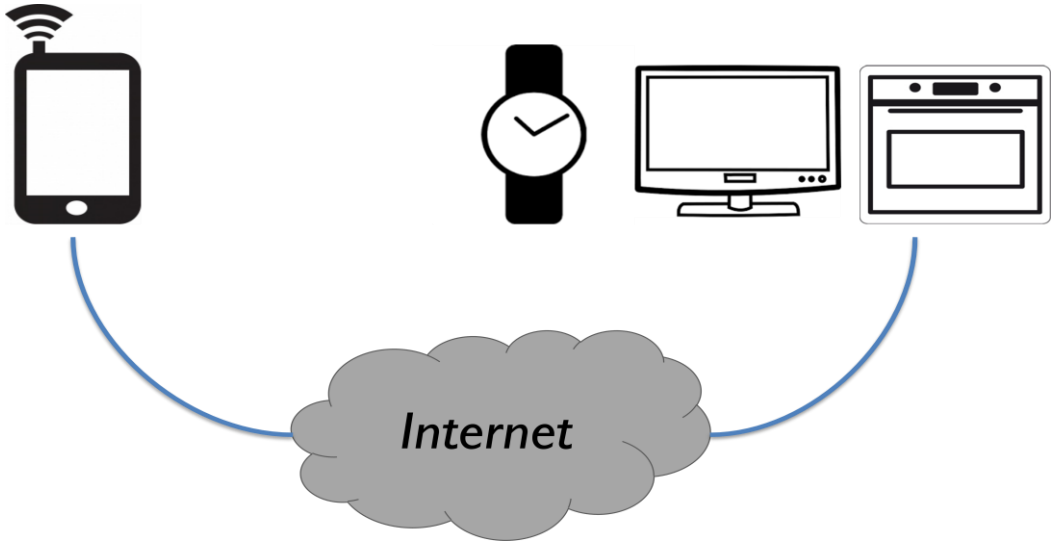
TABLE RONDE DU 13 FÉVRIER 2015
« LE DROIT ET L'INTERNET DES OBJETS »

LE DROIT DES RÉSEAUX APPLIQUÉ A L'INTERNET DES OBJETS



PRESENTE PAR
CLARA ALCOLEA, CAROLINE JUILLET ET MYRIAM KITAR

RAPPORT REALISE SOUS LA DIRECTION DE M. LE PROFESSEUR FREDERIC LAURIE
MASTER II. « DROIT DES MEDIAS ET DES TELECOMMUNICATIONS
AIX-MARSEILLE UNIVERSITE

ANNEE UNIVERSITAIRE 2014-2015

TABLE DES ABREVIATIONS

ANFR	Agence Nationale des Fréquences Radioélectriques
ARCEP	Autorité de Régulation des Communications Electroniques et des Postes
CSA	Conseil Supérieur de l'Audiovisuel
FAI	Fournisseur d'Accès à Internet
FM	Frequency Modulation
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSMA	GroupeSpeciale Mobile Association
ICANN	Internet Corporation for Assigned Names and Numbers
IDO	Internet Des Objets
IP	Internet Protocol
LIR	Local Internet Registries
LSA	Licensed Shared Access
LTE	Long Term Evolution
M2M	Machine to Machine
MNC	Mobile Network Code
RIR	Regional Internet Registries
RSPG	Radio Spectrum Policy Group
UIT	Union Internationale des Télécommunications
UNB	Ultra Narrow-Band

SOMMAIRE

INTRODUCTION

« *L'internet des objets, par sa capacité à élargir progressivement la notion de réseau de réseaux en construisant un réseau de capteurs pour des objets, contribuera également à structurer des types de réseaux inédits en tissant entre objets et individus des formes de structuration aussi nouvelles que celles qu'ont constitué les communautés dans l'Internet*[1] ».

Le développement de l'Internet des objets, qui implique une communication entre des machines ou entre des objets qui ne sont pas nécessairement électroniques au départ, amène à s'intéresser aux évolutions possibles du droit des réseaux encadrant les communications électroniques. L'évolution du monde numérique a entraîné le développement de ce nouvel internet qui nous dirige vers une réalité dont on ne saisit certainement pas encore toute l'ampleur.

L'internet des objets est un réseau de réseaux dans lequel des systèmes d'identification électronique identifient des objets connectés, des entités numériques afin de pouvoir récupérer et mémoriser les données qui s'y rattachent. L'internet des objets est une extension de l'internet que nous connaissons aujourd'hui, il permettra à des objets du quotidien d'être reliés à internet et à toutes les fonctions que cela implique. L'expression « machine-to-machine », souvent utilisée pour parler de l'internet des objets, désigne une communication faite entre des machines et ce, sans intervention humaine. Elle a une dimension industrielle. L'expression « Internet des objets » est quant à elle plus générale puisqu'elle regroupe toute communication entre des objets du quotidien.

Le droit des réseaux est le droit applicable aux communications électroniques selon l'article L32 du Code des postes et des communications électroniques. Cet article dispose en effet que l'on entend par un tel réseau *« toute installation ou tout ensemble d'installations de transport ou de diffusion ainsi que, le cas échéant, les autres moyens assurant l'acheminement de communications électroniques, notamment ceux de commutation et de routage ».* Les communications concernées sont toutes les correspondances privées et toutes les communications au public par voie électronique. À ces communications s'applique le principe de neutralité du réseau ayant pour effet un traitement identique entre les correspondances privées et les communications au public. Cela s'explique par le fait que les réseaux sont indifférents au contenu qu'ils transportent.

L'internet des objets crée toutefois une troisième réalité de communication, à savoir la communication entre tout objet, or cette dernière peut correspondre aussi bien à la catégorie de la correspondance privée que de celle de la communication au public. L'arrivée de l'Internet des objets bouleverse donc le schéma de la communication tel que prévu par le Code des postes et des communications électroniques, faut-il pour autant modifier le droit des réseaux existant ?

[1]BENGHOZI (P.), BUREAU (S.), MASSIT-FOLEA (F.), *L'Internet des objets. Quels enjeux pour les Européens ?*, Rapport de la chaire Orange Innovation and Régulation, Ecole polytechnique et TELECOM, Paris Tech. 2008, p.14.

En partant du principe que l'internet des objets crée une nouvelle réalité de communication, on peut estimer qu'une évolution du droit des réseaux est nécessaire sans qu'il soit indispensable de le changer en profondeur. En effet, les correspondances privées et la communication au public par voie électronique existent toujours. L'internet des objets apparaît alors comme une mutation de l'Internet mobile, des usages et des technologies, mutation que le droit devra prendre en compte sans en être fondamentalement bouleversé.

Quel sera cependant le rôle du droit des réseaux dans l'Internet des objets ?

Le rôle du droit des réseaux dans l'Internet des objets va être de connecter des objets du quotidien à internet afin qu'ils puissent par la suite communiquer entre eux. Avant l'annonce publique du World Wild Web en 1990, le développement de l'internet a du faire face à de nombreux problèmes techniques afin qu'il puisse être utilisable à l'échelle mondiale. Internet est en effet constitué d'une multitude de réseaux répartis dans le monde et interconnectés. Ces réseaux communiquent entre eux et s'échangent des données.

Le développement de l'Internet des objets et les notions qui lui sont liées (de la RFID au « machine-to-machine ») se heurtent eux-aussi à de nombreux défis afin d'assurer le bon fonctionnement des réseaux utilisés. Les réseaux étaient au cœur de l'Internet, puis de l'Internet mobile, ils seront également au cœur de l'Internet des objets.

Pour assurer le bon fonctionnement de ces réseaux de communication dans l'Internet des objets, il faut faire face à des défis techniques (I), il faut également pouvoir proposer des garanties juridiques (II).

PARTIE I

DES DEFIS TECHNIQUES NECESSAIRES AU BON FONCTIONNEMENT DES RESEAUX DANS L'INTERNET DES OBJETS

Il existe deux grandes catégories de défis techniques dont la résolution est nécessaire pour assurer le bon fonctionnement des réseaux dans l'internet des objets. En premier lieu, il est nécessaire que soit réorganisée l'utilisation de ressources limitées qui sont nécessaires au fonctionnement des réseaux (A). En deuxième lieu, nous verrons qu'il est nécessaire qu'une harmonisation de l'interopérabilité des systèmes soit mise en place (B).

A. Une nécessaire réorganisation de l'utilisation de ressources limitées

La connexion d'un objet à un réseau nécessite l'utilisation de ressources qui sont, elles, limitées. Le développement massif de l'internet des objets a donc notamment pour effet de provoquer deux types de pénuries dont leurs utilisations doivent donc être repensées et réorganisées pour permettre le bon fonctionnement des réseaux. D'abord en ce qui concerne le risque depénurie de fréquences (1), ensuiteconcernant la pénurie d'adresses IP (2).

1- La pénurie de fréquences

Les fréquences sont essentielles dans le fonctionnement technique de l'internet des objets. Cependant, il s'agit de ressources naturelles limitées et le développement des objets connectés entraîne une croissance des besoins en fréquences. L'utilisation des fréquences représente un enjeu économique important pour le secteur du numérique qui ne pourra se développer sans les fréquences. Rappelons tout de même qu'il n'y a même pas trente ans, l'utilisation des fréquences était majoritairement utilisée en matière de sécurité ou d'usage non marchand[2]. Aujourd'hui, le nombre des besoins en fréquences est tel, qu'il n'existe plus assez de gammes facilement exploitables (entre 400 MHz et 6 GHz) et qu'il devient plus difficile de dégager de nouvelles bandes pour des usages exclusifs[3]. Face à ce risque de « pénurie », des solutions aussi bien juridique (1.1) que technique (2.2) sont aujourd'hui mises en place et discutées. Le but est de réorganiser l'utilisation des fréquences afin de garantir un accès à tous les utilisateurs.

1.1- Solution juridique

La principale solution qui est envisagée par les pouvoirs publics repose sur un usage et un partage dynamique du spectre des fréquences. Le principe est d'optimiser et d'organiser au mieux le partage des fréquences entre les différents utilisateurs au niveau européen et au niveau national.

[2] TOLEDANO (J.), *Une gestion dynamique du spectre pour l'innovation et la croissance*, rapport de la mission ministérielle sur le spectre hertzien, 31 mars 2014, p. 9
[3] TOLEDANO (J.), *op. cit.*, p. 12

D'abord au niveau européen, plusieurs initiatives ont été prises afin d'encourager au partage du spectre et notamment pour prévoir l'arrivée massive des objets connectés. Dès 2009, la directive 2009/140/EC, modifiant les directives 2002/21 CE, relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques,impose à ce que des travaux concernant le partage du spectre des fréquences soient effectués. La directive de 2009 précise aussi que les radiofréquences doivent être utilisées de manière efficace et effective et doivent permettre des économies d'échelles et l'interopérabilité des services.

Cela a notamment donné lieu à la mise en place en 2012 à un Programme pluriannuel de politique du spectre par une décision en date du 14 mars 2012. Cette décision oblige les Etats membres de l'Union européenne à faire un inventaire des bandes de fréquences qui pourraient se prêter au partage du spectre.

En parallèle à cette décision, plusieurs avis sur la question ont été rendus. En 2012, la Commission européenne a publié une communication dans le but d'encourager le partage du spectre. De plus, le groupe RSPG (Radio Spectrum Policy Group) a publié en 2013 un avis relatif au « *LicensedShared Access »* (LSA) où il est prôné un accès partagé et sans licence au spectre des fréquences.

Ensuite au niveau national, c'est notamment au législateur d'autoriser le partage du spectre entre les utilisateurs. En France, l'article 22 de la loi du 16 juillet 1986 relative à la réglementation des télécommunications, prévoit que les fréquences radioélectriques appartiennent au domaine public de l'Etat. Par conséquent, les fréquences sont en principe inaliénables et imprescriptibles. Ainsi, toute occupation privative du domaine public permet la perception de redevances et est conditionnée à une autorisation administrative.

En l'occurrence, en matière d'objets connectés utilisant un réseau ouvert au public, l'ARCEP est compétente pour conférer le droit d'utilisation des fréquences aux exploitants des installations privées sous forme d'autorisation individuelles. Ainsi pour Thomas PEZ, professeur des Universités, il est déjà possible en droit français un partage de fréquences[4]. Soit dans le cadre d'une autorisation individuelle avec plusieurs co-titulaires, résultant d'une occupation privative du domaine public hertzien. A charge pour les titulaires de verser une redevance et de respecter les conditions fixées par l'ARCEP. Soit dans le cadre d'une autorisation générale qui permet une utilisation collective du domaine public par l'ensemble desusagers, sans redevance mais avec l'obligation de respecter les conditions de l'ARCEP.

Il semble donc que le droit positif français est adapté àun partage « dynamique » des fréquences tel qu'encouragé par l'Union européenne[5].C'est d'ailleurs dans cette perspective, qu'en juillet 2014, le rapport ministériel rendu par Joëlle Toledano, membre du Conseil d'administration de l'ANFR et professeur d'économie en université, fait aussi état de la

[4]PEZ (T.),« L'incidence du partage du spectre sur le droit français applicable aux fréquences radioélectriques », *in* Une gestion dynamique du spectre pour l'innovation et la croissance, rapport de la mission ministérielle sur le spectre hertzien confiée au professeur Joëlle Toledano, 31 mars 2014, p 112.

[5] TOLEDANO (J.), *Une gestion dynamique du spectre pour l'innovation et la croissance*, rapport de la mission ministérielle sur le spectre hertzien, 31 mars 2014, p. 29.

nécessité de promouvoir le partage dynamique du spectre des fréquences. En effet, le rapport recommande au gouvernement de mettre en place une véritable stratégie du spectre notamment en vue de préparer l'arrivée massive de l'internet des objets. Il s'agit ainsi « *d'intensifier l'usage du spectre, de promouvoir le partage dynamique et de mettre en place les mécanismes incitatifs adaptés*»*6*. Selon le rapport, la solution consiste à rendre plus de fréquences accessibles à tous donc sans licence.

De son côté, l'ARCEP a rapidement pris acte de ces recommandations. De juillet à octobre 2014, l'autorité a ouvert une consultation publique sur « l'utilisation des fréquences libres ». La consultation publique a notamment mis en exergue le fait que les fréquences libres, puisqu'elles ne sont soumises à redevances, encouragent une utilisation flexible du spectre qui peut être bénéfique aux entreprises innovantes. Cela a donné lieu à un projet de décision de l'ARCEP qui prévoit en son article 2 que **«** *l'utilisation par des dispositifs à courte portée des bandes de fréquences listées à l'annexe 1 de la présente décision est autorisée sous réserve du respect des conditions techniques précisées à cette même annexe pour chaque bande de fréquences et, dans ces conditions, n'est pas soumise à autorisation individuelle* »[7].

Les pouvoirs publics semblent aujourd'hui avoir pris conscience de la problématique liée à l'utilisation des fréquences. La principale solution est davantage tournée vers une nouvelle organisation du partage du spectre des fréquences, afin que les utilisateurs ne se voient pas restreint dans le développement et l'utilisation des objets connectés. Mais à côté de cette solution réglementaire, il est aussi développé des solutions de la part d'acteurs privés. Il s'agit de solutions techniques visant elles aussi à répondre à la problématique des fréquences que posent en partie l'arrivée de l'internet des objets.

1.2 – Solutions techniques

Le rapport de Joëlle Toledano envisage plusieurs techniques pour connecter les objetsen fonction de leurs natures : « des réseaux mobiles (2G/3G ou 4G), des réseaux dédiés utilisant des fréquences basses ouvertes, des liaisons Wifi ou Bluetooth »[8]. Les techniques sont donc nombreuses mais une doit retenir notre attention en ce qu'elle est particulièrement novatrice et répond à la problématique de la pénurie de fréquences.

Aujourd'hui, seule la très prometteuse start-up française SIGFOX a réussi à développer un réseau basses fréquences, spécifiquement dédié aux objets connectés. Crée en 2009 par Ludovic Le Moan, l'entreprise est la seule à ce jour à disposer d'une telle capacité. Le réseau utilise la technologie radio dite « bande ultra étroite » ou « UNB » et utilise des fréquences particulièrement basses et qui ne nécessitent pas d'autorisation. Sigfox est donc un opérateur qui permet de faire communiquer les objets connectés. A la manière d'un opérateur « classique », il suffit d'acheter un modem (entre 5€ et 15€) et de s'abonner (abonnement entre 1€ et 9€ par an) pour pouvoir utiliser le réseau mais les coûts restent tout même largement inférieurs à un opérateur « classique ». Cependant, l'utilisation des basses

[6] TOLEDANO (J.), *op. cit.*, p. 14.
[7] Projet de décision n°2014-xxxx de l'ARCEP en date du xxxxxx 2014, fixant les conditions d'utilisation des fréquences radioélectriques par des dispositifs courte portée.
[8] TOLEDANO (J.), *Une gestion dynamique du spectre pour l'innovation et la croissance*, rapport de la mission ministérielle sur le spectre hertzien, 31 mars 2014, p. 13.

fréquences suppose que le client ne peut envoyer « *qu'entre 0 et 140 messages par jour et chaque message peut contenir jusqu'à 12 octets de données réelles de charge utile* »[9]. Mais le principal avantage réside dans le fait que la consommation d'énergie des appareils échangeant des données est largement diminuée en comparaison aux réseaux téléphoniques. Ainsi, les objets connectés qui utilisent le réseau Sigfox peuvent avoir jusqu'à dix ans autonomie.

A l'heure actuelle, la start-up a déjà réussi à déployer un réseau entier en France et est présent en Espagne, aux Pays-Bas ou encore en Grande-Bretagne. Sigfox a en effet besoin d'installer beaucoup moins d'antennes qu'un opérateur téléphonique « classique »; à titre de comparaison, il faut 1 à 3 antennes Sigfox pour 1000 km² couvert alors qu'il en faut 20 pour les opérateurs de téléphonie. Sigfox est aussi présent dans des grandes villes comme New York et Moscou et a pour ambition de devenir le premier réseau international d'objets connectés.

Il faut noter qu'Anne Lauvergeon a quitté son poste de PDG d'Areva en avril 2014 pour devenir présidente de Sigfox, startup de 60 employés. De plus, début février 2015, l'entreprise a réalisé une levée de fond record de 100 millions d'euros ce qui lui permettra de se déployer notamment en Asie et aux Etats-Unis[10]. Plusieurs opérateurs télécoms (Telefónica, SK Telecom et NTT Docomo Ventures), le fonds d'investissements (Elliott Management Corporation) et les groupes industriels GDF Suez, Air Liquide et Eutelsat sont entrés au capital dans des proportions non communiquées. A ce titre, certains observateurs parlent aujourd'hui du « *futur Google de l'internet des objets* »[11].

Qu'il s'agisse d'initiatives de la part des autorités publiques ou de la part d'acteurs privés, des solutions sont donc mises en place pour essayer de remédier au besoin croissant de cette ressource limitée que sont les fréquences. Il en est de même concernant le phénomène de pénurie affectant les adresses IP.

2- La pénurie des adresses IP

Sur Internet, les systèmes communiquent entre eux via des adresses IP. Ces adresses IP sont utilisées par des routeurs pour permettre à deux systèmes distants de communiquer entre eux.Une adresse IP est un numéro d'identification unique qui est attribué à chaque appareil connecté à un réseau utilisant l'Internet Protocol. Chaque objet connecté aura nécessairement une adresse IP qui lui est propre.

Au départ, l'IANA (Internet AssignedNumbersAuthority) était l'organisation qui avait pour rôle de gérer les espaces d'adressage IP. Depuis 1998, elle est devenue une composante de l'ICANN (Internet Corporation for AssignedNames and Numbers). L'ICANN définit les procédures d'attribution et de résolution de conflits dans l'attribution des adresses mais délègue la gestion pure de ces ressources à des instances régionales puis locales, dans chaque

[9] MALE (O.), « Sigfox, technologie de rupture pour le M2M », domotique-info.fr, 25 février 2015.
[10] CHAPERON (I.), « Levée de fonds record pour la start-up française Sigfox », *lemonde.fr*, 11 février 2015.
[11] MOREAU (M.), « Sigfox, le google de demain », *frenchweb.fr*, 4 décembre 2012.

pays, appelées « Internet Registries »[12]. Il existe aujourd'hui cinq RIR :
- RIPE-NCC (Réseaux IP Européens, créé en 1992) pour l'Europe et le Moyen-Orient ;
- APNIC (Asia Pacific Network Information Center, créé en 1993) pour l'Asie et le Pacifique ;
- ARIN (American Registry for Internet Numbers, créé en 1997) pour l'Amérique du Nord (entre 1993 et 1997, ce rôle était attribué à InterNIC) ;
- LACNIC (Latin American and Caribbean IP addressRegionalRegistry, créé en 1999) pour l'Amérique latine et les îles des Caraïbes ;
- AfriNIC(African Network Information Center, créé en 2005) pour l'Afrique.

Les adresses IP sont finalement allouées à l'utilisateur final qui en fait la demande par un Local Internet Registry (LIR) autorisé par l'instance régionale. Un LIR est généralement un fournisseur d'accès Internet ou une grande organisation comme les entreprises multinationales. Il est sous l'autorité de l'instance régionale de gestion de l'adressage.

Le mode de fonctionnement utilisé jusqu'à présent est en IPv4, sous la forme « xxx.xxx.xxx.xxx » ; « x » étant un nombre entre zéro et 255, soit 256 possibilités. Une adresse IPv4 est codée sur 32 bits, soit un peu plus de quatre milliards d'adresses disponibles. En dix ans, près d'1,6 milliard d'adresses IPv4 ont été attribuées et avec la multiplicité de périphériques se connectant à internet, la situation devient critique. D'autant plus que les pays émergents comme l'Inde et la Chine en sont de grands consommateurs. Le constat est sans précédent : chaque organisme en charge de la distribution et de la gestion des adresses IP fait état de la pénurie d'adresses IPv4. Après l'Asie qui a atteint un seuil critique en avril 2011, l'Europe en septembre 2012, c'est au tour de la zone Amérique d'être touchée[13] en 2014.

La solution à ce problème existe pourtant depuis quelques années puisqu'en 2003, il était déjà fait état de la future transition vers l'IPv6 et de ses avantages[14]. L'IPv6 est caractérisé par un espace d'adressage de 128 bits, ce qui procure un ensemble d'adresses internet pratiquement illimité. Les autorités publiques n'ont eu de cesse, ces dernières années, de prendre des dispositions pour encourager le passage à l'IPv6.

En 2008, la Commission européenne a pris un « Plan d'action pour le déploiement du protocole internet IP version 6 (IPv6) en Europe ». Cette action a pour but de favoriser la croissance de l'utilisation d'Internet. Ce plan d'action expose la situation actuelle et envisage les mesures à prendre par les différents acteurs de l'internet (organismes de régulation, fournisseurs d'accès internet, fournisseurs d'infrastructures etc.).

Lors de l'Assemblée mondiale de normalisation des télécommunications qui a eu lieu à Johannesburg en 2008 (AMNT-08), les Etats Membres de l' Union internationale des télécommunications (UIT) sont parvenus à un consensus et ont adopté la Résolution 64 intitulée « Attribution des adresses IP et encouragement du déploiement de l'IPv6 ». Cette résolution a pour objectif de sensibiliser l'opinion à l'épuisement des adresses IPv4 et

[12]ARCEP, « L'Autorité favorise le développement d'Internet en France », *arcep.fr*, mis en ligne le 13 février 2006, consulté le 11 février 2015.
[13]FILIPPONE D., « Pénurie d'adresses IPv4, la sonnette d'alarme est tirée », *Le monde informatique*, 24 juin 2014.
[14]POSEY B., « IPv4 contre IPv6 : les atouts du successeur », *ZDNet*, 3 juin 2003.

d'encourager la transition vers l'IPv6. Elle encourage également les Etats membres à établir des plans de mise en œuvre vers cette transition. En 2012, l'AMNT, qui s'est tenue cette fois à Dubaï, a révisé la Résolution 64 pour renforcer la transition et la mise en œuvre du protocole IPv6.

Pourtant l'adoption du protocole IPv6 ne va pas assez vite et le stock d'IPv4 est au bord de l'épuisement. Face à ce constat, l'ICANN, organisme de droit privé américain chargé d'attribuer les noms de domaine et les numéros sur internet, a également tiré la sonnette d'alarme pour encourager le passage à l'IPv6[15].

La France ne fait pas exception au retard mondial. Pourtant, en juillet 2014, « *une proposition de loi avait été déposée par une vingtaine de députés afin de tenter d'imposer l'IPv6 à tous les appareils connectés, et ce, dès le 30 juin 2015* »[16]. Mais ce texte n'est pas à l'ordre du jour. Cependant, récemment, Madame Corinne Erhel, membre de la commission des Affaires économiques a permis d'attirer de nouveau l'attention sur le sujet, en posant une question au ministère en charge du numérique. Cette dernière demandait « *dans quelle mesure l'État pourrait ouvrir la voie à une adoption plus rapide de cette nouvelle norme nécessaire au développement de ces filières en encourageant les constructeurs ainsi que les revendeurs-distributeurs à rendre compatibles les terminaux connectés tout en incitant à ce que les services en ligne soient eux aussi joignables en v6* »[17]. Le gouvernement a alors répondu que « *les acteurs économiques ayant décidé de déployer le protocole IPv6 ont pu se fournir auprès des grands équipementiers (…). Selon Google, en septembre 2014, 5,6 % de ses utilisateurs en France accèdent au moteur de recherche au travers d'une adresse IPv6, contre environ 4 % dans le monde et la France continue à être l'un des leaders mondiaux en termes d'adoption de l'IPV6 (…) ».* En comparaison, la Belgique obtient une moyenne de 28,6% d'utilisateurs, l'Allemagne 11,91% et les Etats-Unis 11,85%.

De plus, le gouvernement énonce qu'afin « *de mobiliser les administrations aux enjeux liés à la transition IPv4/Pv6, une circulaire interministérielle du 8 décembre 2011 a été diffusée demandant aux administrations d'intégrer la norme IPv6 dans leurs marchés publics d'achats de biens et de services faisant appel au protocole IP »,* ce qui n'annonce véritablement rien de concret.

Enfin, le projet de loi Macron « *pour la croissance et l'activité* »[18], examiné en ce mois de janvier 2015 par une commission spéciale, comporte une proposition de Corinne Enhel qui souhaitait obliger tous les équipementiers à vendre des terminaux compatibles avec la norme IPv6 à compter du 1er janvier 2017. La commission n'a pas approuvé sa proposition.

Emmanuel Macron a cependant déclaré que le gouvernement était d'accord avec cette ambition mais que celle-ci relevait davantage du droit communautaire. Le ministre s'est ainsi

[15] DUVAUCHELLE A., « Icann : IPv6, ça urge », *ZDNet.fr*, 23 mai 2014.
[16]GAVOIS S., « Questionné sur l'IPv6, le gouvernement botte une nouvelle fois en touche », *Nextimpact.com*, 3 décembre 2014.
[17]Question n° 58954, de Mme Corinne Erhel, publiée au JO – Assemblée Nationale, le : 01/07/2014 page : 5431
[18]Assemblée nationale, travaux préparatoires, Projet de loi pour la croissance et l'activité, n° 2447, déposé le 11 décembre 2014, mis en ligne le 11 décembre 2014 et renvoyé à une commission spéciale chargée d'examiner le projet de loi pour la croissance et l'activité.

engagé à saisir la Commission européenne « *dans les plus brefs délais* » à ce sujet. « *C'est à la fois une nécessité sur le plan technologique et industriel, et un élément de compétitivité pour notre économie »*[19].

L'adoption de l'IPv6 doit également passer par les fournisseurs d'accès internet (FAI)qui doivent rendre accessible cette technologie. Le 25 novembre 2014, l'ARCEP a publié un rapport sur la qualité du service fixe d'accès à l'internet[20] et remarque que *seuls Free et SFR offrent une connectivité IPv6 à leurs clients grands publics parmi les 5 opérateurs testés* » ; Orange, Numéricâble et Bouygues Télécom, étant encore cantonnés à l'IPv4.

Mais le problème principal de cette transition résulte dans le fait que l'IPv6 n'a pas été conçu pour être compatible avec l'IPv4. Lors du Forum mondial des politiques de télécommunication et des technologies de l'information et de la communication (FMPT-13), qui s'est réuni à Genève du 14 au 16 mai 2013, a été débattu puis adopté l'avis 4. Cet avis reconnaît que « *la transition de l'IPv4 à l'IPv6 nécessite obligatoirement de passer par une phase «double pile» au cours de laquelle les hôtes utilisent simultanément les deux protocoles, à savoir IPv6 pour communiquer avec d'autres hôtes IPv6, et IPv4 pour communiquer avec d'autres hôtes IPv4*[21] ». L'existence d'adresse IPv4 est donc nécessaire pour permettre le passage à l'IPv6.Selon plusieurs études, plus de 50 milliards d'objets seront connectés à internet d'ici 2020. Le déploiement du protocole IPv6 est donc considéré comme essentiel si l'Internet des objets devient une réalité.

Si l'IPV4 et l'IPV6 sont considérés comme incompatibles, les systèmes concernés par l'Internet des objets ne peuvent pas l'être ou le rester, au risque de créer un enchevêtrement de technologies au fonctionnement chaotique. Par conséquent, il faudrait que tous les systèmes puissent fonctionner en harmonie.

B. Une nécessaire harmonisation dans l'interopérabilité des systèmes

L'interopérabilité est la capacité que possède un système à fonctionner avec d'autres systèmes existants ou futurs, sans aucune restriction. En matière d'internet des objets, chaque industriel, chaque organisme de standardisation et de normalisation apporte sa pierre à l'édifice avec des technologies, des objets ou des normes différents, or tout ceci doit pouvoir fonctionner en harmonie.

L'internet des objets consiste à faire communiquer plusieurs systèmes entre eux, pour cela il est nécessaire d'utiliser des protocoles communs. Selon le rapport rendu par l'Institut National des Hautes Etudes de la Sécurité et de la Justice en décembre 2014, *« la mise en application, à une large échelle, du concept d'internet des objets apparaît largement tributaire d'une standardisation de la communication entre objets, dite M2M »*[22]. Plusieurs besoins apparaissent alors, le premier étant la constitution d'un langage commun constitué de

[19]BERNE X., « Fibre, IPv6, Open Data… Vote des premières mesures de la loi Macron », *NextINpact.fr,* janvier 2015.
[20]ARCEP, « Qualité du service fixe de l'accès à l'internet », *arcep.fr*, mis en ligne en le 13 novembre 2014.
[21]UIT, « Passage du protocole IPv4 au protocole IPv6 et adoption de ce dernier », itunews.itu.int.
[22]Institut national des hautes études de la sécurité et de la justice, Travaux des auditeurs « Sécurité des objets connectés, Décembre 2014, p14

protocoles de communication clairement définis. Ce langage commun ne pourra passer que par une standardisation. Nous verrons ainsi quelles sont les tentatives de standardisation pour créer l'interopérabilité (1) et quelles sont les procédés techniques pour y arriver (2)

1- Les tentatives de standardisation pour créer l'interopérabilité

Il est nécessaire de standardiser puisque les standards sont avant tout liés à des technologies telles que le Wi-Fi, le Bluetooth, et autres, qui permettent de communiquer. Le problème est que les organismes qui sont à l'origine des standards peuvent être spécialistes des normes, mais pas forcément des objets connectés.

De plus, certains organismes ont mis en place des standards liés à des secteurs d'activité particuliers qui correspondent à des besoins particuliers des technologies, or toutes les technologies ne fonctionnent pas de la même manière. L'existence d'un grand nombre de standards entraîne des incompatibilités entre ces derniers et des risques de confusion, de contradiction. Standardiser est une solution indispensable pour répondre à des questions d'interopérabilité, de communication mais il n'y a pas encore de standards applicables à toute technologie et à tout secteur.

Selon le Commissariat général à la stratégie et à la prospective dans son rapport sur « L'internet des objets : défis et perspectives pour la France et l'Europe » du 7 avril 2014 *« si l'Europe ne cherche pas à imposer des standards, elle subit une problématique de gouvernance »*[23].

Environ 140 organismes dans le monde s'intéressent actuellement à la normalisation de la communication machine-to-machine, cette activité de normalisation représentant en effet un élément primordial pour le développement de l'internet mobile vers l'internet des objets[24]. Il existe énormément de standards particuliers concernant des applications spécifiques, toutefois il est indispensable de prévoir des standards plus universels.

L'Union internationale des télécommunications, une agence de l'ONU a eu l'initiative la plus « universelle »[25]en juin 2012. Il s'agit de l'IoT-GSI : Internet of Things Global Standard Initiative.

L'organisme Global Standard1 aussi appelé GS1 s'est également intéressé à la standardisation, avec son initiative « EPC Global ». Cet organisme est une association à but non lucratif destinée à élaborer des standards, elle comporte des membres dans plus de 100

[23]Commissariat général à la stratégie et à la prospective, « L'internet des objets : défis et perspectives pour la France et l'Europe », 7 avril 2014, p18.
[24]Institut national des hautes études de la sécurité et de la justice, Travaux des auditeurs « Sécurité des objets connectés », Décembre 2014, p14
[25]Institut national des hautes études de la sécurité et de la justice, *ibid*.

pays, dont la France. Le système EPC pour Electronic Product Code est un identifiant individuel unique qui permet lui aussi d'identifier un produit électronique. L'EPC global Network définit l'organisation des systèmes d'informations destinés à assurer l'échange des informations EPC globablement. L'un de ses éléments principaux, l'ONS pour Object Naming Service, a été inspiré du DNS pour Domain Name System.
L'European Telecommunication Standards Institute, organisme à but non lucratif qui publie des normes de télécommunications, a publié trois spécifications pour les réseaux dédiés à la communication machine-to-machine et à l'Internet des objets. Cette publication intervient après une étude portée par des experts privés dont les sociétés Sigfox et Semtech.

Ces spécifications techniques concernent les réseaux de communication sans-fil bas-débit, c'est-à-dire les réseaux relatifs à la communication machine-to-machine. Les trois spécifications ont pour références GS LTN 001 pour le traitement des cas d'usage, GS LTN 002 pour ce qui concerne l'architecture des réseaux et GS LTN 003 pour les protocoles et les interfaces.

Le sigle LTN correspond à *LowThroughput Networks*, ces réseaux permettront de connecter des équipements électroniques, des objets connectés pour un coût dérisoire. Ces réseaux utilisent les fréquences basses, ce qui permettra de libérer la bande passante utilisée pour le réseau cellulaire et donc ne pas imposer de nouvelles infrastructures onéreuses pour l'Internet des objets. L'intérêt de ces réseaux est que les objets connectés ne consomment par définition que très peu de données et d'énergie. Le développement de ces normes permet de trouver une solution pour faire face au développement de l'Internet des objets et la nécessité de trouver des réseaux adaptés sans surchargés les réseaux existants.

A ces trois normes, le groupe de standardisation de l'European Télécommunication Standards Institute élabore quant à lui une norme pour la communication machine-to-machine sous le nom de TCM2M. Le deuxième besoin consiste à identifier électroniquement chaque objet connecté. Chaque objet connecté aura en effet une identification propre qu'il faudra pouvoir lire et transmettre via un protocole dans le réseau internet.

2- Les technologies existantes permettant l'interopérabilité

Concernant l'identification des objets connectés, deux technologies existent et peuvent répondre aux besoins d'interopérabilité. Il s'agit des puces RFID et des puces NFC. Le sigle RFID signifie en anglais « radio frequency identification », en français il s'agit d'identification de radio fréquences. Les puces RFID représentent une méthode utilisée pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » ou « RFID tag ». Les radio-étiquettes sont le plus souvent des étiquettes auto-adhésives incorporées dans des objets ou produits. Elles sont composées d'une antenne associée à une puce électronique, ce qui leur permet de recevoir et de répondre aux requêtes radio-émises depuis un émetteur-récepteur. Les informations peuvent être échangées sur une distance de 10 à 200mètres.

Ces puces RFID répondent au besoin d'identification des objets connectés puisqu'elles contiennent elles-mêmes un identifiant entre autres données. Cette technologie permet ainsi d'identifier des objets grâce à une étiquette électronique ou code-barres. Les puces RFID sont utilisées depuis des années pour les cartes d'accès aux transports publics, les télépéagesd'autoroutes notamment. Elles constituent une première réponse pour l'interopérabilité des objets connectés.

Il existe également les puces NFC, le sigle NFC désignant en anglais « Near Field Communication », ce qui signifie en français « Communication en champ proche ». Il s'agit d'une technologie de communication sans-fil à courte portée et haute fréquence qui permet l'échange d'informations entre des périphériques jusqu'à une distance d'environ 10cm. Les puces NFC découlent d'une extension de la norme ISO/CEI 14443 qui standardise les cartes de proximité en utilisant la RFID, ces cartes combinant l'interface d'une carte à puce et un lecteur au sein d'un seul périphérique. Les puces NFC sont capables de communiquer avec le matériel standardisé par la norme ISO précitée, avec un autre périphérique NFC et avec d'autres infrastructures sans-contact.

Ces puces NFC permettent de nombreux usages, tels que le paiement sans contact, la billetique. Cette technique n'est cependant utilisable que sur de très courtes distances, elle suppose donc une démarche volontaire de l'utilisateur.

Ces deux technologies participent ainsi au langage commun que l'internet des objets doit constituer. Elles participent en effet au développement de l'Internet en permettant à des objets de communiquer avec des équipements électroniques qui seront connectés au réseau. Elles sont déjà utilisées et utilisables à l'international.

À ces deux technologies efficaces et utiles pour l'Internet des objets s'ajoutent les technologies déjà existantes du Bluetooth et du Wi-fi. Le Bluetooth est une technologie, un standard de communication basse consommation. Il permet de simplifier les connexions entre des appareils électroniques, des objets connectés en supprimant les liaisons par fil.

L'avantage du Bluetooth est sa très faible consommation d'énergie et son coût très bas. Il est utile pour l'interopérabilité puisqu'il permet la communication entre deux appareils électroniques et donc deux objets connectés à partir du moment où ces deux appareils ont l'option Bluetooth.

Le Wi-Fi désigne des protocoles de communication sans-fil qui découlent des normes IEEE 802.11. Cette norme est utilisée à l'international pour caractérisée tous les réseaux locaux sans fil. « Wi-Fi » est une marque déposée et c'est la Wi-Fi Alliance qui est l'organisme chargé de s'occuper de l'interopérabilité entre les matériels conformes aux normes IEEE 802.11. Un réseau Wi-Fi est donc en réalité un réseau qui répond à ces normes IEEE. Le réseau Wi-Fi est utilisable à l'international pour toute connexion internet, il est donc

interopérable pour un usage dans l'Internet des objets.

Ces quatre technologies correspondent à des normes qui permettent de répondre aux besoins d'interopérabilité de l'Internet des objets.

Tous ces efforts de standardisation ne permettent pas encore d'avoir uniquement des normes universelles et des systèmes qui permettent une communication parfaite entre chaque machine.Il existe encore une forte indécision dans le monde industriel, par conséquent des industriels de l'informatique et de l'électronique s'allient afin de réfléchir à des standards pour l'internet des objets. C'est le cas des très grosses entreprises américaines AT&T, Cisco, General Electric, IBM et Intel qui se sont associées en mars 2014.

Une parfaite interopérabilité des systèmes semble alors pour le moment utopique. Le directeur général France de Global Standard1, Pierre Georget a d'ailleurs affirmé *« il y aura certainement plusieurs réseaux dédiés à des applications spécifiques. Ces réseaux devront cohabiter mais l'interopérabilité ne sera pas forcément totale ».* [26]

Certains défis techniques ne sont donc pas encore tout à fait relevés pour assurer le développement de l'Internet des objets parallèlement à l'existence de systèmes et de réseaux adéquats. Or à côté de ces défis techniques, il est nécessaire que des garanties juridiques soient assurées pour que les réseaux dans l'internet des objets puissent fonctionner.

[26]ARCEP, « La lettre de l'autorité de régulation des communications électroniques et des postes », Janvier-Février 2009, www.arcep.fr, p21.

PARTIE II

DES GARANTIES JURIDIQUES NECESSAIRES AU BON FONCTIONNEMENT DES RESEAUX DANS L'INTERNET DES OBJETS

Avec l'arrivée de l'internet des objets, les garanties prévues par le droit positif ne semblent pas toujours suffire. En effet, plusieurs problématiques se posent notamment concernant la responsabilité des acteurs, de la mise en réseau de l'objet ou encore de la sécurité des réseaux. On observera dans un premier temps qu'il existe une mutabilité de la responsabilité des acteurs des réseaux (A). Nous verrons dans un deuxième temps qu'il est nécessaire de garantir une utilisation sereine et sûre des réseaux (B).

A. Une mutabilité de la responsabilité des acteurs des réseaux

« *Internet est considéré comme un espace de liberté mais liberté rime aussi avec responsabilité*[27] ».

D'ici quelques années, il conviendra certainement d'adapter la législation à l'internet des objets, puisque les objets connectés vont prendre une part de plus en plus importante dans le monde du numérique. Leur future place prépondérante amène à se demander quelles seront les conséquences si le réseau est défaillant et qu'il ne permet plus aux objets d'être connectés entre eux. Cette interrogation amène donc à la notion de responsabilité.

La responsabilité est une notion bien implantée dans la législation française. Sur internet, la détermination de la responsabilité dépendra de la qualité de la personne. Il convient de voir à présent quelle sera la responsabilité des différents acteurs présents sur le réseau que sont les FAI (1), les hébergeurs (2), les éditeurs (3), en se basant sur des textes existants et de s'interroger sur la responsabilité concernant les produits défectueux (4).

1- La responsabilité des fournisseurs d'accès internet (FAI)

Le FAI offre un accès pour permettre la connexion à des services en ligne. La loi portant confiance en l'économie numérique (LCEN) du 21 juin 2004 a défini son régime. Sa responsabilité est contractuelle. Tout d'abord, l'article 15 de la LCEN dispose que le FAI est responsable de plein droit à l'égard de l'acheteur, de la bonne exécution des obligations résultant du contrat, que ces obligations soient exécutées par lui-même ou par d'autres prestataires de service.

Le juge y a vu une obligation de résultat dans l'arrêt de la première chambre civile de la Cour de cassation du 19 novembre 2009 concernant Free. La cour énonce qu'il *« doit assurer les services promis, sans pouvoir rejeter la responsabilité d'une mauvaise exécution sur un autre intervenant »*.Il ne peut donc pas s'exonérer de sa responsabilité à l'égard de son client en raison d'une défaillance technique, sauf cas de force majeure évidemment.

[27]Anonyme, « Responsabilité sur le web », *eduscol.fr*, consulté le 11 février 2015.

Le FAI a également une obligation de conservation des données de connexion à l'égard des internautes. Cette obligation résulte du système de l'internet où les FAI sont en position de connaître les sites qui ont été consulté par un internaute et à ce titre, la LCEN organise la conservation par les FAI des données de connexion. Cette conservation date de la loi de 2001 relative à la sécurité quotidienne, loi relative au terrorisme.

Il ne devrait donc pas y avoir de difficultés à faire appliquer cette responsabilité à l'internet des objets.

2- La responsabilité des hébergeurs

Les hébergeurs fournissent un service permettant la mise en ligne et la mise à disposition au public d'un contenu, c'est un prestataire technique comme le FAI. La fonction d'hébergement permet de donner un espace machine c'est-à-dire qu'elle consiste à stocker sur des serveurs, connectés en permanence aux réseaux, des données informatiques.

La responsabilité des hébergeurs est limitée et aménagée. Comme ils n'ont pas l'obligation générale de surveiller les contenus présents sur leur site, ils ne seront responsables que s'ils ont été au courant de l'existence d'un contenu illicite sur leur site et qu'ils ne l'ont pas retiré rapidement à partir du moment où ils ont été informés de l'existence de ce contenu, lors de la notification. Les conditions sont inscrites dans l'article 6 I-2 de la LCEN. Cet article dispose que « *les personnes physiques ou morales qui assurent la fonction d'hébergeur ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ses services si elle n'avait pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si dès le moment où ils en avaient eu cette connaissance, elles ont agis promptement pour retirer ces données ou en rendre l'accès impossible* ».

L'article 6 I-5 dispose que la connaissance des faits litigieux est présumée acquise par l'hébergeur lorsqu'il est destinataire d'une notification donc de l'existence du contenu. Cette notification est le point de départ de la procédure visant à supprimer un contenu illicite. La responsabilité de l'hébergeur est subsidiaire donc on doit montrer qu'on a recherché préalablement la responsabilité de l'éditeur. En pratique, la lettre de notification à l'hébergeur suit immédiatement la lettre de notification à l'éditeur. Cette notification crée une présomption de connaissance dans la mesure où elle doit être faite par des moyens permettant d'assurer la date certaine de l'envoi et de la réception de cette notification.

3- La responsabilité des éditeurs

L'éditeur est celui qui met en ligne un contenu, mis à la disposition du public, sur un service qu'il a créé ou dont il a la charge. La loi du 29 juillet 1982 sur la communication audiovisuelle, modifiée par la loi du 12 juin 2009, évoque l'éditeur mais en tant que créateur de contenu. La LCEN est également restée flou concernant leur statut. La réponse adéquate pour les objets connectés pourrait alors se trouver à l'article 1384 du code civil qui prévoit

que l'on est responsable du dommage qui est causé par le fait des choses que l'on a sous sa garde.

4- La responsabilité du fait des produits défectueux

L'article 1386-4 du code civil précise que le produit est défectueux lorsqu'il n'offre pas la sécurité à laquelle on peut légitimement s'attendre.
En ce qui concerne les vices cachés, le code civil définit le vice comme étant celui rendant la chose impropre à l'usage auquel on la destine ou qui diminue tellement cet usage que l'acheteur ne l'aurait pas acquise ou en aurait donné un moindre prix.

La loi du 19 mai 1998 a transposé dans le droit français la directive européenne du 25 juillet 1985 relative à la responsabilité du fait de produits défectueux. Ainsi, la loi définit les responsables comme le fabriquant du produit fini (ou d'une partie composante), et le producteur d'une matière première. Concernant les vices cachés, le code civil ne vise que le vendeur.

Cette responsabilité du fait des produits défectueux pourra donc certainement s'appliquer aux objets connectés.

A côté des garanties de la responsabilité des acteurs des réseaux, il est aussi nécessaire de garantir une utilisation sereine et sûre des réseaux pour permettre le bon fonctionnement de l'internet des objets.

B. Une nécessité d'assurer une utilisation sereine et sûre des réseaux

Comme il a été démontré tout au long de ce rapport, l'approche juridique et technique sont souvent complémentaires lorsqu'on aborde la question des réseaux, en particulier en ce qui concerne l'internet des objets. En l'occurrence, des garanties juridiques sont nécessaires à la mise en réseau de l'objet connecté (1) et à la sécurité des réseaux (2) mais nous verrons que ces garanties juridiques nécessitent bien souvent en amont des innovations techniques.

1- Les garanties liées à la mise en réseau de l'objet connecté

Les objets connectés vont par définition devoir utiliser un réseau de communication électronique et donc passer par un opérateur qui propose un tel service. Les opérateurs ont un rôle primordial notamment car ils sont les garants auprès des utilisateurs de la bonne communication des objets connectés, ainsi que de la récolte des informations et des mises à jour, etc. C'est les opérateurs qui vont devoir garantir la mise en en réseau des objets connectés.

L'article 32 quinzièmement du code des postes et des communications électroniques définit l'opérateur comme « *une personne physique ou morale exploitant un réseau de communication électronique ouvert au public ou fournissant un service de communication électronique*».

La notion d'opérateur est très générale car elle concerne tant les opérateurs de réseaux que les opérateurs de service. Structurellement, beaucoup d'opérateurs de réseaux sont des opérateurs de services et ces opérateurs bénéficient à plein de la liberté de communication. En matière de police, l'exigence qui s'impose aux opérateurs, c'est une simple déclaration d'activité auprès de l'ARCEP. Cette déclaration entraine le bénéfice d'une série de droit et la mise à la charge de certaines obligations.

A priori, l'arrivée de l'internet des objets ne devrait pas modifier le statut des opérateurs ou le régime qui leurs est applicable. Cependant, il faut tout de même observer qu'avec l'arrivée de l'IDO, de nouvelles garanties sont nécessaires (1.1). Face à cela, plusieurs solutions sont proposées (1.2) sans qu'aucune n'englobe entièrement toute la problématique.

1.1- Les nouvelles garanties nécessaires à la mise en réseau de l'objet connecté

Pour que l'objet puisse passer par le réseau d'un opérateur, dans bien des cas, c'est la carte SIM intégrée dans l'objet qui permet d'accéder au réseau de l'opérateur choisi. La carte SIM est une puce électronique, contenant un microcontrôleur et une mémoire[28].

La carte permet à l'opérateur de stocker les informations spécifiques à l'abonné de son réseau. Le choix de l'intégration d'une carte à puce dans les systèmes est basé sur la nécessité de disposer « d'un élément sécurisé contenant l'identifiant et les données de connexion d'un utilisateur donné, d'un élément amovible permettant de personnaliser un nouveau téléphone avec les données de connexion ; l'intérêt est de séparer le choix d'un terminal de la notion d'abonnement ; d'un un espace de stockage d'information pour les données personnelles de l'abonné, mais également des paramètres de personnalisation de son terminal et enfin d'un espace pour les applications de l'opérateur»[29].

A l'heure actuelle, la majorité des cartes SIM qui sont fabriquées sont « verrouillées » et permettent aux opérateurs de limiter l'utilisation de la carte SIM uniquement à leur réseau. Il s'agit de cartes SIM dites « cartes SIM propriétaires ». Ainsi, lorsqu'un utilisateur change d'opérateur, il doit changer également sa carte SIM. Or, le principal problème qui se pose est certainement le fait que la plupart des objets connectés qui sont fabriqués rendent inaccessibles la carte SIM qui est intégrée dans chaque objet. Plusieurs garanties sont pourtant nécessaires pour l'utilisateur.

D'abord, il faut pouvoir changer d'opérateur facilement, sans avoir besoin de changer de carte SIM, puisque, comme il a été dit précédemment, la majorité des objets connectés n'auront pas une carte SIM aussi facilement changeable comme, à titre d'exemple, les cartes SIM que l'on connait pour les téléphones mobiles. Ensuite, il est important de soulever le fait que les propriétaires d'objets connectés seront sans aucun doute amener à se déplacer dans le monde ; et avec eux, les objets connectés. Il faut donc pouvoir assurer la fonctionnalité de l'objet,

[28] ANONYME, « Définition de la carte SIM », *wikipédia.org*, 28 novembre 2014.
[29] ANONYME, « Définition de la carte SIM », *wikipédia.org*, 28 novembre 2014.

même à l'étranger. Or, la plupart des opérateurs n'ont pas de réseau à l'international. Enfin, il faut pouvoir assurer aussi la fonctionnalité de l'objet même en cas de défaillance du réseau de l'opérateur. Cela est essentiel, notamment par exemple pour les objets connectés dont le fonctionnement 24 heures sur 24 va devenir parfois une obligation d'ordre vitale. Les SIM propriétaires peuvent donc se révéler être un frein pour le développement de l'internet des objets et à son bon fonctionnement.

1.2 – Les solutions envisagées aux nouvelles garanties de mise en réseau

Plusieurs solutions sont envisagées en grande partie par les industriels. En premier lieu, on pourrait envisager que les fabricants d'objets aient leur propre carte SIM[30] donc des cartes SIM non verrouillées afin de pouvoir changer d'opérateur quand ils le décident. Cependant, il faudrait alors une modification de la recommandation UIT-T E.212 qui dispose que « les MNC ne doivent être attribués qu'aux réseaux publics offrant des services de télécommunications publics, et ne doivent être utilisés que par ces réseaux ». Ainsi, cette recommandation réserve l'allocation de cartes SIM aux opérateurs de télécommunications et ce qui exclut donc les fabricants d'objets connectés.

Ensuite, il existe aussi une solution qui vient de l'initiative privée. C'est celle du développement de carte SIM dite « universelle » que proposent par exemple la start-up française MATOOMA. L'entreprise a en effet réussi à mettre au point une carte SIM qui permet en principe de rejoindre le réseau de n'importe quel opérateur dans le monde, sans changer de carte SIM. L'avantage, c'est que la carte SIM utilise la technologie dit de la « radio intelligente » qui permet de rejoindre le meilleur réseau disponible. Cela permet d'assurer la fonctionnalité de l'objet à l'étranger et de façon permanente. Ainsi, lorsque le réseau de l'opérateur auquel est connecté l'objet est défaillant, la carte SIM change automatiquement de réseau.

Enfin, la dernière solution vient de la GSMA. La GSMA est une association qui représente 850 opérateurs de téléphonie mobile à travers 218 pays du monde et 200 fabricants et autres industriels du secteur des réseaux GSM et dérivés. L'association a adopté le 14 octobre 2014 une spécification concernant une carte SIM intégrée, fiable, et modifiable à distance. Il s'agit de la spécification GSMA eUICC Embedded SIM[31]. Cette solution permet d'intégrer la carte dans l'objet dès sa fabrication et le profil de l'abonné pourrait être mis à jour et modifiable en fonction de l'opérateur et de l'offre choisie par le consommateur. Plus aucune manipulation physique ne sera nécessaire pour rendre l'objet communicant, il suffira seulement de la programmer.

Il faut souligner ici que cette spécification est, à l'heure actuelle, seulement envisagée pour l'internet des objets. Les opérateurs font preuve d'une grande prudence concernant cette spécification et souhaitent limiter cette possibilité aux « nouveaux objets » afin que cela

[30] ENTRAYGUES (A.), « Objets communiquants, le droit saura-t-il répondre ? », *Expertises*, Octobre 2014, p. 335.
[31] ELYAN (J.), « Cartes SIM inamovibles, une aubaine pour le marché de l'Internet des objets », *lemondeinformatique.fr*, 14 octobre 2014.

n'affecte pas les téléphones portables, les ordinateurs ou encore les tablettes[32] car cela conduirait les opérateurs à perdre la maîtrise qu'ils ont sur leurs clients.

Selon un rapport[33] publié par Beecham Research, l'adoption de la spécification GSMA eUICC Embedded SIM va entraîner une augmentationdes ventes d'objets connectés de 34 % d'ici à 2020. Le rapport prévoit que l'adoption de cette spécification générera environ 8,9 milliards de dollars US de revenus issus des services de connectivité pour les opérateurs de téléphonie mobile rien qu'en 2020. De plus, le rapport estime que dans le cas où cette spécification est adoptée en tant que norme de fait, le marché des connexions SIM intégrées pourrait couvrir 639 millions de connexions à l'échelle mondiale. Il s'agirait d'une hausse d'environ 478 millions d'ici à 2020.

Lors de la conférence Mobile 360 d'Octobre 2014 qui a eu lieu à Dubaï, la GSMA a annoncé que « les plus grands opérateurs de téléphonie mobile AT&T, Etisalat, NTT DOCOMO, Telefónica et Vodafone Group, aux côtés des fabricants de cartes SIM et de modules Gemalto, Giesecke&Devrient, Morpho, Oberthur Technologies, Sierra Wireless et Telit, ont tous lancé des solutions conformes à la spécification GSMA Embedded SIM pour la fourniture « sans fil » à distance d'appareils machine-machine (M2M) »[34].

De même que pour les garanties liées à la mise en réseaux de l'objet connecté, il faut aussi assurer des garanties liées à la sécurité des réseaux de l'objet connecté afin de ne pas freiner leurs développements. Une fois de plus, il s'agit des garanties essentielles au bon développement et fonctionnement de l'internet des objets.

2- Les garanties liées à la sécurité des réseaux de l'objet connecté

L'annonce du développement à venir de l'Internet des objets amène nécessairement à prendre en compte les risques inhérents aux nouvelles technologies développées. L'Internet des objets va avoir de très nombreuses applications, dans des domaines variés du quotidien, par conséquent toutes ces mises en œuvre de l'Internet des objets dans notre environnement impliquent une fiabilité et une sécurité des communications entre les objets. Les solutions liées à la sécurité seront abordées (2.2) après avoir exposé dans un premier temps la problématique de la fiabilité des réseaux existant (2.1).

2.1- La problématique de la fiabilité des réseaux existants

L'internet des objets implique la communication d'objets entre eux à l'aide de réseaux sans fil, or ces réseaux sont aujourd'hui encore très vulnérables face à d'éventuelles intrusions malveillantes. Dans une logique de communication machine-to-machine, il est très difficile d'identifier si tous les composants du réseau qui interagissent entre eux sont viables ou non.

[32] GODELUCK (S.), « La carte à puce du mobile fait sa révolution », *Lesechos.fr*, 19 février 2013.
[33] BEECHAM RESEARCH, *Analyse des avantages de la spécification GSMA Embedded SIM pour l'industrie des produits mobiles compatibles avec la technologie M2M*, rapport indépendant, 11 octobre 2014.
[34] ANONYME, « Mobile 360 Middle Est », *Businesswire.com*, 14 octobre 2014.

Le colonel Philippe Davadie a précisé lors du Colloque du 19 septembre 2014 sur « La sécurité de l'Internet des objets », *que « l'explosion combinatoire des objets connectés à venir va déplacer le paradigme de la sécurité au-delà de ces équipements, vers les réseaux qui les traitent. Sur le plan de la sécurité, chaque objet deviendra une porte d'entrée possible pour une intrusion sur le réseau »*[35].Il semblerait que l'arrivée des objets connectés puisse entraîner des risques d'intrusions sur les réseaux et déplacer le problème de la sécurité des objets en eux-mêmes vers des problèmes de sécurité des réseaux utilisés par ces objets.

La sécurité des objets connectés constitue donc un véritable enjeu. En effet selon l'Institut National des Hautes Etudes de la Sécurité et de la Justice, « la diffusion croissante de ces objets génère également de nouveaux risques pour la sécurité numérique des institutions des entreprises et des particuliers qui appellent de nouvelles réponses »[36].

L'Internet des objets a d'ailleurs été rebaptisé *« l'Internet des vulnérabilités »*[37]par Symantec, une société américaine fondée en 1982 et qui est spécialisée dans les logiciels informatiques.
Pour prouver cette vulnérabilité, l'entreprise HEWLETT-PACKARD et sa division Fortify ont testé la sécurité de dix objets connectés du quotidien, chacun de ces objets communiquaient avec un service cloud et des applications mobiles. Le rapport intitulé « Internet of ThingsResearchStudy » rendu en 2014 a mis en évidence que chacun des objets testés comportait 25 points faibles dans leur fonctionnement et dans la sécurité du réseau utilisé. Cela constitue un total de 250 points faibles pour 10 objets. Selon ce même test, 76% des appareils testés utilisaient des services de réseau non sécurisés.

Non seulement les objets connectés comportent en eux-mêmes des points faibles et ne fonctionnent pas sur des services de réseau sécurisés, mais en plus les hackers sont de plus en plus performants et ne se retiennent pas de prouver eux-aussi la vulnérabilité de la sécurité des réseaux de l'Internet des objets. Ainsi lors de la Conférence Black Hat en 2014 (conférence américaine portant sur la sécurité de l'information, composée d'experts en sécurité et de hackers), des chercheurs en sécurité ont réussi à pirater un Thermostat connecté de la marque NEST en seulement 15 secondes.

De nombreux autres hackers ont également réussi à pirater des voitures connectées, des grilles pains connectés et bien d'autres objets de notre quotidien. Il apparaît donc indispensable de sécuriser les réseaux, les systèmes utilisés par les objets connectés, à défaut, l'Internet des objets pourrait devenir une nouvelle réalité très dangereuse.

2.2- Les solutions potentielles pour parvenir à une sécurisation des réseaux

Ces solutions ne sont pour l'heure ni juridiques, ni très nombreuses. C'est le gros point noir

[35]Chaire de cyberdéfense et cybersécurité, *La sécurité de l'Internet des objets*, Synthèse du colloque, 19 septembre 2014, Paris, p3.
[36]SCHOTT (C.), « Sécurité des objets connectés, Décembre 2014, INHESJ, p13.
[36]BOULESTIN (R.), « L'Internet des Objets ? Plutôt l'Internet des vulnérabilités pour Symantec », *silicon.fr*, 2 décembre 2013.

de l'Internet des objets. Il est en effet regrettable que les autorités européennes se soient pour l'instant concentrées sur la question de la protection des données personnelles, sans prendre suffisamment en compte la mise en place d'un réseau sécurisé. Le Groupe de l'article 29 a en effet rendu des recommandations les 16 et 17 septembre 2014 sur la question de la protection des données personnelles mais il ne s'est pas prononcé sur la question de la sécurité indispensable des réseaux sur lesquels les données vont circuler et être échangées.

Bien que les autorités européennes ne se soient pas prononcées sur la nécessité de proposer des réseaux sécurisés pour accompagner le développement de l'Internet des objets, différents acteurs peuvent agir pour tenter de sécuriser un minimum les systèmes.

Une implication importante des fabricants, des fournisseurs d'objets connectés est tout d'abord indispensable. Ils doivent en effet prendre en compte tous les risques liés à l'hyper connexion dont va découler l'utilisation des objets connectés. Cela peut se traduire notamment par l'utilisation de technique de sécurisation des objets connectés telles que le cryptage, l'authentification, ou encore le concept du « privacy by design » qui consiste à sécuriser l'objet dès sa conception afin qu'il soit sûr dès l'origine. Cela peut aussi se traduire par une information des futurs consommateurs sur les risques liés à l'utilisation des objets et à leur connexion aux réseaux. Les industriels peuvent également s'associer avec des acteurs de la sécurité informatique.

Si les fabricants doivent s'investir dans la sécurité, une implication des utilisateurs d'objets connectés est également tout aussi nécessaire. Les utilisateurs doivent être conscients des risques liés à la sécurité lorsqu'ils utiliseront leurs objets connectés.
Cette conscience des risques doit s'accompagner d'une utilisation avisée des objets connectés et de toutes les fonctions de sécurité dont les appareils disposent.

Didier Appell, Directeur de l'offre cyber sécurité de Sogeti High Tech, filiale du groupe Capgemini et pôle d'excellence de l'ingénierie et du Conseil en Technologie a précisé que *« l'un des enjeux du développement de l'Internet des objets est la possibilité de rendre interopérables des équipements dotés de protocoles de communications différents sans être la source de vulnérabilités »*.[38]Pour l'instant, cet enjeu en demeure un.

En effet, l'implication des fabricants, des utilisateurs ne suffira pas pour que les réseaux de l'Internet des objets soient sécurisés. Les opérateurs de télécommunications devront respecter leurs obligations portant sur la qualité du service qu'ils proposent en assurant la permanence, la disponibilité et la qualité du réseau et des services. Ils doivent également assurer l'intégrité des communications qui empruntent les réseaux, tous les opérateurs ont l'obligation d'informer leur client des conditions de sécurité de leur réseau ainsi que des risques pouvant peser sur les réseaux. Ainsi en septembre 2014, l'opérateur Orange avait averti plusieurs centaines de milliers de ses abonnés que leurs mails avaient été détournés par des pirates informatiques.

[38]ANONYME, « Quelle sécurité pour l'Internet des objets ? », *www.thalesgroup.com*, 17 septembre 2014.

Tout le matériel, tous les logiciels et toutes les installations doivent être protégés. La sécurité des réseaux de télécommunications implique aussi la transparence des conditions de mise en œuvre de la sécurité. C'est pour cette raison que les opérateurs doivent publier des spécifications techniques relatives à leur réseau. Ces spécifications sont le résultat de négociations internationales et elles doivent être communiquées à tous les constructeurs de terminaux dans le souci d'appliquer des normes communes afin que tout terminal, qu'il soit émetteur ou récepteur puissent transporter dans les mêmes conditions de sécurités toutes les communications.

L'Union Internationale des Télécommunications devra certainement intervenir afin de se positionner sur l'encadrement juridique de la sécurité indispensable de ces réseaux. La recommandation UIT-T Y.2061 de juin 2012 prévoit tout de même la prise en charge d'applications de communication orientées machine dans l'environnement des réseaux de prochaine génération. Deux concepts apparaissent alors essentiels à la sécurité des réseaux, il s'agit des fonctions d'authentification et d'autorisation. Selon cette recommandation, toutes les applications de communication orientées machine doivent proposer des fonctions d'authentification et d'autorisation pour l'accès des données, pour la connexion à un réseau local, etc.

Les concepts d'authentification et d'autorisation sont ainsi à mettre en œuvre pour la sécurité des systèmes dans l'Internet des objets mais entre ce qui doit être fait et ce qui est fait, il y a souvent un écart significatif et d'autant plus problématique.

Tous les Etats et gouvernements devront se positionner et se rendre en compte des risques liés à la connexion de milliards d'objets à des réseaux non préparés. L'hyperconnexion des objets aura nécessairement des répercussions sur l'Etat français puisque ce dernier est chargé d'assurer « la paix, la tranquillité et la sécurité publiques à l'intérieur de ses frontières »[39].

En conclusion, ce nouveau volet des réseaux correspond à un marché qui laisse place à de nouveaux opérateurs, ce qui aura des conséquences sur la réglementation. A l'heure actuelle, on peut cependant affirmer que le droit des réseaux existant n'est pas totalement prêt à l'arrivée massive des objets connectés. Comme bien souvent, le droit intervient postérieurement aux avancés technologiques.

***

[39]DAVADIE (P), « Objets connectés : quels enjeux pour la sécurité et la sûreté », septembre 2014, www.chaire.cyber.fr, p4.

BIBLIOGRAPHIE

ARTICLES

- ANONYME, « Quelle sécurité pour l'Internet des objets ? »,*thalesgroup.com*, 17 septembre 2014.

- ANONYME, « Mobile 360 Middle Est », *businesswire.com*, 14 octobre 2014.

- ARCEP, « L'Autorité favorise le développement d'Internet en France », *arcep.fr*, 13 février 2006.

- ARCEP, « La lettre de l'autorité de régulation des communications électroniques et des postes », *arcep.fr*,Janvier-Février 2009.

- BERNE X., « Fibre, IPv6, Open Data… Vote des premières mesures de la loi Macron », *NextINpact.fr*, 19 janvier 2015.

- BOULESTIN (R.), « L'internet des objets ? Plutôt l'internet des vulnérabilités pour Symantec », *silicon.fr*, 2 décembre 2013.

- CHAPERON (I.), « Levée de fonds record pour la start-up française Sigfox », *lemonde.fr*, 11 février 2015.

- DAVADIE (P.), « Objets connectés : quels enjeux pour la sécurité et la sûreté », *chaire.cyber.fr*, septembre 2014.

- DUVAUCHELLE A., « Icann : IPv6, ça urge », *ZDNet*, 23 mai 2014.

- ELYAN (J.), « Cartes SIM inamovibles, une aubaine pour le marché de l'Internet des objets », *lemondeinformatique.fr*, 14 octobre 2014.

- ENTRAYGUES (A.), « Objets communiquants, le droit saura-t-il répondre ? », *Expertises*, Octobre 2014.

- FILIPPONE D., « Pénurie d'adresses IPv4, la sonnette d'alarme est tirée », *Lemondeinformatique.fr*, 24 juin 2014.

- GAVOIS S., « Questionné sur l'IPv6, le gouvernement botte une nouvelle fois en touche », *Nextimpact.com*, 3 décembre 2014.

- GODELUCK (S.), « La carte à puce du mobile fait sa révolution », *Lesechos.fr*, 19 février 2013.

- MALE (O.), « Sigfox, technologie de rupture pour le M2M », domotique-info.fr, 25 février 2015.

- MOREAU (M.), « Sigfox, le google de demain », *frenchweb.fr*, 4 décembre 2012.

- POSEY B., « IPv4 contre IPv6 : les atouts du successeur », *ZDNet,* 3 juin 2003.

RAPPORT

- ARCEP, *Qualité du service fixe de l'accès à l'internet*, Rapport de l'ARCEP, novembre 2014, 45p.

- BEECHAM RESEARCH, *Analyse des avantages de la spécification GSMA Embedded SIM pour l'industrie des produits mobiles compatibles avec la technologie M2M*, Rapport indépendant, 11 octobre 2014, 29p.

- BENGHOZI (P.), BUREAU (S.), MASSIT-FOLEA (F.), *L'Internet des objets. Quels enjeux pour les Européens ?*, Rapport de la chaire Orange "innovation and régulation", Ecole polytechnique et TELECOM, Paris Tech. 2008, 65p.

- CHAIRE DE CYBERDEFENSE ET CYBERSECURITE, *La sécurité de l'Internet des objets*, Rapport de synthèse sur le colloque sécurité de l'IDO, 19 septembre 2014, Paris, 5p.

- COMMISSARIAT GENERAL A LA STRATEGIE ET A LA PROSPECTIVE,*L'internet des objets : défis et perspectives pour la France et l'Europe,*Rapport rendu le 7 avril 2014, 35p.

- INSTITUTION NATIONAL DES HAUTES ETUDES DE LA SECURITE ET DE LA JUSTICE, *Sécurité des objets connectés*, Rapport sur les Travaux des auditeurs, Décembre 2014, 64p.

- PEZ (T.),« L'incidence du partage du spectre sur le droit français applicable aux fréquences radioélectriques », *in Une gestion dynamique du spectre pour l'innovation et la croissance,* Rapport de la Mission ministérielle sur le spectre hertzien confiée au professeur Joëlle Toledano,31 mars 2014, pp. 93-118.

- SCHOTT (C.), *Sécurité des objets connectés*,Rapport INHESJ, décembre 2014, 64p.

- TOLEDANO (J.), *Une gestion dynamique du spectre pour l'innovation et la croissance*, rapport de la Mission ministérielle sur le spectre hertzien, 31 mars 2014, 128 p.

DEBATS ET QUESTIONS PARLEMENTAIRES

- Question n° 58954, de Mme Corinne Erhel, publiée au JO – Assemblée Nationale, le 1er juillet 2014, page 5431

- Assemblée nationale, travaux préparatoires, Projet de loi pour la croissance et l'activité, n°2447, déposé le 11 décembre 2014, mis en ligne le 11 décembre 2014 et renvoyé à une commission spéciale chargée d'examiner le projet de loi pour la croissance et l'activité.

SITE INTERNET

www.anfr.fr

www.arcep.fr

www.cnes.fr

www.csa.fr

www.larousse.fr/encyclopedie

www.numerama.com

www.reseaux-telecoms.net

www.wikipédia.fr

www.zdnet.fr

TABLE DES MATIERES