MISSIONS ÉCONOMIQUES

Mission pour la Science et la Technologie

AMBASSADE DE FRANCE AUX ETATS-UNIS

Revue « Science & Technologies de l'Information et de la Communication » Etats-Unis

N°4 – Janvier 2006

Dossier

Le RFID aux Etats-Unis

Auteurs de l'article
sebastien.morbieu@ambafrance-us.org

jean-philippe.lagrange@ambafrance-us.org

1. Introduction

Le nom RFID recouvre en fait un ensemble de technologies et d'applications très variées. Portée, bande de fréquences utilisée, prix, encombrement, consommation d'énergie sont des facteurs qui les différencient. Davantage que des équivalents au code barres interrogeables par ondes radio (ou *smart labels* ou EPC pour *Electronic Product Code*), les marqueurs RFID peuvent fournir des informations issues de capteurs, ou des données enregistrées et modifiables. Des systèmes plus évolués permettent aussi une communication entre marqueurs. Un *système* RFID est ainsi constitué de marqueurs/capteurs, de lecteurs, le cas échéant d'un réseau sans fil connecté à un réseau classique, d'un middleware adapté à l'utilisation (collecte des informations, intégration etc.), de services adaptés à l'emploi considéré, côté utilisateur final, ainsi que d'outils de gestion. Aux Etats-Unis, la technologie RFID se répand à une vitesse accélérée ces dernières années. Il est annoncé qu'elle représenterait une activité de plusieurs milliards de dollars (engendrant des économies de plusieurs milliards de dollars dans les chaînes logistiques). La technologie qui suscite le plus d'intérêt actuellement est celle qui utilise les ultra hautes fréquences, bon compromis entre vitesse de lecture, portée, présence de plusieurs marqueur et coût. Un cap important a été franchi fin 2004 avec l'adoption de l'*EPC Generation 2* (initialement mis au point par Intermec Technologies, Everett-Washington, la version d'origine EPC ayant été créée par le MIT Auto-ID Lab) comme norme ouverte par l'EPC Global, ainsi que celle du portefeuille complet de la norme ISO/IEC 18000:2004, complété par ISO/IEC TR 24710:2005.

2. Applications déployées

Des composants RFID sont utilisés pour le péage autoroutier sur de nombreux réseaux et comme carte de paiement pour certaines stations d'essence Exxon. Cette technologie est également utilisée pour l'identification des animaux (au départ en 125 kHz, puis en 134,2 kHz standard international). Le RFID est notamment utilisé par suite du « *National Farm Animal Identification and Records* », qui a concerné plus d'un million de têtes de 1999 à 2004. Par ailleurs, plusieurs sociétés proposent des systèmes RFID (incompatibles) pour l'identification des animaux de compagnie, qui sont bien répandus (plusieurs millions). La technologie est surtout utilisée à très grande échelle pour la gestion de la chaîne logistique : Wal-Mart, la plus grande chaîne de grande distribution, requiert depuis 2005 de ses 100 plus gros fournisseurs la présence de marqueurs RFID sur les cartons et, depuis janvier 2006, le demande à ses 300 plus gros fournisseurs. Wal-Mart fait partie de EPCGlobal, une alliance d'industriels qui vise à promouvoir l'utilisation de RFID et EPC pour la gestion de la chaîne logistique. EPC est un système d'identification des produits reposant sur RFID, similaire au code barres, mais qui contient (en sus des codes du fabricant et de la classe du produit) un code permettant d'identifier les produits d'une même série. Le *Departement of Defense* (DoD) exige de ses 43 000 fournisseurs, depuis le printemps dernier, le marquage RFID des marchandises destinées à deux de ses centres de dépôt. Le code

Pour en savoir plus :

La norme ISO/IEC 18000:2004
http://www.iso.org/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=ISO%2FIEC+18000

La norme ISO/IEC TR 24710:2005
http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=38820&ICS1=35&ICS2=40&ICS3

EPC Global
http://www.epcglobalinc.org

Programme NAIS
http://animalid.aphis.usda.gov/nais

http://www.rfidjournal.com
http://www.rfidgazette.org
http://www.rfidnews.org
http://www.gcn.com

http://www.acq.osd.mil/log/rfid/DoD_Suppliers'_Passive_RFID_Information_Guide_v8.0.pdf

Expérimentation du DoD :
http://www.govworks.gov/vendor/RFP_docs/60916_A6_BPA.doc
http://www.securitymanagement.com/library/gao05345_rfidreport1205.pdf

Contrôle d'accès au Fort McPherson :
http://rfid.idtechex.com/knowledgebase/en/casestudy.asp?freefromsection=121

d'identification des tags peut-être EPC ou un code spécifique au DoD. Les tags sont à ultra haute fréquence (autour de 900 MHz). Le DoD expérimente par ailleurs certains systèmes RFID très complets pour la localisation du matériel : des marqueurs actifs permettant une communication à plusieurs centaines de mètres, des systèmes munis de GPS, d'autres combinant RFID à un système de communication par satellite (SACOM Iridium). Des systèmes RFID sont également utilisés pour le contrôle d'accès à certaines installations militaires (par exemple le Fort McPherson, siège de l'état major de l'armée de terre). Au-delà, certaines bibliothèques l'utilisent aussi pour la gestion des emprunts et retours ; dans certains aéroports la technologie est employée pour le suivi des bagages et des passages aux inspections de sécurité. Elle est par ailleurs assez bien utilisée pour les badges d'authentification. L'agence hospitalière du ministère des anciens combattants (dont le réseau hospitalier dessert 5 millions de personnes) a commencé en 2005 à mettre en usage le RFID pour le suivi des médicaments.

3. Quelques exemples d'applications en développement ou à venir

Le séminaire de la FDA :
http://www.fda.gov/bbs/topics/NEWS/2006/NEW01293.html

Applications médicales
http://medicalconnectivity.com/categories/rfid/

La FDA (*Food and Drug Administration*) recommande d'équiper les palettes de médicaments de systèmes RFID dans le but de lutter contre la contrefaçon, un séminaire consacré à cette question aura lieu les 8 et 9 février 2006. Des études sont en cours pour connaître l'effet du champ créé par l'utilisation de RFID sur certains médicaments. Certains hôpitaux testent des systèmes s'appuyant sur RFID : principalement pour le suivi du matériel (et éviter les vols), du personnel, des patients, visiteurs (localiser et vérifier les accès), parfois pour l'identification des médicaments et des patients, voire pour des capteurs sur les patients. VeriChip a développé une puce RFID destinée à être implantée sous le tissu adipeux, la seule à avoir reçu l'agrément de la FDA. Elle peut-être utilisée pour l'identification des patients dans les hôpitaux (une soixantaine d'établissements utilisent cette technologie), mais aussi pour authentifier les accès etc.. Le *Department of Homeland Security* teste des formulaires d'entrée et de sortie du territoire I-94 (formulaires pour les ressortissants dispensés de visa) équipés de marqueurs RFID depuis l'été 2005 et pour un an environ. Ces marqueurs passifs, interrogeables sans authentification contiendront uniquement un identifiant, qui sera lié aux informations personnelles contenues dans une base de données. Le DHS a par ailleurs équipé une centaine de postes frontière terrestres (avec le Mexique et le Canada) de voies RFID (programme FAST) où peuvent passer des chargement qui ont été pré contrôlés au départ. American Express et Mastercard ont lancé des cartes de paiement dotées d'une puce RFID. De tels systèmes peuvent être intégrés dans les téléphones (système dit NFC pour *Near Field Communication*) ; Motorola a annoncé de tels produits.

4. Les passeports RFID

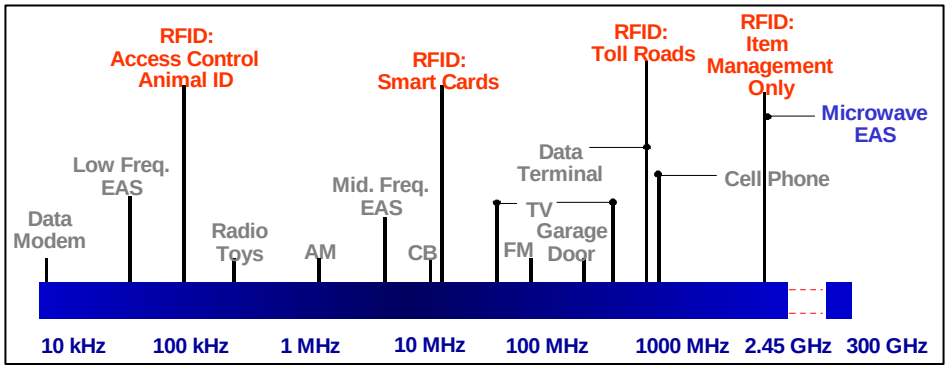
I-94 et RFID
http://www.dhs.gov/dhspublic/display?content=4720

Le gouvernement américain a exigé des pays dont les ressortissants peuvent entrer aux Etats-Unis sans visa qu'ils mettent en place des passeports numériques équipés de données biométriques avant octobre 2005. Le « *Enhanced Border Security and Visa Entry Reform Act* » de 2002 requérait la mise en place d'équipement aux points d'entrées aux Etats-Unis, mais ces équipements ne sont toujours pas prêts (problèmes de compatibilité). Le gouvernement souhaite équiper les passeports américains d'un système RFID d'ici à octobre 2006, mais rien n'est encore finalisé : les choix techniques ne sont pas encore arrêtés et des conflits légaux consécutifs au choix des fournisseurs sélectionnés pour tests après appel d'offre auront retardé le processus. Pour éviter que ces passeports RFID ne soient interrogeables en permanence, ils seraient recouverts d'une sorte de cage de Faraday et, surtout, comporteraient un système d'autorisation utilisant une cryptographie asymétrique pour l'interrogation des données (mais selon certains experts la sécurité serait compromise par une clef qui resterait inchangée sur la durée de vie d'un passeport).

5. Réglementation

Aux Etats-Unis, c'est l'*Office of Engineering and Technology* (OET) de la *Federal Communications Commission* qui est responsable de la mise à jour des règlements pour tout ce qui concerne l'emploi privé des fréquences (la *National Telecommunications and Information Administration* étant en charge des emplois par l'administration fédérale). Les systèmes RFID sont régulés selon la section 15 des règles de la FCC : en contrepartie du libre accès aux fréquences considérées, les équipements doivent répondre à des critères stricts édictés par l'OET, notamment sur la puissance d'émission, le champ électromagnétique créé et la stabilité qui implique des contraintes en terme de portée. Les appareils les plus courants utilisent les basses fréquences (autour de 125 ou 134,2 kHz), les hautes fréquences (autour de 13,56 Mhz : utilisée à l'échelle mondiale), les ultra hautes fréquences (autour de 463 Mhz et entre 868 et 956 Mhz) ou les micro ondes (autour de 2,45 Ghz ou 5,8 Ghz). La portée varie selon les équipements utilisés de l'ordre du centimètre à plusieurs centaines de mètres.

La section 15 des règles de la FCC http://www.fcc.gov/oet/info/rules/part15/part15-91905.pdf



Un problème d'uniformité des réglementations des fréquences au niveau mondial

Les industriels souhaitent un produit qui puisse être autorisé mondialement pour l'application gestion de la chaîne logistique, alors que les fréquences autorisées varient suivant les pays. La FCC a autorisé ODIN (l'un des leaders en intégration de systèmes RFID aux Etats-Unis) à utiliser dans ses laboratoires les fréquences autorisées en Europe ou au Japon (mais pas aux Etats-Unis), pour favoriser la présence américaine sur ces marchés, mais aussi le développement de produits pouvant fonctionner mondialement, nécessaires pour la gestion logistique.

6. Problèmes posés par les composants RFID

Respect de la vie privée

La FTC (*Federal Trade Commission*) a organisé en mars 2005 une table ronde. Ce fut l'occasion d'observer la diversité des avis sur la question. Certains industriels avaient déjà établi des règles de bonne conduite pour la protection de la vie privée des consommateurs (par exemple les « *EPCGuidelines* »). Ainsi les produits portant un marqueur RFID doivent informer le consommateur de cette présence, et le marqueur doit pouvoir être désactivé avant la sortie du magasin. Certains groupes souhaitent une réglementation dans le domaine. Plusieurs projets de lois étatiques et fédérales souhaitent encadrer l'utilisation de RFID afin de limiter son impact sur les problèmes relatifs à la vie privée.

Le rapport de la FTC suite à sa table ronde « *Radio Frequency IDentification: Applications and Implications for Consumers* » http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf

Sécurité

La faible sécurité de certains produits introduits sur le marché peut par ailleurs être sujet d'inquiétude : des chercheurs de John Hopkins University sont parvenus à « pirater » le système *Digital Signature Transponder* (DST) de

Piratage du DST : http://rfidanalysis.org/DSTbreak.pdf

Texas Instruments utilisé entre autre par ExxonMobil SpeedPass et par des clés de voitures (en raison d'une taille de clé cryptographique trop faible : 40 bits). De fait, les classes 0 à 2 définies par la norme EPC (composants passifs) correspondent à une sécurité faible, nonobstant la faible portée associée. Il faut atteindre les classes 3 (semi passif) et 4 (actif) pour que le niveau de sécurité soit satisfaisant. Le *Government Accountability Office* (GAO) est sensibilisé à ces risques et a publié en mai 2005 un rapport sur le sujet, dans lequel il met en évidence le fait que les administrations qui se sont engagées dans l'emploi de RFID n'ont pas pris sérieusement en compte, à une exception près, les risques en matière de sécurité et en matière de protection de la vie privée, et pointe l'insuffisance des contre-mesures envisagées. Dans le même ordre d'idée, le « think tank » RAND a enquêté auprès de six grandes entreprises qui utilisent des puces RFID dans leurs locaux (contrôle d'accès et au-delà). Une seule avait formulé par écrit les règles d'emploi et de déploiement, mais à l'attention du service de sécurité. Les employés se trouvaient donc dans l'ignorance des implications et limites de l'emploi de cette technologie.

Le rapport du GAO : "*Information security - Radio Frequency Identification Technology in the Federal Government*" http://www.gao.gov/new.items/d05551.pdf

Enquête de la RAND http://www.rand.org/pubs/research_briefs/RB9107/index1.html

Fiabilité

Avant un emploi massif et efficace il faudrait trouver une solution aux problèmes techniques mis en évidence lors des expériences. Les taux de reconnaissance diminuent fortement lors de la présence de nombreux marqueurs (problèmes d'interférences et d'alimentation par champ électromagnétique insuffisante dans le cas de marqueurs passifs) ; les ondes sont fortement atténuées par le métal et l'eau. Il est parfois nécessaire d'adapter l'emballage des produits pour le rendre compatible avec une utilisation RFID ...

7. Recherche & Développement

Dans l'ensemble la plus grande part des travaux consacrés au RFID ou tirant partie du RFID relève actuellement de la recherche applicative, ce qui n'est pas très surprenant. Cela va jusqu'à des travaux dont le propos est de réduire le coût de fabrication des composants RFID tout en augmentant leur capacité. Une autre caractéristique importante est que les travaux relatifs au RFID sont souvent des travaux portant sur des réseaux de composants sans fil (pas tous RFID), avec intégration dans le Web. En effet, dès que l'on sort du cadre 'un code objet lu par un lecteur, puis lecture d'un autre code objet', un système rassemblant des composants RFID doit être vu comme un réseau sans fil, en règle générale intégré dans le réseau Internet. À cet égard, la recherche sur les RFID a de nombreux liens avec celle sur les réseaux sans fil ou avec celle sur le « *pervasive computing* ». Par ailleurs, pour des composants actifs dont la capacité va nettement au-delà du code barre, la recherche de base est très étroitement liée à celle portant sur les systèmes embarqués (modèles logiques, travail sur l'autonomie etc.).

Recherches centrées sur le RFID

On peut relever que, si certaines universités ont créé des centres de longue date, à commencer par le MIT, il y a une floraison de nouveaux centres consacrés au RFID. Tous ces centres viennent s'ajouter à une infrastructure de recherche qui, notamment du côté industriel, est déjà significative : centres de Sun Microsystems, Texas Instrument (dont l'unité *Sensors & Actuators*, mais sans la partie RFID, vient d'être vendue à LLC), Intel, Seattle et Berkeley, Wal-Mart, IBM (pour le middleware), Microsoft (qui a même créé un *RFID Council*), etc. Du point de vue industriel Dallas (notamment TI et Sun, tandis que pour IBM c'est Zürich) apparaît comme étant le centre principal pour ce qui est du RFID au sens strict, ce à quoi l'on peut ajouter le MIT Auto-ID Lab et ses partenaires industriels.

Centres consacrés au RFID créés en 2005 :

- Le *Radio Frequency Identification Center of Excellence* (http://www.engr.pitt.edu/site/rfid) a ouvert en octobre dernier à l'université de Pittsburgh (chargé aussi de gérer le portefeuille de brevets RFID de l'université, laquelle est un des principaux centres du domaine avec le MIT).

- Le *RFID Lab* de l'Université du Wisconsin à Madison, adossé sur un groupe d'industriels, se positionne aussi comme centre de test pour les nouveaux marqueurs RFID (http://www.uwrfidlab.org).

- Le *RFID Research Group* de l'université du Nord Texas à Denton (http://www.txcdk.org/rfid).

- Le *RFID Research Center*, fortement pluridisciplinaire, (http://itrc.uark.edu/view.asp?article=242) vient d'ouvrir au sein de l'université d'Arkansas (le financement associe notamment Tyson Foods et Wal-Mart, ainsi que des dons matériels de grands industriels, dont Intel, Cisco-Eagle et Microsoft).

- Le tout nouveau *Center for food distribution and retailing* de l'université de Floride (http://cfdr.ifas.ufl.edu), pour lequel le RFID est un axe majeur (là encore clairement très applicatif).

Les principaux thèmes de recherche qui apparaissent sont :

- les logiciels embarqués des composants, à considérer comme une partie de la recherche sur les systèmes embarqués.
- l'amélioration du hardware : amélioration de la portée et de la directivité des antennes, maîtrise des interférences, de l'autonomie (alimentation solaire, reposant sur les vibrations, les flux d'air, voire les gradients de température / pression), miniaturisation (un nouveau domaine est le recours à des nano-composants) …
- la prise en compte des interférences entre puces RFID (« tag anti-collision ») ou entre lecteurs RFID (« reader anti-collision »), question rendue accrue par le déploiement d'applications qui comportent un grand nombre de composants ou par la proximité d'un grand nombre de lecteurs, à portées croissantes, avec des sensibilités différentes au bruit, etc.
- la conception et l'architecture des composants RFID, voire des systèmes (réseau de composants + middleware + applications), ce qui commence par l'intégration dans le monde du RFID des techniques (outils de conception etc.) qui se sont développées dans le domaine des puces et des systèmes embarqués, mais également la prise en compte de nouveaux matériaux (silicium sur isolant, silicium pressé) utilisés pour les microprocesseurs.
- les problématiques liées aux réseaux de systèmes RFID (gestion d'ensemble par des outils Web adaptés etc.) et au trafic que représentent les données d'un très grand nombre de capteurs (routage, évitement des collisions, gestion adaptative du trafic etc.). Cela va jusqu'à des réflexion sur un réseau global rassemblant toutes sortes d'objets équipés : '*Internet of things*' et autres IrisNet.
- le middleware pour les RFID, en particulier l'intégration des données envoyées par de grands nombres de capteurs RFID, les services Web pour piloter des applications RFID…
- la sécurité des informations (concernant la vie privée etc.) dans les systèmes RFID.
- les recherches portant sur l'application du RFID, dans le domaine de la santé (suivi de patients, aide aux handicapés), celui de l'environnement (réseaux de suivi de zones naturelles), celui du bâtiment (domotique, suivi de structures), l'automobile (suivi des composants et contrôle) etc.

Les centres qui apparaissent comme les plus actifs, outre ceux listés ci-dessus, semblent être :

- le MIT via le MIT Auto-ID Lab et son rôle dans les Auto-ID Labs et dans EPC Global.
- Intel et ses partenaires universitaires.
- un ensemble d'universités réparties à travers le pays : UCLA (CENS et WINMAC), UCB, Harvard (projet CodeBlue pour le suivi médical de patients), Carnegie Mellon, Université de Columbia (centre WICAT, système MoteTrack), Ohio University, Virginia University, Urbana Champaign (essentiellement pour la thématique réseau), Université de Washington, GeorgiaTech (aide aux aveugles).

http://www.intel.com/research

Le projet CodeBlue
http://www.eecs.harvard.edu/~mdw/proj/codeblue

Le système MoteTrack
http://www.eecs.harvard.edu/~konrad/projects/motetrack

Les financeurs sont, outre les industriels (probablement en premier lieu), la NSF, la DARPA, les NIH et de puissantes fondations liées au monde de la santé (association Alzheimer ou AAHSA par exemple) pour les applications correspondantes du RFID.

Un rapport d'ambassade plus détaillé paraîtra très prochainement. (MS&T)

Industrie

Développement des réseaux d'accès par courants porteurs en ligne

Auteur de l'article
michel.combot@missioneco.org

Pour en savoir plus :

Current Communications :
http://www.currentgroup.com

TXU Electric Delivery :
http://www.txuelectricdelivery.com

Cinergy :
http://www.cinergy.com

HomePlug Powerline Alliance :
http://www.homeplug.org

ComTek :
http://www.comtekbroadband.com

Revue TIC n°85 :
« La FCC définit le cadre réglementaire de la technologie des courants porteurs"
http://www.bulletins-electroniques.com/actualites/23879.htm

Current Communications, société spécialisée dans la technologie des courants porteurs en ligne pour l'accès Internet et basée dans le Maryland, a annoncé au mois de décembre 2005 le déploiement d'un réseau de transmission par courants porteurs en ligne sur le réseau électrique de TXU Electric Delivery, une société de transmission et de distribution d'électricité au Texas. Ce réseau servira, d'une part, aux besoins propres de TXU (lecture automatique de compteurs, service de « grille intelligente ») et, d'autre part, à la mise en place d'un service d'accès Internet et de services sur IP (voix, vidéo) pour près de 2 millions de foyers qui seront couverts par ce réseau. Current Communications dispose déjà d'un réseau similaire dans l'Ohio, qui couvre 50 000 habitations, en partenariat avec Cinergy, et que la société souhaite étendre à près de 250 000 foyers d'ici à la fin de l'année 2006. Le réseau déployé au Texas devrait entrer en concurrence directe avec les réseaux en fibre optique jusque chez l'habitant (FTTH) déployés par AT&T (ex-SBC) et Verizon dans la région. Pour la partie « usage interne », TXU paiera près de 150 millions de dollars sur 10 ans pour l'utilisation du réseau déployé par Current Communications. Pour la partie « accès Internet », le Chairman de la société, William Berkman, annonce des vitesses d'accès de 10 Mb/s, pour des débits symétriques. Si la politique tarifaire n'a pas été dévoilée, Current Communications commercialise plusieurs forfaits dans l'Ohio sur la base de débits symétriques – 30 dollars par mois pour 1 Mb/s, 35 dollars pour 2 Mb/s et 40 dollars pour 3 Mb/s – pour un taux d'adoption estimé par les analystes à 15% (7500 abonnés). Par ailleurs, la société devrait profiter des dernières spécifications de la *HomePlug Powerline Alliance*, permettant une compatibilité entre réseaux de courants porteurs en ligne « *indoor* » et « *outdoor* ». Enfin, Current Communications déploiera des services de voix sur IP dans l'Ohio d'ici à la fin du premier semestre 2006. TXU Electric Delivrery va investir dans Current Communications, qui dispose déjà de nombreux investisseurs : Goldman Sachs, Google et Hearst Corporation entre autres. Le déploiement réalisé au Texas représentera le plus gros déploiement commercial de la technologie des courants porteurs en ligne aux Etats-Unis. Outre les réseaux de Current Communications, la ville de Manassas en Virginie a déployé un réseau, en partenariat avec la société ComTek, auprès de ses 12500 foyers et 2500 habitations. A ce jour, 850 abonnés ont souscrit aux services d'accès commercialisés par ComTek. (ME)

Le développement des solutions bureautiques *web-based*

Auteur de l'article
magali.voisin-ratelle@missioneco.org

L'analyse complète des solutions bureautiques *web-based* dans la revue «Convergences Numériques et Audiovisuel» éditée par la Mission Economique de San Francisco :
http://www.missioneco.org/etatsunis/documents_new.asp?V=7_PDF_114560

Le secteur des suites bureautiques *web-based* a évolué rapidement depuis quelques mois. Le développement des applications web en Ajax et la tendance « web 2.0 » actuelle ont conduit à l'apparition de plusieurs nouveaux acteurs sur le segment naissant des « suites » logicielles. En effet, la domination de Microsoft Office sur ce marché était réputée comme inattaquable malgré les incursions des logiciels *open source* tels que OpenOffice 2.0, la suite bureautique de Sun Microsystems. La majorité des ces nouvelles solutions fonctionne sur le principe d'une offre gratuite offrant peu de fonctionnalités et peu d'espace disque pour stocker les documents, avec un modèle de revenus qui repose sur la publicité contextuelle. Des offres *premiums* offrant plus de fonctionnalités, plus d'espaces et plus d'utilisateurs, sont disponibles sur une base payante. Il existe ainsi un certain nombre de suites bureautiques plus ou moins avancées, des outils de gestion courante (calendrier et bloc notes) ainsi

que d'autres outils performants en cours de développement, à l'image des services fournis par ThinkFree, AjaxOffice, gOffice, Bindows, Writely ou encore Airset. (ME)

Internet

Rapport de la FTC sur l'efficacité de la lutte antispam

Auteur de l'article
sebastien.morbieu@ambafrance-us.org

Pour en savoir plus :

http://news.com.com/FTC+says+federal+spam+law+has+worked/2100-1028_3-6003071.html

http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf

CAN SPAM *Act* :
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf

Projet US SAFE WEB *Act* :
http://www.ftc.gov/reports/ussafeweb/Proposed%20US%20SAFE%20WEB%20Act.pdf

Revue TIC n°99 :
« Yahoo et Cisco font converger leurs technologies d'authentification des e-mails »
http://www.bulletins-electroniques.com/actualites/028/28486.htm

Réponse nationale à un problème global, le Congrès avait voté en 2003 le CAN-SPAM (« *Controlling the Assault of Non-Solicited Pornography and Marketing* ») *Act* pour lutter contre le spam. Un rapport de la FTC (« *Federal Trade Commission* ») au Congrès évalue l'efficacité des mesures retenues, et établit des recommandations pour une amélioration de la lutte contre le spam. Le rapport note une diminution du nombre de spams mais concède qu'il n'est pas possible de mesurer l'impact qu'a eu le CAN-SPAM sur cette diminution. Le CAN-SPAM *Act* a créé un cadre législatif pour les emails publicitaires : ceux ci doivent inclure un lien pour ne plus les recevoir ; les publicitaires respectent globalement bien ce cadre. Néanmoins, les spams deviennent de plus en plus malveillants – diffusion de malware et phishing – mais la FTC considère que les lois existantes sont suffisantes. Le rapport confirme l'avis du Congrès lors de l'adoption du CAN-SPAM *Act* : le problème du spam ne sera pas résolu de façon uniquement législative, il nécessite une réponse technologique et une coopération internationale. Des mesures ont été prises par certains fournisseurs d'accès pour lutter contre les ordinateurs compromis, qui relaient 60 à 80% du spam. Ces fournisseurs exigent que les emails soient envoyés par leurs serveurs et instaurent des limites dans le nombre d'envoi. 80% des emails sont bloqués avant l'entrée sur les réseaux de certains fournisseurs d'accès car déjà identifiés comme spam, les 20% restant sont ensuite soumis à des filtres antispam, jugés efficaces par la FTC. La Commission a par ailleurs incité au déploiement de systèmes d'authentification par domaine, qui se répandent actuellement (voir Revue TIC n°99). La FTC, qui ne dispose pas de réelles statistiques sur l'origine du spam par pays, note des difficultés dans la coopération internationale pour la lutte contre le spam : il est par exemple impossible de mener des investigations lorsqu'un nom de domaine est enregistré à l'étranger. La FTC s'est impliquée dans des réseaux informels de coopération dans la lutte contre le spam : *London Action Plan on International Spam Enforcement Cooperation*, participation à l'*International Consumer Protection and Enforcement Network* et signature de *Memoranda of Understanding* avec les agences de lutte contre le spam en Angleterre et en Australie d'une part, et en Espagne d'autre part ; elle défend ses positions auprès de la *Spam Task Force* de l'OCDE, du forum de Coopération Economique Asie Pacifique et du Sommet Mondial sur la Société de l'Information et a participé avec 30 agences dans le monde à l'« *Operation Spam Zombies* », dans la continuité de l'« *Operation Secure Your Server* » de 2004. Pour pouvoir lutter de façon internationale contre le spam, la FTC recommande l'adoption de l'US SAFE WEB *Act*, qui lui permettrait d'une part d'échanger des informations avec des services étrangers, et d'autre part de ne pas rendre publiques les informations lors d'investigations. Elle souhaite mettre en place une coopération pour l'application des lois, encourager les partenaires étrangers à inciter les industriels à mettre en place des outils technologiques de lutte contre le spam et fournir une assistance technique dans la lutte contre le spam aux pays qui en ont besoin. En ce qui concerne la pornographie, la FTC ne dispose pas de statistiques pouvant évaluer le respect de l'ALR (*Adult Labeling Rule*), qui fixe des règles pour la signalisation d'emails pornographiques, mais observe que le spam pornographique est en déclin. Le Michigan et l'Utah ont mis en place des listes d'emails de mineurs et interdisent l'envoi de messages pornographiques à ces listes. L'existence de ces listes peut, selon la FTC, présenter un danger grave et elle met en garde contre des lois qui seraient adoptées au niveau étatique. Ses recommandations sont l'application de l'ALR, l'adoption du US SAFE WEB *Act* et une sensibilisation aux technologies qui filtrent les messages à contenu pornographique. (MS&T)

Régulation

La question de la neutralité pour l'Internet

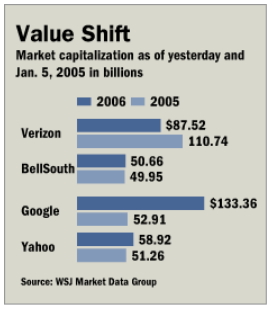
Auteur de l'article
michel.combot@missioneco.org

Pour en savoir plus :

Revue TIC n°103 :
Voir Archives.

> Les 4 principes d'action de la FCC sur le marché du haut débit :
> Les consommateurs doivent pouvoir (1) avoir accès au contenu légal de leur choix ; (2) avoir accès aux services et applications légaux de leur choix ; (3) connecter les terminaux de leur choix ; (4) profiter de la concurrence entre fournisseurs d'accès, de services et d'applications.

"*Some [consumers] want a lower speed, and for other consumers, it may be worth more to them to pay for a better quality of service or better speed.*"
Kevin Martin, Président de la FCC



"We talk to them [Google] all the time, and they understand the issue."
Ivan Seidenberg, *Chairman & CEO*, Verizon

En août 2005, la *Federal Communications Commission* (FCC) dérégulait les services d'accès haut débit (voir Revue TIC n°103). Néanmoins, l'Agence précisait à l'époque les principes de son action sur ce marché, pouvant aboutir éventuellement à des décisions réglementaires *ex-post* (voir ci-contre). Ainsi, la Commission s'attachait au principe de neutralité pour l'Internet, le consommateur devant pouvoir accéder à toutes les applications et services qu'il souhaite, notamment les services de voix ou de vidéo sur IP de fournisseurs indépendants. Depuis, le débat sur cette question de neutralité occupe de plus en plus le devant de la scène. A l'occasion du *Consumer Electronics Show* (CES) qui s'est tenu du 5 au 8 janvier 2006 à Las Vegas, Kevin Martin, Président de la FCC, a expliqué que l'Agence ne disposait pas de l'autorité nécessaire pour faire respecter ce principe de neutralité. Même si la FCC s'opposerait, dans la limite de ses pouvoirs, au blocage de contenu spécifique, Kevin Martin considère normal la mise en place d'offres d'accès différenciées en fonction du débit et de classe de service, nécessaires par exemple pour la bonne utilisation de services de téléchargement de contenu « concurrents » de ceux développés par les fournisseurs d'accès Internet. Alors que de nombreux services de téléchargement de contenu audiovisuel se mettent en place, notamment par Google, AOL ou Microsoft, ces derniers souhaitent que le Congrès intervienne et définisse de manière claire et précise un cadre pour cette neutralité. Si la menace d'un blocage pur et simple reste relativement hypothétique, celle d'une différenciation entre services du fournisseur d'accès et service de fournisseurs tiers apparaît plus probable, sachant que les principaux fournisseurs d'accès Internet haut débit aux Etats-Unis, opérateurs de télécommunications et câblo-opérateurs, ont investi énormément pour déployer des services avancés (*Video-On-Demand*, DVR, IPTV), fortement rémunérateurs. S'exprimant aussi à l'occasion du CES, le *Chairman* & CEO de Verizon, Ivan Seidenberg, a ainsi déclaré que les fournisseurs tiers de contenu (Google et Microsoft par exemple) devraient participer à l'effort de financement lié au déploiement des réseaux à très haut débit, pour permettre à leurs abonnés de disposer d'une bande passante suffisante à la bonne exploitation des services – sans quoi la mise en place de forfaits différenciés apparaît inéluctable. Néanmoins, les fournisseurs d'accès ont tout intérêt à s'entendre avec les fournisseurs de contenus, une bataille commerciale n'ayant pas de sens alors que les complémentarités semblent évidentes (Verizon et SBC collaborent ainsi déjà de manière étendue avec Yahoo). Par ailleurs, le rapport de force n'est pas forcément en faveur des opérateurs de télécommunications ou des câblo-opérateurs. Si les capitalisations boursières de Google et Yahoo par exemple, ont progressé en 2005, celle de Verizon a fortement diminué. Verizon a ainsi indiqué ainsi être en discussion avec Google pour que ce dernier rétribue l'opérateur en contrepartie d'une garantie sur les débits à destination de ses clients. De même BellSouth vient d'entamer des négociations avec MovieLink, pour son service de téléchargement de vidéo et films par Internet. (ME)

Législation

Nouveau projet de loi au Congrès pour le secteur des communications électroniques

Auteur de l'article
michel.combot@missioneco.org

Pour en savoir plus :

Le texte du projet de loi :
http://thomas.loc.gov
(Taper le numéro de loi : S2113)

Un troisième projet de loi en matière de communications électroniques a été introduit au Congrès en décembre 2005 par le Sénateur DeMint (R-Caroline du Sud). Après le projet du Sénateur Ensign (R-Nevada) et le texte du Représentant Barton (R-Texas), le « *Digital Age Communications Act* » (S2113) vise à réformer lui aussi la loi des télécommunications de 1996 dans le cadre de la croissance rapide des services sur IP (voix, vidéo, …). Le texte prévoit la disparition quasi-totale des régulations locales et étatiques en matière de communications électroniques au profit d'un cadre fédéral

harmonisé, indépendant du type de service déployé. Les systèmes de concessions locales pour les services de télévision (franchise) seraient ainsi supprimés. Les Etats fédérés seraient chargés de faire respecter les dispositions fédérales mais aussi de gérer, pour le compte de l'Etat fédéral, le fonds de service universel, qui serait plafonné à 3,65 milliards de dollars par an. Enfin, l'ensemble des opérateurs et fournisseurs aurait accès de manière non discriminatoire aux droits de passage, tant privés que publics. (ME)

Éditeur : Ambassade de France aux Etats-Unis
4101 Reservoir Road NW – Washington, DC 20007-2173 – USA

Rédacteurs en chef :
Michel Combot - *Réseau des Missions Economiques*
Jean-Philippe Lagrange - *Mission pour la Science et la Technologie*

Rédacteurs :
Réseau des Missions Economiques (ME)
Michel Combot – Tél.: +1 415 781 09 86 – Fax : +1 415 781 47 50
Email : michel.combot@missioneco.org
Magali Voisin-Ratelle – Tél.: +1 415 781 09 86 – Fax : +1 415 781 47 50
Email : magali.voisin-ratelle@missioneco.org
Mission pour la Science et la Technologie (MS&T)
Jean-Philippe Lagrange – Tél: +1 202 944 6237 – Fax: +1 202 944 6244
Email : jean-philippe.lagrange@ambafrance-us.org
Christophe Lerouge – Tél. : +1 415 397 4440 – Fax : +1 415 397 9947
Email : christophe.lerouge@consulfrance-sanfrancisco.org
Sébastien Morbieu – Tél. : +1 202 944 6582– Fax : +1 202 944 6244
Email : sebastien.morbieu@ambafrance-us.org

Date de parution : 13 janvier 2006