer sur un réseau filaire ou sans fil en se présentant leur identifiant pour éviter les écoutes et les intrusions.

Il est également utilisé pour préserver l'intégrité des données (il détecte les modifications) et leur confidentialité (en empêchant la lecture par une personne non autorisée) car il génère un système de cryptographie tout au long de la communication. Kerberos fournit aux utilisateurs des " tickets ", afin qu'ils s'identifient eux-mêmes auprès du réseau et des clés de chiffrement pour sécuriser la communication. Le ticket est une séquence de quelques centaines de bits qui peut être intégrée dans n'importe quel autre réseau. De cette façon, le logiciel peut implémenter ce protocole afin de s'assurer de l'identification des utilisateurs concernés.

Des solutions de protection biométrique sont également développées. La biométrie permet l'identification d'une personne sur la base de ses traits physiques propres[67] soit sur la base de certains de ses comportements.[68] Des données comme les empreintes digitales, sont traduites par un algorithme, puis chiffrées et servent de clés d'accès au réseau wi-fi.[69]

Le développement de ces techniques a lieu concomitamment aux travaux menés pour l'amélioration de la norme wi-fi.

3. Les espoirs portés sur la future norme 802.11x

La future norme wi-fi IEEE 802.11x actuellement en développement, résoudra les problèmes logiciels et matériels d'authentification et de chiffrement. Elle sera dynamique en ce qu'elle permettra un chiffrement avec des clefs de 128 bits différentes pour chaque nouvelle session.

Il y aura un protocole d'authentification mutuelle à l'aide de TLS (*transport layer security*).

Elle proposera enfin une authentification du client au niveau du point d'accès lui-même grâce à l'introduction du protocole LEAP (*light extensible authentification protocol*).

Il sera toujours possible à un cracker de casser les codes de chiffrement en les interceptant afin d'analyser les flux de données. Mais le " cassage " des codes sera fastidieux. Entre temps, les clés auront été changées. Le logiciel permet de générer de nouvelles clés toutes les cinq minutes. Les codes découverts par le hacker ne seront plus d'actualité.

Certaines versions propriétaires du wi-fi permettent déjà de changer les codes, mais de façon manuelle. Avec la norme 802.1x cela se fera automatiquement.

Cette future norme ne sera pas publiée avant la fin de l'année 2003. Ceci a conduit les membres du *Wi-fi Alliance* à collaborer avec l'IEEE afin de développer une version

---

[67] Tels que les empreintes digitales, la forme de la main, l'iris, la voix, la rétine, le visage, l'ADN, les odeurs.
[68] Tels que sa démarche, sa manière de taper sur un clavier.
[69] Cf. pour un exemple d'application : <http://www.asc2002.com/summaries/o/OP-08.pdf>, ou <http://www.bluefishwireless.com/index.html>.

améliorée de la norme 802.11. Cette collaboration a abouti à la création du *Wi-fi Protected Access* (WPA) solution logicielle aux failles du WEP.

Par ailleurs, il y a des versions propriétaires qui améliorent le label wi-fi standard par des solutions élémentaires de sécurité en matière de chiffrement. Le logiciel de chiffrement brouillera totalement la transmission qui sera décodée par le destinataire.

D'autres logiciels utilisent des clés spéciales qui permettent aux ordinateurs de converser entre eux. L'ordinateur émetteur transmet une clé ou un code à l'ordinateur récepteur et si les clés s'associent entre elles, l'émetteur est autorisé à pénétrer le système.

En plus de l'ensemble de ces solutions, le protocole SSL devra être utilisé pour toutes les données sensibles, comme c'est déjà le cas dans les transactions électroniques.

Il est également conseillé d'effectuer l'audit du réseau. Ceci consiste à la vérification du champ d'émission du réseau. Cet audit physique permet de contrôler la diffusion (ou non) du réseau en dehors du périmètre désiré et l'existence (ou non) d'un réseau sans fil tiers dans ce même périmètre. D'autre part, un audit informatique permet de certifier que le degré de sécurité obtenu est bien égal à celui voulu.

L'administrateur doit enfin surveiller son réseau. La surveillance peut s'effectuer non seulement au niveau physique avec des outils dédiés[70], mais aussi au niveau des applications à l'aide d'un système classique de détection des intrusions.[71]

Les administrateurs sont vivement engagés à combiner ces diverses solutions, afin d'avoir un niveau de protection suffisamment élevé en attendant la mise sur le marché de la norme 802.11ix. Plus il y aura de couches de protection, plus les communications seront sécurisées.

Les gestionnaires des *hotspots* sont eux conviés, comme la plupart le font déjà, à mettre en œuvre des protections sur les réseaux afin de sécuriser les communications des utilisateurs. En effet, pour faciliter l'accès à leur réseau, les gestionnaires des sites *hotspots* répugnent à installer des processus de sécurité. Il leur est dans ce cas conseillé de limiter l'utilisation du réseau à la consultation d'Internet et à l'émission de courriels non confidentiels.

Les mesures de protection prises par l'administrateur du réseau seront renforcées par l'attitude de l'utilisateur du réseau. Il est par exemple recommandé à l'utilisateur de ne pas laisser les ordinateurs personnels allumés et connectés en permanence au réseau local radio pour parer les intrusions et usurpations.[72]

---

[70] PrismDump, Airtraf, AirIDS.
[71] Notamment, prelude, snort.

[72] Cf. communiqué de la CNIL 14 mars 2003 : <http://www.cnil.fr/thematic/index.htm>.

Mais il reste indispensable que l'administrateur remplisse ses obligations d'information et de conseil vis-à-vis de l'utilisateur, qui, sensibilisé aux risques, sera apte à adopter une attitude responsable.

B. Les solutions juridiques

Le législateur a voulu prévenir les atteintes à la vie privée et à la correspondance en instituant des mécanismes sanctionnant les accès aux réseaux (1) et aux systèmes de traitement de données (2).

1. Les sanctions applicables à l'accès aux réseaux attentant à la vie privée

L'article 226-17 du CP incrimine le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver leur sécurité et notamment qu'elles ne soient déformées, endommagées, communiquées. Cette incrimination est la sanction pénale de l'obligation de sécurité imposée par la loi du 6 janvier 1978 aux maîtres de fichier, et est punie de cinq ans d'emprisonnement et de 300 000 € d'amende.

Cette incrimination pourrait venir compenser la faiblesse de l'obligation de sécurité incluse parmi les exigences essentielles. La déficience de l'obligation de sécurité est issue de l'interprétation qu'en fait l'ART. Cependant, l'imprécision de l'article 226-17, en dépit des principes généraux du droit pénal, ne permettra pas de remédier à cette lacune. Le texte utilise en effet l'adjectif on ne peut plus indéfini " *toutes* ", sans autre précision.

Quant à la violation du secret des correspondances, elle est punie d'un an d'emprisonnement et de 45 000 euros, aussi bien lorsqu'elle est commise par un particulier que par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public.

Selon les dispositions du code pénal, il y a violation du secret des correspondances dès lors qu'il y a atteinte au secret.[73] Cette atteinte est caractérisée par l'interception, le détournement, l'utilisation ou la divulgation des correspondances émises.

L'élément intentionnel résulte de la connaissance de ce que le message visait un destinataire déterminé.

L'article 20 de la loi du 10 juillet 1991 écarte l'incrimination dans l'hypothèse où l'interception est ordonnée par les pouvoirs publics " *pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne* ". L'interception peut être également ordonnée par une autorité judiciaire dans le cadre d'une commission rogatoire.[74]

[73] Articles 226-15, alinéa 2 et 432-6.
[74] Article 22.

Concernant le détournement du contenu informationnel par piratage informatique, il faut constater qu'il n'existe pas de sanction autonome, tel le vol d'information. L'article 311-1 du code pénal qualifie de vol " *la soustraction frauduleuse de la chose d'autrui* ". La Cour de cassation a toujours refusé de soumettre la notion de vol aux biens immatériels. Elle a ainsi exclu les communications par minitel,[75] une onde hertzienne[76] et les informations.[77] Le détournement de l'information est appréhendé par le vol du support de l'information, le temps nécessaire à sa reproduction. L'information étant un bien incorporel, elle ne peut faire l'objet d'appropriation. Son détournement ne peut être sanctionné que s'il y a eu enlèvement du bien matériel la contenant, ainsi par exemple d'un CD ROM.

Ce point qui pourrait être qualifié de vide juridique en matière de wi-fi, n'a au contraire rien de spécifique à la technologie. Le problème avait déjà été soulevé bien avant concernant par exemple une personne qui prend connaissance d'un document confidentiel et qui en utilise le contenu de mémoire.

Ces cas s'étant révélés plus fréquents avec le développement de l'informatique, il est apparu nécessaire d'incriminer ces actes par des infractions spécifiques.

2. Les sanctions applicables à l'accès au système de traitement de données

Très souvent en matière de télécommunications, la violation du secret des correspondances ou le détournement de données, est commise par l'intrusion dans un système de télécommunications.

Or, l'intrusion dans un système de traitement automatisé de données ou STAD est incriminée aux articles 323-1 à 323-7 du code pénal. Il n'y a pas de définition légale du STAD, mais au cours des travaux parlementaires le Sénat l'a qualifié de " *tout ensemble composé d'une ou plusieurs unités de traitement automatisé de mémoire, de logiciel, de données, et d'organes d'entrée sortie et de liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par un dispositif de sécurité*". Cette définition intègre des éléments matériels et immatériels permettant le traitement d'informations. Le terme de " *données* " est plus large que celui couvert par la loi du 6 janvier 1978 et n'est pas limité aux données à caractère personnel.

Les systèmes de télécommunications sont concernés par cette définition car ils sont automatisés dans la mesure où leur gestion est assurée par des logiciels.

La jurisprudence a précisé que la protection était accordée aux systèmes ouverts au public, c'est-à-dire non protégés par un dispositif de sécurité.[78]

---

[75] Crim. 12 décembre 1990, Bull. crim. n°470.
[76] CA Paris, 24 juin 1987, D. 1998, sommaire 226 obs. Hassler.
[77] CA paris, 13ème chambre A ; 25 novembre 1992 Gazette du Palais.
[78] CA Paris, 11ème chambre, 5 avril 1994, JCP E 1995, I, p 207 n°461.

Cependant, depuis un arrêt de la Cour d'appel de Paris en date du 30 octobre 2002, des doutes planent. Dans cette affaire, la Cour d'appel a infirmé un jugement du tribunal de grande instance de Paris[79] qui, sur le fondement de l'article 323-1 code pénal, avait condamné une personne qui s'était introduite dans un système informatisé pour démontrer sa fragilité. Les magistrats écartent l'incrimination d'intrusion frauduleuse dans le système au motif qu'il " *ne peut être reproché à un internaute d'accéder aux données ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition, l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès* "[80].

Cette décision est certes une décision d'opportunité visant surtout à sanctionner la désinvolture du maître de fichier en lui refusant la possibilité de se prévaloir des dispositions pénales. Elle est pourtant dangereuse car des hackers en tireront profit. Ainsi par exemple appliqué au wi-fi, afin d'agrandir les réseaux communautaires, les adeptes du wi-fi recherchent les réseaux sans fils non sécurisés par le *war-driving* et le *war-crossing*.[81]

Sur le fondement de l'arrêt de la cour d'appel de Paris, un adepte du wi-fi qui accède au réseau filaire par le biais d'un réseau sans fil, peut opposer l'absence d'élément intentionnel du fait que l'intrusion a été réalisée régulièrement à l'aide d'une carte réseau sans fil. Or, l'intention frauduleuse est caractérisée étant donné que la recherche de réseau wi-fi non sécurisé a pour but de bénéficier gratuitement d'un accès au réseau filaire.

Il faut donc interpréter l'arrêt de la cour d'appel de Paris comme voulant accorder une circonstance atténuante à celui qui pénètre dans un STAD dans le seul but de démontrer l'insuffisance de fiabilité d'un système sans intention d'en tirer un quelconque bénéfice ou de lui porter atteinte. Cette interprétation n'est pas pour autant conforme à l'article 323-1 alinéa 1 qui incrimine le seul accès frauduleux au STAD comme élément suffisant. Ceci doit être compris comme le fait de s'introduire dans un système en ayant conscience de l'irrégularité de l'accès. D'autant plus que l'alinéa 2 du même article poursuit que " *lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement* ", la peine et l'amande sont doublées.

L'article 323-3 sanctionne lui la suppression ou la modification frauduleuse des données contenues dans un STAD ainsi que l'introduction de données dans un STAD. Ceci dans le cas de figure où la motivation première du pirate était de parvenir à l'une ou l'autre de ces fins. Le délit est puni trois ans d'emprisonnement et de 45 000 € d'amende.

---

[79] TGI Paris, 13 février 2002, Communication commerce électronique mai 2002, commentaire n° 72 ; Juriscom.net : <http://www.juriscom.net/jpt/visu.php?ID=318>.

[80] CA Paris, 12ème chambre section A, Antoine c/ Ministère public, *Société Tati, affaire Kitétoi*, Communication commerce électronique janvier 2003, pages 30-31, commentaire n°5 Luc Grynbaum ; Foruminternet.org : <http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=443>.

[81] Cf supra.

L'article 323-2 CP incrimine le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données. Ce délit est puni de trois ans d'emprisonnement et de 45 000 €. Seraient concernés par cette incrimination les dénis de service par désassociation et les dénis de service sur batterie[82].

Section 2 – Wi-fi et régime du contenu relevant de la correspondance publique

La constatation de l'inadaptation du droit des télécommunications en raison de son objet conduit à rechercher d'autres régimes juridiques applicables au contenu du réseau radioélectrique.

§ 1. Les raisons de l'exclusion du droit des télécommunications

Le droit des télécommunications vise à réguler le marché des télécommunications (A) en favorisant l'installation et le développement des supports de télécommunications (B).

A. L'objet du droit des télécommunications : la régulation économique du marché

Le droit des télécommunications a pour objet la régulation du marché des télécommunications en faveur de l'exercice d'une concurrence effective entre les acteurs. Cette régulation mise en place dès 1990 devait faire perdre à France Télécom son monopole public.

L'ouverture du marché s'est faite progressivement dans le sillon des prescriptions communautaires, avec dans une première phase la libéralisation de la fourniture des terminaux et des services de télécommunications pour aboutir à l'ouverture complète du marché. La loi du 26 juillet 1996 achève cette libéralisation[83].

Pour supprimer toute entrave à l'accès au marché, un ensemble de dispositifs du droit de la concurrence et du droit administratif sont mis en œuvre. Il a fallu dans un premier temps faire perdre à l'opérateur historique sa situation monopolistique en se conformant aux dispositions du droit communautaire prohibant les réglementations et autres aides en faveur des entreprises dans lesquelles les Etats ont des intérêts.[84]

Par ailleurs, une autorité administrative indépendante, l'Autorité de régulation des télécommunications, a été instituée en janvier 1997. Elle est chargée de contrôler le respect de la législation et sa compétence s'exprime en matière d'arbitrage des litiges entre les acteurs. Avec le Conseil de la concurrence, elle veille à l'élimination des ententes et des abus de position dominante sur le marché des télécommunications.

---

[82] Cf supra.
[83] Loi n°96-659 du 26 juillet 1996 sur la réglementation des télécommunications ; Foruminternet.org : <http://www.foruminternet.org/documents/lois/lire.phtml?id=18>.
[84] Actuel article 86 du traité de Rome.

Les législations en droit des télécommunications répondent à l'évolution du marché. Il s'agit d'un ordre public évolutif qui s'adapte aux objectifs qui lui sont propres. Ainsi la libéralisation du marché des télécommunications a eu lieu progressivement selon les lois du marché.

B. Le droit des communications électroniques, droit des supports

Le droit des télécommunications a pour finalité de favoriser le développement des infrastructures et des services de télécommunications à l'aide du droit de la concurrence, afin d'assurer la meilleure circulation des flux d'information.

Cette définition était juste à une époque où il n'y avait pas encore une imbrication entre les télécommunications et la communication audiovisuelle. Cependant aujourd'hui, les évolutions techniques récentes par lesquelles les réseaux anciennement réservés à l'acheminement des programmes de communication audiovisuelle permettent le transfert des services de télécommunications et inversement.[85]

Le droit de la télécommunication s'applique donc aux infrastructures et services de communications et de télécommunications filaires et non filaires, permettant la communication à distance.

La limite entre la transmission de l'information et l'information elle-même paraît alors moins visible. Cette confusion entre les deux régimes juridiques se manifeste plus particulièrement concernant le statut des services en lignes. Ainsi, dans le projet de loi sur l'économie numérique, l'article premier qualifie de communication publique en ligne " *toute communication audiovisuelle transmise sur demande individuelle formulée par un procédé de télécommunication* ".

Cette définition a fait l'objet de nombreuses critiques de la part de la doctrine et de l'ART. L'Autorité reproche en effet au législateur les risques de confusion possible entre l'accès au contenu et le contenu lui-même qui peut être de la compétence du Conseil supérieur de l'audiovisuel dès lors qu'il ne s'agit pas d'un service de télécommunication.[86]

Il est pourtant nécessaire de trouver une distinction entre les supports et le contenu en raison de l'enjeu relatif au régime juridique. Tous les acteurs militent pour un tel effort. Une partie de la doctrine exprime cependant sa préférence pour le droit de la télécommunication par le constat de sa domination. Ce dernier est aujourd'hui un instrument contribuant à la mise en œuvre des politiques de développement économique. En matière de réseaux locaux radioélectriques, des espoirs sont exprimés pour que cette technologie constitue une alternative à l'accès à l'Internet.

[85] Cf. en ce sens Lucien Rapp in *Lamy droit de l'informatique et des réseaux,* édition 2003, n° 1838.
[86] Cf. avis n°02-1090 de l'ART en date du 3 décembre 2002 sur le projet de loi relatif à l'économie numérique.

La détermination du champ d'intervention du droit des télécommunications est d'autant plus difficile que la numérisation des réseaux et des données d'une part, et la compression de ces dernières d'autre part, ont permis l'apparition d'une nouvelle industrie technologique à la fois au service des télécommunications et de l'audiovisuel. Cette convergence a abouti à l'émergence d'un nouveau marché des communications. Pour consacrer cet élément de fait, la notion de " *communications électroniques* " a été adoptée au niveau communautaire dans un ensemble de directives parmi lesquelles la directive " cadre " du 7 mars 2002.

Selon la directive, répond à la qualification de " *réseau de communications électroniques* ",

" *Les systèmes de transmission et, le cas échéant, les équipements de commutation ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux terrestres fixes et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, (...)* ".

La directive rappelle dans le considérant 5 qu'il est nécessaire de circonscrire " *la réglementation de la transmission de celle des contenus* ".

L'ART propose de soumettre au droit des télécommunications ou des communications électroniques, l'ensemble des infrastructures de communication et les services de communication donnant accès aux réseaux en vue de communications privées.

Cette proposition ne donne pas la possibilité de soumettre le contenu à d'autres régimes que celui du droit des télécommunications. En effet, elle se préoccupe essentiellement du vecteur de la communication et des activités de fourniture de services d'accès aux réseaux. Elle reste pour ce dernier cas polémique, étant donné que les professionnels de l'Internet sont soumis à la loi du 30 septembre 1986. Ce qui risque d'être le cas de l'opérateur wi-fi offrant un accès à Internet. La position de l'ART est justifiée par les services aujourd'hui accessibles par Internet. Le service de téléphonie ne pourrait raisonnablement lui échapper sous le motif qu'il est délivré par le biais d'Internet. Des difficultés relatives à la détermination des régimes applicables existent réellement.

Il y a une juxtaposition du droit des télécommunications avec les divers régimes juridiques applicables au contenu de la société de l'information.

§ 2. Les régimes applicables au contenu de la société de l'information et à la correspondance privée

La loi du 30 septembre 1986 en son article 2 qualifie la communication de " *toute mise à disposition du public ou de catégories de public, par un procédé de télécommunication, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont*

pas le caractère d'une correspondance privée ". Malgré les contestations doctrinales, le droit positif intègre dans cette définition les sites accessibles sur Internet et les services en ligne. Il en résulte que la loi du 30 septembre 1986 s'applique aux professionnels de l'Internet (A).

D'autres régimes juridiques interviennent et sont fonction, soit du mode de mise en ligne du contenu pour ce qui est du droit de la presse, soit de la destination du contenu pour ce qui est des dispositions relatives à la correspondance privée (B).

A. Les articles 43-7 et suivants de la loi du 30 septembre 1986

Sont concernés par ces dispositions, le fournisseur d'accès à Internet, le fournisseur d'hébergement et le fournisseur de contenu. L'idée de ce mécanisme de responsabilité est d'assurer l'indemnisation de la victime d'actes illicites. Elle trouve en effet auprès des fournisseurs de services l'assurance de leur solvabilité et lui évite d'avoir à rechercher le véritable auteur du délit dans les méandres de la toile.

L'article 12 de la directive du 8 juin 2000, pose en faveur du fournisseur d'accès à Internet, un régime d'exclusion de principe de responsabilité. Ce principe a été retenu par le législateur lors de la loi du 1er août 2000 et par le projet de loi pour la confiance dans l'économie numérique. Par analogie à l'obligation de neutralité de l'opérateur de télécommunications,[87] le fournisseur d'accès doit se contenter de transporter l'information.

Pour la transposition de la directive, le projet de loi LEN précise que les autorités judiciaires peuvent ordonner en référé à tout prestataire technique[88] des mesures propres à faire cesser un dommage occasionné par le contenu d'un service de communication publique en ligne. Parmi ces mesures figure l'interruption du service d'accès au contenu dommageable.[89] Les FAI pourraient ainsi être contraints à opérer ponctuellement des mesures de filtrage.

Hors les mesures de filtrages, le futur régime de la loi LEN reprend les dispositions de la loi du 31 septembre 1986 soumettant les fournisseurs d'accès à deux séries d'obligations. Ils doivent informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner. Dans le prolongement de cette obligation, ils doivent proposer à leurs abonnés au moins l'un de ces moyens. Par ailleurs, ils détiennent et conservent les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont ils sont prestataires. Ces données doivent être fournies à l'éditeur de service et être tenues à la disposition de l'autorité judiciaire à sa demande.[90]

---

[87] Article L 32-1, 5 II CPT.
[88] Il s'agit des fournisseurs d'accès et d'hébergement dont l'activité est définie respectivement aux articles 43-7 et 43-8.
[89] Cf. article 2 II du projet LEN qui introduit un article 43-12 à la loi du 30 septembre 1986.
[90] Actuel article 43-7 et 43-9 de la loi du 30 septembre 1986, article 43-13 du projet de loi.

Appliqué aux opérateurs qui assurent aux usagers l'accès à des réseaux de données à haut débit au moyen exclusif de technologies utilisant la bande 2,4 GHz, en tant que fournisseurs d'accès à Internet, le régime d'exclusion de responsabilité s'appliquera en leur faveur.

Qu'en est-il cependant du particulier ou d'une association wi-fiste qui partagent un même accès à Internet ? Des propositions et des réserves ont été émises concernant la communauté wi-fi et le cas du particulier opérateur de télécommunications. La qualification de fournisseur d'accès peut-elle cependant être retenue ?

Cette qualification n'aurait que peu d'intérêt en cas d'infractions commises par le biais de l'abonnement Internet de ce particulier étant donné qu'il bénéficiera d'un régime d'exclusion de principe de responsabilité. Un bémol doit être placé, car l'application de ce régime permettrait d'obliger le particulier à mettre en œuvre des dispositifs de sécurité.

Il faudrait agir sur le fondement de la responsabilité civile ou pénale.

Dans les contrats de fourniture d'accès analysés,[91] le fournisseur de services met à la charge de l'abonné toute utilisation effectuée à partir de son poste avec ses identifiants de connexion, étant donné qu'il est gardien de la chose.

Ces mêmes contrats prévoient la résiliation lorsque, à l'aide de l'abonnement de l'utilisateur, des actes contraires à la " netiquette " ont été commis.

Le fournisseur d'accès dispose donc d'une arme contre les délits commis par le biais de son accès Internet qui consiste, grâce aux dispositions contractuelles, à mettre fin à la connexion de l'abonné.

Par ailleurs, la personne victime pourra engager une action en responsabilité délictuelle ou pénale selon la gravité des agissements. La commission d'infractions par un tiers sur l'Internet par le biais d'un accès hertzien, a pour inconvénient de rendre anonyme l'identité du véritable auteur du dommage. Seule l'identité de l'abonné au réseau filaire est connue du fait des recommandations faites aux FAI par l'article 43-9 de la loi du 30 septembre 1986. Ainsi, la victime qui a subi un préjudice causé par un délit commis sur Internet par ce moyen, agira contre la personne dont l'identité est apparente. Sur le terrain civil, les articles 1382 et suivants trouveront à s'appliquer et, sur le terrain pénal, la victime pourra agir sur le fondement de la complicité par fourniture de moyen.

Avec le développement rapide du wi-fi, dans certains contrats de fourniture d'accès, une clause a été introduite permettant la résiliation lorsque l'abonné a partagé sa connexion Internet. Certains fournisseurs ont en effet introduit dans leur contrat une clause prohibant de telles pratiques qui engendrent des pertes économiques importantes sur le marché potentiel des abonnés à Internet.

[91] France-Télécom-Wanadoo, Tiscali, AOL.

Cette interdiction était déjà possible par le jeu de la clause exclusive de garantie pour les accès aux services en ligne effectués à l'aide de matériels et équipements non validés par le fournisseur.

Cette clause cependant ne permettait pas la résiliation du contrat et restait évasive quant à la notion d'équipements qui devaient recevoir la validation du FAI.

Par ailleurs, elle ne tenait pas compte de l'hypothèse où le client permettait un accès payant à sa connexion par une forme de " sous-traitance " dans la fourniture de service d'accès.

Aux Etats-Unis, pour contourner ce problème, les FAI ont adressé par courrier une injonction aux abonnés qui partageaient gratuitement ou à titre onéreux leur connexion à Internet, leur demandant de cesser ces pratiques. A défaut d'obtempérer, le client supporte les charges de la résiliation du contrat.[92]

La tendance actuelle est de refuser au particulier la possibilité de faire un tel partage. Ainsi, il est spécifié que l'usage du modem est strictement domestique ou professionnel dans le cas d'un réseau d'entreprise. Le client reste responsable des utilisations faites de son modem.

Le non-respect de cette clause peut entraîner la résiliation du contrat.

Il est difficilement imaginable que le client puisse écarter cette clause sur le fondement de l'article L 132-1 et suivants du code de la consommation ou de l'article 1135 du code civil lorsqu'il s'agit d'un professionnel. L'ART en effet laisse aux FAI le soin d'admettre ou non que leurs clients partagent leur connexion haut débit avec des tiers.

Ce refus peut paraître contestable dans les hypothèses où le FAI fournit un service gratuit et que l'abonné à son tour offre le partage de sa connexion gracieusement. Le FAI ne peut alors prétendre subir un manque à gagner.

Au contraire, lorsque l'accès à la connexion de l'abonné est payant, le FAI peut opposer cet argument. De même lorsque le FAI fournit un service contre paiement[93].

Le client pourrait dans certains cas répondre par l'inopposabilité de la clause dans l'hypothèse où elle aurait été rajoutée dans les conditions générales du contrat d'accès qui figure en ligne. Très souvent, le FAI indique que les conditions générales en ligne (qui peuvent être modifiées à la discrétion du professionnel) prévalent sur les conditions générales imprimées. Or la Commission des clauses abusives a regretté dans sa

[92] <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2873688,00.html>
[93] Dans la plupart des cas, l'accès aux bornes RLAN est payant dans les *hotspots* et dans le cadre des communautés, il y a un partage des frais d'accès entre les membres.

recommandation sur les contrats d'accès à Internet[94] cette pratique qui donne prépondérance à un document pouvant se prêter par nature à évolution, alors même que la clause ne serait pas acceptée par le consommateur. Ceci aggrave en effet le déséquilibre entre le client et le professionnel qui modifie le contrat de manière unilatérale.

En revanche, lorsque le FAI notifie par voie électronique les modifications contractuelles, l'équilibre contractuel est préservé.

De même, doit être approuvée la démarche des FAI américains qui notifient à leurs clients qu'ils ont été repérés comme émettant des ondes radioélectriques en extérieur et, partant, facilitant l'accès à leur connexion, et à leur demander de prendre les mesures nécessaires. Ceci permet en effet au client de bonne foi qui a mal réglé sa borne de n'être pas immédiatement sanctionné par la résiliation du contrat.

Le partage de l'accès à Internet banalise l'accès au wi-fi. De plus, cela s'inscrit dans les efforts menés pour la libéralisation du marché des télécommunications et du dégroupage de la boucle locale. Cependant, l'ouverture du marché et le développement des technologies de la communication doivent se faire par le biais de l'intervention de professionnels dotés des compétences nécessaires pour garantir les principes touchant à la liberté de la communication et à la vie privée. La libéralisation du marché des télécommunications ne signifie pas en effet une déréglementation pour permettre l'émergence d'un marché ouvert à la concurrence dans l'intérêt des consommateurs. Or, il en va de leur intérêt de préserver leur vie privée.

Il faudrait donc encourager l'implantation de *hotspots* sécurisés afin que les utilisateurs nomades aient une solution alternative à leurs besoins dans le respect des principes s'appliquant à l'Internet.

Les lieux de passage public permettant l'accès à Internet mettent en œuvre des processus d'identification de connexion. Il devient alors possible de sanctionner l'utilisateur qui commet des délits en émettant par exemple du contenu illicite portant atteinte aux droits de propriété intellectuelle (fichiers MP3).

B. Les communications publiques et la correspondance privée

Lorsque le contrôle des messages révèle l'illégalité de leur contenu, divers mécanismes de responsabilité peuvent s'appliquer selon la nature du message. Cette dernière est déterminée par la destination de sa diffusion.

Le message peut être diffusé au public, ou à une ou plusieurs personnes déterminées.

[94] Bulletin officiel de la concurrence, de la consommation et de la répression des fraudes, 31 janvier 2003, p.8 et s.

Les messages dont le contenu est susceptible d'être consultable par toute personne, concernent essentiellement, en matière de wi-fi, les messages provenant d'Internet.

Ils peuvent être soumis aux dispositions de la loi du 30 septembre 1986 s'ils constituent des services de communication audiovisuelle ou radiophonique.

D'autres dispositions peuvent trouver à s'appliquer, comme par exemple des dispositions pénales. La diffusion de messages à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine doit se faire de manière à ne pas être perçue par un mineur.[95]

Dans ce cas, lorsque cette infraction est commise par la voie de la presse écrite ou audiovisuelle, les dispositions particulières de détermination de la responsabilité sont applicables. La loi du 29 juillet 1891 en matière de presse et la loi du 29 juillet 1982 en matière de communication instaurent un régime de responsabilité " *en cascades* ". L'auteur principal des infractions est le directeur de publication qui est chargé de rendre public l'information, à défaut l'auteur, à défaut le producteur pour l'audiovisuel.

La jurisprudence a précisé que pour que le droit de la presse écrite s'applique à Internet, il faut que les critères de périodicité dans le renouvellement du contenu soient réunis.[96]

De même si les personnes coupables de délits veulent se prévaloir de la prescription de trois mois. La Cour de cassation a précisé à ce propos que le point de départ de la prescription est le jour où l'information a été mise en ligne.[97]

Le message peut être destiné à de la correspondance privée.

Dans le cadre des relations de travail, le contenu du message peut concerner les intérêts de l'entreprise. Dans ce cas, la responsabilité du salarié sera recherchée sur le terrain de l'abus de confiance ou de la violation d'une clause de confidentialité, ou d'un secret de fabrique, s'il est tenu par une telle obligation en vertu de son contrat de travail.

Le contenu du message peut porter atteinte à la dignité d'une personne. Il peut s'agir de l'intérêt d'un particulier ou de l'intérêt général. Les messages injurieux ou de harcèlement transmis ouvreront droit à une action de la victime en responsabilité civile ou pénale[98].

---

[95] Article 227-24 du code pénal.

[96] TGI de Paris, référé, 29 mai 2001, C*ommunication commerce électronique,* octobre 2002, commentaire n° 136, page 40, Agathe Lepage.

[97] Trois arrêts se sont prononcés en ce sens en 2001, Crim. 30 janvier 2001 JCP 2001, 10515 ; Juriscom.net : <http://www.juriscom.net/jpt/visu.php?ID=309> ; Crim. 16 octobre 2001, *Communication commerce électronique,* décembre 2001 n°132 ; Juriscom.net : <http://www.juriscom.net/jpt/visu.php?ID=312> ; Crim. 27 novembre 2001 *Communication commerce électronique,* février 2002 n° 32 ; Juriscom.net : <http://www.juriscom.net/jpt/visu.php?ID=315>.

[98] Tribunal correctionnel de Meaux, 19 novembre 2001, s'agissant d'une personne coupable de diffamation publique pour avoir diffusé sur Internet des photographies retouchées faisant apparaître le visage de collègues de travail représentés dans des scènes pornographiques, d'autre part d'injure publique pour avoir donné à

Pour ce qui est des atteintes à l'ordre public, depuis la loi du 4 mars 2002,[99] le droit pénal incrimine la diffusion, la fixation, l'enregistrement ou la transmission d'image, ou la représentation d'un mineur présentant un caractère pornographique. L'incrimination inclut la diffusion dans le cadre d'une correspondance privée comme dans celui d'une correspondance publique.[100]

d'autres collègues l'apparence de singe. *Communication commerce électronique,* février 2002, p. 35 commentaires n° 30 Agathe Lepage.

[99] Loi nº 2002-305 du 4 mars 2002 relative à l'autorité parentale art. 14 Journal Officiel du 5 mars 2002.

[100] Article L 227-23 du code pénal.

Conclusion

L'activité des acteurs du wi-fi est encadrée par des règles juridiques. Ces règles existent pour l'établissement du réseau et pour le contenu qu'il contient. De l'efficacité de ces mécanismes juridiques dépendra le développement du wi-fi. En effet, les opérateurs et les utilisateurs doivent être rassurés sur l'effectivité de leur possibilité de recours en cas de litiges et de violation de leurs droits, avant d'engager des transactions sur ce nouveau média.

La diversité de régimes applicables devrait tranquilliser les utilisateurs du wi-fi mais ne constitue pas un gage de confiance. Il peut sembler difficile à un particulier béotien de se retrouver parmi toutes ces règles de droit.

Par ailleurs, la pluralité de régimes n'assure pas l'homogénéité. Pour le moment, malgré l'introduction d'une réglementation plus souple pour l'établissement des RLAN et de la notion européenne de services et de supports de " *communications électroniques* ", le partage des compétences entre l'ART, le CSA et la CNIL, n'est pas de nature à éclaircir et à faciliter une parfaite appréhension des règles applicables au wi-fi. La multiplicité des régimes applicables ira croissant car de plus en plus de services seront disponibles par l'intermédiaire du wi-fi. Peuvent être cités des services de téléphonie, d'accès à la télévision numérique[101].

L'absence d'effectivité de ces règles pourra tendre à l'irresponsabilité des acteurs.

Cependant, bien avant l'ineffectivité des règles de droit, le principal frein au développement du wi-fi reste l'inexistence de logiciel assurant la sécurité du réseau. Les acteurs peuvent se protéger par des mécanismes juridiques contractuels contre les éventuelles déficiences de leurs partenaires, mais un acte de piraterie est plus difficilement évitable.

La bulle wi-fi n'étant pour le moment que virtuelle,[102] les acteurs ne doivent pas, dans l'euphorie, oublier les précautions à prendre contre les risques de faillite de leurs partenaires.

En cas d'échec du développement de cette technologie, les principales victimes seront les consommateurs juridiquement moins bien informés et protégés.

---

[101] Le projet Pau Broadband Country peut être cité. Expérimenté à partir de novembre 2003, il permettra aux habitants de la ville d'accéder à Internet par le biais d'infrastructures hertziennes et filaires à Internet à 100 Mb/s. La connexion sera possible contre paiement d'une redevance. Seront accessibles des services de téléphonie, de télévision, des administrations publiques. Les risques en matière de wi-fi sont dans la possibilité pour un pirate de se connecter au réseau de la ville sans payer et de bénéficier des diverses prestations. Pour une consultation du site : <http://eco.agglo-pau.fr/Initiatives/PBC/pbc.htm>.

[102] Cf. les articles : *Wi-fi : une nouvelle bulle ?* Journal du net du jeudi 17 juillet 2003 et *Hot spots WI-FI : le grand décollage* de Didier Geneau, Décision Micro du 26 juin 2003.

Bibliographie

ASTOR Philippe, " Le Wi-Fi, un vent de liberté pour les services à haut débit ", 18 février 2003, <http://news.zdnet.fr>.

FLOUR et AUBERT, *Les obligations, 1. L'acte juridique* Armand Collin, 8ème édition, septembre 1998.

GUERRIER Claudine, *Les écoutes téléphoniques,* CNRS droit, novembre 2000.

GUILLEMIN Christophe, " Module WPA : une alternative aux faiblesses de sécurité du Wi-Fi ", 2 avril 2003, <http://news.zdnet.fr>.

Journal du CNRS *Sécurité informatique,* juin 2002, n°40, <http://www.cnrs.fr/Infosecu/num40-sansFond.pdf>.

Lamy droit de l'informatique et des réseaux, édition 2003, n°1834 à 2185.

Lamy droit des médias et de la communication, tome 2, fascicules n° 403 à 439, édition 2002.

PRAT Damien, *" Focus sur les normes Wi-Fi "*, 2 mai 2003, <http://techupdate.zdnet.fr>.

Sitographie

http://www.art-telecom.fr

http://www.cnil.fr

http://www.commentcamarche.net

http://europa.eu.int

http://www.ieee.org

http://www.journaldunet.com

http://www.juriscom.net

http://www.legifrance.gouv.fr

http://pw.lesmanos.com/news.php

http://senat.fr

http://www.weca.net

http://www.wifi-montauban.net

http://www.zdnet.fr

http://www.01net.com

http://eco.agglo-pau.fr/Initiatives/PBC/pbc.htm