ANNALES 2015

CONCOURS INTERNE

POUR LE RECRUTEMENT

DE CADRE SPECIALISTE TECHIQUE

DU CADRE DES POSTES ET TELECOMMUNICATIONS DE NOUVELLE-CALEDONIE

CONCOURS INTERNE OUVERT LES 20 ET 21 AOUT 2015 POUR LE RECRUTEMENT D'UN CADRE SPECIALISTE TECHNIQUE DU CADRE DES POSTES ET TELECOMMUNICATIONS DE LA NOUVELLE-CALEDONIE

EPREUVE ECRITE D'ADMISSIBILITE : VALORISATION DE L'EXPERIENCE PROFESSIONNELLE

DUREE : 4 HEURES — COEF : 4

SUJET

Ce dossier comporte 27 pages y compris la page de garde.

Cadre spécialiste technique, vous êtes nouvellement recruté en qualité de directeur des systèmes d'informations au sein de l'office des postes et télécommunications.

Axe majeur des missions d'aménagement de l'établissement, ce dernier s'est engagé dans une stratégie numérique visant à répondre aux enjeux de développement du territoire.

Face à ces enjeux, la direction générale souhaite adapter sa politique de sécurisation des données.

A l'aide du dossier joint et de vos connaissances, il vous est demandé d'élaborer une note assortie de propositions afin de proposer des axes d'intervention afin de renforcer la politique de sécurisation des données.

Cette note sera également utilisée comme base de travail dans le cadre des échanges avec les élus non-experts sur le volet technique.

BAREME DE NOTATION

Ce rapport doit permettre de dégager des éléments de mise en œuvre de solutions opérationnelles appropriées.

Vous rédigerez ce rapport à l'aide des documents du dossier et en mobilisant vos connaissances.

Les candidats devront organiser leurs idées et leur argumentation en dégageant un plan.

Liste des documents :

Document n° 1- Etude d'impacts sur la vie privée : suivez la méthode de la CNIL - www.cnil.fr - 02 juillet 2015

Document n° 2 : Sécurité numérique et risques: enjeux et chances pour les entreprises - COMPTE RENDU DE L'AUDITION PUBLIQUE DU 19 JUIN 2014 : SÉCURITÉ DES RÉSEAUX NUMÉRIQUES -- www.sénat.fr.

Document n° 3 : L'ENA sur le chemin escarpé de la formation à l'open data- www.lagazettedescommunes.com- 21/05/2015 -Sabine Blanc

Document n ° 4 : 10 conseils pour la sécurité de votre système d'information – www.cnil.fr - 12 octobre 2009

Document n° 5 : Protection de l'information - Enjeux, gouvernance et bonnes pratiques - http://www.cigref.fr/cigref_publications - 2008

Document n ° 6 : La sécurisation des données est un enjeu- http://www.toolinux.com - 13/03/2015

Document n° 7 : Cadre stratégique commun du Système d'Information de l'Etat Synthèse- Février 2013

Document n° 1- Etude d'impacts sur la vie privée : suivez la méthode de la CNIL – www.cnil.fr - 02 juillet 2015

La CNIL publie sa méthode pour mener des PIA (Privacy Impact Assessment) pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits.

De l'application de bonnes pratiques de sécurité à une véritable mise en conformité

La Loi informatique et libertés (article 34), impose aux responsables de traitement de « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données* ».

Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.

Pour aider les TPE et PME dans cette étude, la CNIL a publié en 2010 un premier guide sécurité. Celui-ci présente sous forme de fiches thématiques les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement des données personnelles.

En juin 2012, la CNIL publiait un autre guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

Une méthode plus rapide, plus facile à appliquer et plus outillée

Ce guide a été révisé afin d'être plus en phase avec le projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.

La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL..

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :

1. les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quelles que soient la nature, la gravité et la vraisemblance des risques encourus ;
2. la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.

Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :

1. étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
2. étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
3. étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;

4. validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.

L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

Document n° 2 : Sécurité numérique et risques: enjeux et chances pour les entreprises - COMPTE RENDU DE L'AUDITION PUBLIQUE DU 19 JUIN 2014 : SÉCURITÉ DES RÉSEAUX NUMÉRIQUES – www.sénat.fr.

SOMMAIRE

M. Philippe Wolf, ingénieur général de l'armement, auteur de nombreux articles et ouvrages sur le numérique

Me Éric Caprioli, docteur en droit, avocat à la Cour d'appel de Paris, vice-président du Club des experts de la sécurité de l'information et du numérique (CESIN)

Me Pierre Desmarais, avocat à la Cour d'appel de Paris, correspondant informatique et libertés, spécialisé dans les questions de sécurité numérique

Mme Valérie Maldonado, chef de service, Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)

M. Benoît Virole, docteur en psychopathologie, docteur en sciences du langage, membre de l'Observatoire des mondes numériques en sciences humaines (OMNSH)

DÉBAT

CONCLUSIONS

Mme Anne-Yvonne Le Dain, députée, vice-présidente

M. Bruno Sido, sénateur, président

LES ASPECTS NORMATIFS DU RISQUE NUMÉRIQUE (SÉCURITÉ DES RÉSEAUX NUMÉRIQUES)

Introduction

Mme Anne-Yvonne Le Dain, députée, vice-présidente de l'OPECST. – L'Office parlementaire d'évaluation des choix scientifiques et technologiques a été créé en 1983. C'est le seul organe qui soit commun au Sénat et à l'Assemblée nationale. Composé de dix-huit députés et de dix-huit sénateurs, il élabore des rapports sur des thèmes scientifiques et technologiques particulièrement complexes afin de les vulgariser, pour que tous les parlementaires puissent, en peu de temps, être à même de réagir lorsque des projets de loi sont présentés dans ces domaines. C'est en tout cas son acception initiale.

Depuis, la question scientifique et technologique est entrée dans les inquiétudes du monde moderne et beaucoup de commissions, au Sénat ou à l'Assemblée nationale, se saisissent de sujets qui ont une connotation ou une force scientifique.

Ce n'est pas toujours simple. C'est aussi la raison pour laquelle l'Office parlementaire considère qu'il est de son devoir d'être sur tous les champs et de sortir très largement du domaine dans lequel il semblait peut-être s'être spécialisé, à savoir le nucléaire. En trente ans, l'Office a abordé beaucoup de domaines.

Dès l'an dernier, l'Office a organisé une journée sur le risque numérique que nous approfondissons actuellement par un travail de fond conduit par deux parlementaires, le sénateur Bruno Sido et moi-même, sur les grandes questions autour du numérique, entre risques et opportunités, entre France et Europe, entre Europe et monde. C'est une question importante.

C'est à la suite d'une saisine de la commission des affaires économiques du Sénat que l'Office conduit cette étude autour du risque encouru par les entreprises qui utiliseraient sans trop de précaution les moyens numériques actuels. La commission pense en particulier au stockage des données dans les nuages *(cloud computing)*, mais aussi aux composants présents dans les cœurs de réseaux.

Pour traiter de ces thèmes extrêmement techniques, les rapporteurs ont choisi de prendre comme exemples les entreprises du secteur des télécommunications et celles du secteur de l'énergie, ces deux secteurs étant considérés comme d'importance vitale.

On sent bien également que ces secteurs touchent à de grandes entreprises et à des ETI, mais aussi à des innovations importantes qui peuvent être portées par de très petites entreprises et des entreprises débutantes. Nous sommes en plein dans le champ de la nouvelle économie du XXI^{e} siècle.

En général, chacune des études de l'OPECST donne lieu à une centaine d'auditions. Dans ce cadre, M. Bruno Sido, en tant que président de l'OPECST, et moi-même, en tant que vice-présidente, avons été désignés. Actuellement, nous avons procédé à plus d'une soixantaine d'auditions incluant des visites sur le terrain. Parmi celles-ci, deux journées d'audition publique ouverte à la presse ont été organisées, l'une portant sur l'éducation au numérique et celle d'aujourd'hui qui porte sur le cadre juridique de cette technique, à laquelle vous avez bien voulu participer. Je vous en remercie.

Une troisième journée d'auditions donnera lieu à un dialogue, d'une part, avec les opérateurs d'importance vitale, et, d'autre part, avec les sociétés de sécurité numérique, ce dont je les remercie vivement.

La présente audition est enregistrée en vidéo et figurera, dès les jours prochains, sur les sites de l'Assemblée nationale et du Sénat. Elle fera également l'objet d'un compte rendu qui sera annexé au rapport final.

Comme il a été indiqué à chacun d'entre vous, les interventions d'horizons fort divers seront toutes axées sur la sécurité des réseaux numériques en ce qu'elle concerne les entreprises mais ce sera, à chaque fois, selon les angles d'attaque qui vous sont propres et qui vous caractérisent, selon vous-même, selon l'organisme auquel vous appartenez ou encore en fonction de vos thèmes de recherche privilégiés, selon votre choix et donc votre liberté.

Quant à moi, compte tenu de la grande qualité des intervenants rassemblés aujourd'hui et de l'actualité brûlante de nos débats et de ce sujet qui est très présent dans l'espace public national et européen, j'ai insisté auprès de Mme Axelle Lemaire, secrétaire d'État chargée du numérique, auprès du ministre de l'économie, du redressement productif et du numérique, M. Arnaud Montebourg, pour qu'elle vienne parmi nous à l'occasion de cette journée. Mme Axelle Lemaire nous rejoindra vers 16 heures.

Je vais donner la parole à Mme Isabelle Falque-Pierrotin. Les missions dévolues à la CNIL, qui fut, dès 1978, l'une des premières institutions, non seulement française, européenne, mais mondiale, à travailler sur ces questions-là, ont considérablement évolué. Il s'agit maintenant de les concilier avec celles dont l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est en charge.

Sécurité des réseaux numériques : cadre juridique, risques, aspects sociétaux

Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL). - À la CNIL, nous avons dressé un constat. Cet univers numérique pose des questions de sécurité extrêmement complexes et un peu nouvelles.

Premièrement, nous sommes face à un écosystème qui fait intervenir de multiples acteurs, avec des relations qui ne sont pas toujours précises entre les prestataires, les acteurs principaux et toute une série d'acteurs qui interviennent derrière. Il y a une forme de **dilution des responsabilités.**

Deuxièmement, dans cet univers où les technologies se renouvellent en permanence, **les questions de sécurité sont sans cesse renouvelées.** Le nuage numérique ou *cloud*, les données massives ou *big data*, les objets connectés ou le *Bring Your Own Device (BYOD)* posent, chacun, une question de sécurité et une manière d'assurer la sécurité qui sont nouvelles.

Troisièmement, **cette culture de l'Internet place l'individu au centre**. C'est à la fois formidable de par les pouvoirs d'actions que cela lui donne, mais en même temps, cela conduit certains d'entre eux à adopter une pratique de contournement. On l'a vu dans des législations qui ne recevaient pas l'approbation de la masse des individus, je pense au téléchargement de musique. Cela peut aussi conduire beaucoup d'individus à se mettre eux-mêmes dans une situation de péril par rapport à leur propre sécurité. Notamment au sein des réseaux sociaux, les individus divulguent beaucoup de données personnelles. Évidemment, cela pose de nouvelles questions de sécurité.

À ces comportements s'ajoute une dimension supplémentaire : l'attractivité des données personnelles. Les données qui sont au coeur de l'économie numérique sont un gisement extrêmement séduisant et attractif pour les entreprises mais aussi pour les gouvernements dans le cadre de la lutte contre le terrorisme ou dans celui de l'espionnage. Cette convoitise vis-à-vis des données renouvelle également les questions de sécurité.

Ces quatre facteurs nous conduisent à rechercher une nouvelle manière de traiter les problèmes de sécurité dans cet univers numérique. Première question : sommes-nous armés pour les traiter ? Je crois que la réponse est oui, à une condition : que nous ayons une réponse qui corresponde à la culture de l'univers auquel nous faisons face. Concrètement, nous devons apporter une réponse de « sécurité en réseau ». En effet, **aucun acteur n'a l'ensemble des clés pour piloter à lui seul la sécurité de cet univers.** En revanche, si l'on s'adresse à l'ensemble des acteurs concernés, et que chacun d'entre eux a une action, une responsabilité particulière en termes de sécurité, alors nous pouvons collectivement garder cet univers sous contrôle, en tout cas au niveau de la sécurité de celui-ci.

Qu'est-ce que signifie avoir une « sécurité en réseau » ? Le premier axe, ce sont les entreprises. Vous l'avez dit, madame Le Dain, c'est le coeur de votre préoccupation d'aujourd'hui. L'objectif est de **responsabiliser ces acteurs** professionnels et ces entreprises, afin qu'ils intègrent dans leur propre fonctionnement cet objectif de garantie de la sécurité des réseaux, et pour nous, à la CNIL, de la sécurité des données personnelles.

Ces acteurs professionnels, nous les connaissons : à travers l'article 34 de notre loi informatique et libertés qui responsabilise en termes de sécurité les responsables de traitement. Ce sont à la fois les opérateurs de réseau et ceux qui offrent des services. Tous ces acteurs professionnels ont la responsabilité des données personnelles qui transitent chez eux ou qu'ils utilisent. Ils doivent en assurer l'intégrité et veiller à ce que l'accès par des tiers auxdites données soit strictement encadré. Dans cet « accès par les tiers », on voit arriver ceux qui convoitent les données à des fins commerciales ou de renseignement.

Cet article 34 est la pierre angulaire de l'enjeu de sécurité au regard de la loi informatique et libertés. Nous l'appliquons de façon uniforme en général mais avec des régimes particuliers liés à certaines catégories de données.

Par exemple, les données de santé font l'objet dans notre législation d'une protection plus forte en termes de sécurité et il existe, notamment, un régime juridique des hébergeurs des données de santé qui doivent être agréés.

On distingue aussi des catégories particulières d'acteurs. Les opérateurs de communications électroniques sont ainsi tenus, depuis 2011, **de notifier les failles de sécurité** (article 34 *bis* de la loi). Cela signifie que celles-ci doivent être signalées dans un délai court à la CNIL, quel que soit le niveau de la faille. Et s'ils ne le font pas, ils encourent des sanctions pénales. Par ailleurs, ces opérateurs ont l'obligation d'informer les personnes de l'existence de cette faille, sauf si celle-ci n'a porté atteinte à aucune donnée personnelle ou qu'ont été prises des mesures pour qu'il n'y ait pas de violation de données personnelles dans le cas où la faille interviendrait. Par exemple, si les données ont été cryptées, il n'y aura pas d'obligation de notification aux personnes même si un tiers y a accès. Les opérateurs ont donc une obligation renforcée en termes de sécurité des données personnelles, par rapport à la responsabilité générale de l'article 34.

Enfin, certaines technologies ou usages font l'objet d'un encadrement spécifique de la CNIL par des recommandations, par exemple, sur le vote électronique ou la carte bancaire sans contact.

Tout cet arsenal est-il efficace ? À ce stade, dans la politique de contrôle que nous menons, et qui ne porte pas spécifiquement sur cette question de la sécurité, je dirais que nous constatons, **dans la plupart des cas, des manquements en termes de sécurité des traitements.** Même si certains de ces manquements peuvent être aisément corrigés ou révèlent surtout un manque de culture « *privacy* », plutôt qu'une volonté de contourner la loi, ce constat est loin d'être positif.

D'autre part, concernant les failles de sécurité, les opérateurs de réseau ont eu beaucoup de réticences à appliquer cette législation, à tel point que nous avons dû les réunir au début de l'année pour leur adresser le message ferme que cette législation s'appliquait, qu'on la leur expliquait, mais que cela faisait désormais partie de leurs obligations.

J'aurais donc tendance à penser que la prise en compte de ces questions de sécurité est progressive mais lente, même si les outils de conformité existent. Je n'ai pas mentionné les outils pédagogiques que nous développons par ailleurs. Nous travaillons ici en étroite collaboration avec l'ANSSI.

De plus, nous rencontrons des difficultés dans la mobilisation de ces outils. Les sanctions que nous pouvons prononcer, notamment les sanctions pécuniaires, obéissent à une procédure contradictoire assez sophistiquée. Pour qu'il y ait sanction pécuniaire, il faut une mise en demeure préalable. Or, dans le cas des failles de sécurité, lorsque nous sommes saisis, la faille est en général déjà fermée. Donc la mise en demeure ne sert pas à grand-chose.

Au cours de l'année **2013**, selon la société *Symantec*, les failles de sécurité ont augmenté de 62 %, dont **plus de dix failles majeures, c'est-à-dire concernant plus de 10 millions de personnes.** Face à des situations de ce type, dans la plupart des cas, nous ne pouvons au maximum que prononcer un avertissement public. Ce n'est pas satisfaisant.

Comment, dès lors, améliorer le dispositif ? D'abord, nous avons fait des propositions qui ont été prises en compte dans la loi du 17 mars 2014 sur la consommation (loi n° 2014-344 du 17 mars 2014, article 105 modifiant l'article 44 de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). Nous avons demandé la possibilité d'opérer des **contrôles en ligne.** Dans le cadre des failles de sécurité, ces contrôles à distance sont extrêmement efficaces.

Ensuite, nous avons fait une proposition à la ministre, Mme Axelle Lemaire, pour que nous puissions prendre **des sanctions sans mise en demeure préalable dans certains cas** très particuliers d'urgence ou de gravité extrême. Notamment lorsqu'on se trouve en présence d'une faille majeure qui doit être très rapidement traitée, nous pourrons ainsi avoir la possibilité d'aller au-delà d'un seul avertissement.

Le règlement européen est un autre élément qui va changer la donne sur la question de la responsabilisation des opérateurs économiques. Il va donner à la sécurité une dimension nouvelle pour deux raisons. Premièrement, **les sous-traitants vont se voir attribuer des responsabilités spécifiques au regard de la loi informatique et libertés,** au même titre que les responsables de traitement, ce qui n'est pas le cas aujourd'hui. Les sous-traitants sont actuellement soumis à une obligation de sécurité, mais nous ne pouvons prononcer de sanctions que par rapport aux responsables de traitement.

La deuxième avancée du règlement européen est la mise en place de l'*accountability*, c'est-à-dire la **responsabilisation des entreprises** par rapport aux données personnelles, à travers un certain nombre d'instruments internes aux entreprises par lesquels elles doivent démontrer qu'elles appliquent effectivement les principes de la loi informatique et libertés. Par exemple, le *Privacy Impact Assessment (PIA)*, **outil d'analyse d'impact,** va les conduire à mener une analyse de risque sur les traitements importants qu'elles mettent en œuvre. Ces *PIAs* peuvent renforcer la responsabilisation des acteurs professionnels.

En conclusion, concernant les acteurs professionnels, je crois que nous disposons des outils et nous les complétons à la marge mais que la prise de conscience ne se fait pas aussi vite qu'on pourrait le souhaiter.

La deuxième cible, ce sont les individus. J'ai compris en vous écoutant, madame Le Dain, qu'ils n'étaient pas au centre des préoccupations de votre étude. Mais, en réalité, l'individu est un personnage central dans la sécurité. On sait bien qu'**une partie des failles de sécurité vient des individus eux-mêmes, notamment au sein de l'entreprise**. Il est donc absolument essentiel de faire passer des messages auprès d'eux. À cet égard, je vois deux leviers.

Le premier levier consiste à développer une culture de la sécurité auprès des individus, montrant l'interdépendance nouvelle entre les uns et les autres à travers cette interconnexion généralisée, et les réflexes nouveaux qu'il faut avoir. C'est l'une des briques très importantes au sein du programme général d'éducation au numérique que nous promouvons avec d'autres. La CNIL a en effet pris l'initiative de construire un collectif visant **à faire reconnaître l'éducation au numérique comme une grande cause nationale en 2014**. Il faut faire passer un message général auprès des individus en leur disant qu'ils sont, désormais, acteurs de la sécurité et qu'ils doivent en être conscients.

Le deuxième levier, probablement plus positif, est de dire à l'individu que, par rapport à ces atteintes à la sécurité, notamment relatives à ses données, il peut, lui-même, améliorer la maîtrise de ses données personnelles et donc celle de sa sécurité, en mobilisant les droits qui sont les siens, au regard de la loi informatique et libertés ou du futur projet de règlement européen.

Par exemple, le droit à l'oubli qui va être consacré par le projet de règlement européen. Il s'agit de la capacité qu'a l'individu de maîtriser le devenir de sa donnée et c'est aussi un moyen d'assurer la sécurité de ses données par rapport à d'éventuelles captations par des tiers.

Le droit à l'oubli vient d'être renforcé par un arrêt de la Cour de justice de l'Union européenne qui a affirmé un droit complémentaire qui est le droit au déréférencement, c'est-à-dire la possibilité pour chaque individu, non seulement d'aller voir le site auprès duquel l'information a été initialement publiée, mais de s'adresser aux moteurs de recherche pour demander le déréférencement de sa donnée dans certaines conditions. C'est la première fois que ce droit est affirmé. C'est un élément de sécurisation, par l'individu lui-même, de ses données.

Un autre exemple est le droit à la portabilité des données. Ce droit n'existe pas actuellement en droit français, mais il existera en application du projet de règlement européen. Ce droit à la portabilité offre aux individus la possibilité d'aller voir la plate-forme, le vendeur auprès duquel il a déposé toute une série de données personnelles, pour récupérer celles-ci et les porter ailleurs. Là aussi, c'est un moyen pour l'individu de maîtriser ses données et d'en assurer lui-même la sécurité.

Concernant la responsabilisation des individus, toutes les nouvelles initiatives qui se développent aujourd'hui vont permettre à l'individu de récupérer ses données pour les valoriser d'une autre façon et pour profiter d'un certain nombre de nouveaux services. Je pense, par exemple, au projet *MesInfos* (fing.org). Tous ces services nouveaux visent à placer l'individu dans la chaîne de sécurité, en lui faisant passer le message suivant : **vous êtes les acteurs de votre propre sécurité.**

La troisième dimension est collective. Les enjeux de sécurité sont systémiques. Bien que la CNIL soit moins directement concernée par cet aspect, l'affaire *Prism* a révélé que nous sommes face à une infrastructure générale d'information qui conduit à automatiser la surveillance, de manière systématique et indifférenciée, de tous les citoyens européens à travers l'usage quotidien qu'ils font des plates-formes. Pour des raisons de lutte contre le terrorisme, nous dit-on. Ce dispositif de surveillance révèle la complexité des partenariats entre les acteurs publics et privés, mais, au fur et à mesure que s'égrènent les révélations de M. Snowden, nous apprenons que **la question ne concerne pas que l'Europe et les États-Unis d'Amérique, mais aussi ce qui se passe chez chacun.**

Par rapport à ces révélations, la CNIL pose deux questions : comment assurons-nous la maîtrise de notre gisement informationnel, c'est-à-dire les données de nos concitoyens européens, par rapport à des tiers étrangers ? Comment assurons-nous, sur ce gisement de données informationnelles, la protection des libertés de nos concitoyens français ou européens, y compris vis-à-vis des services de renseignement du pays de chacun ?

En tant qu'autorité en charge de la protection des données personnelles, la CNIL s'est intéressée à ces deux objectifs. Des réponses commencent à se mettre en place. Elles sont complexes et pas encore conclusives.

Lors d'une audition qui s'est tenue quelque temps après l'affaire *Prism*, nous avions proposé au Parlement européen une première réponse, qui a été reprise par les parlementaires. C'est l'introduction, dans le projet de règlement, de l'article 43a, qui dit la chose suivante : dès qu'une autorité administrative étrangère veut avoir accès à des données concernant des citoyens européens, elle doit, d'une manière ou d'une autre, avoir l'accord d'une autorité nationale européenne. Un tel accord reste à définir, mais c'est un verrou car on ne peut plus, dès lors, aspirer, sans rendre des comptes, le gisement de données de citoyens européens pour des raisons de renseignement, de lutte contre la corruption, de contrôle des données passagers, etc. On ne le sait pas, mais, en réalité, beaucoup de finalités ont déjà conduit à des demandes d'accès de ce type. Or, cela ne peut être fait sans qu'il y ait une négociation et un cadre qui soient élaborés entre l'autorité étrangère qui demande l'accès et les autorités nationales européennes concernées. Ce débat est assez technique, mais essentiel car il peut permettre de « glisser un pied dans la porte » si je puis dire.

Faut-il aller au-delà et imaginer une loi de blocage au niveau européen ? Il faut y réfléchir. On sent bien qu'on ne peut pas continuer à laisser se mettre en place une surveillance généralisée, systématique et automatisée, d'autant qu'un deuxième élément est intervenu. L'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 a invalidé la directive *data retention* relative à la conservation des données de connexion au regard de la charte des droits fondamentaux - articles 7 et 8. En résumé, les juges disent qu'il existe une forme de disproportion dans le dispositif qui a été adopté. Le rapport d'analyse et d'évaluation qui a été rédigé par la Commission quelques mois avant, avait également conclu que ce dispositif n'était pas optimum.

On voit bien que, vis-à-vis de tiers extérieurs à l'Union, il faut apporter des réponses et affirmer la souveraineté numérique de l'Europe. Mais, d'une façon générale, des accès aussi massifs, indifférenciés et automatisés, concernant des citoyens européens, y compris par leurs propres autorités de renseignement, ne sont pas acceptables.

Cela a conduit la CNIL à faire une proposition aux autorités nationales françaises. Aujourd'hui, les fichiers de renseignement ne font l'objet d'aucun contrôle externe de qui que ce soit. Cela n'est pas sain, compte tenu de l'ampleur de la surveillance qu'a révélée l'affaire *Prism*. Désormais, il est nécessaire d'apporter des garanties aux citoyens sur l'existence d'un cadre, proportionné, de ladite surveillance. **Nous avons proposé aux pouvoirs publics que la CNIL puisse être chargée du contrôle des fichiers de souveraineté** dans certaines conditions, notamment dans des conditions d'habilitation « secret défense », avec un collège spécifique qui existe déjà à la CNIL à travers le droit d'accès indirect. Ces fichiers de souveraineté sont totalement dérogatoires au regard de notre loi par rapport aux autres fichiers de police. Nous demandons que ce collège spécialisé de la CNIL puisse contrôler non pas l'activité des services de renseignement, mais le fait que ces fichiers fonctionnent dans le respect du droit des personnes.

Je terminerai par une dernière proposition pour améliorer cette « sécurité en réseau ». La CNIL travaille avec d'autres autorités publiques : l'ANSSI, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), *Signal Spam* et toute une série d'autorités avec lesquelles nous avons signé des conventions sur ces questions de sécurité pour travailler ensemble. Il me semble que nous gagnerions collectivement beaucoup si, sur cette question

de la sécurité, nous allions peut-être plus loin à travers un groupe de contact, en tout cas des échanges continus entre les acteurs publics concernés, sur ces questions qui sont d'intérêt commun.

M. Bruno Sido, président de l'OPECST. - Merci madame la présidente pour l'éclairage nouveau que vous avez su donner à votre présentation. Je suppose qu'elle va donner lieu à des questions après l'intervention de M. Gilles Babinet.

Mme Le Dain et moi-même nous sommes rendus à Bruxelles la semaine dernière pour une journée d'entretien avec des responsables de la sécurité numérique. Il nous est apparu que l'imbrication des normes juridiques et techniques internationales, européennes et nationales, avait atteint un certain degré de complexité - c'est un euphémisme -, peut-être au détriment de leur efficacité.

Pour autant, des solutions ne sont pas davantage à attendre d'un surcroît de normes que d'une simplification de celles-ci. Elles viendront plutôt d'une réflexion d'ampleur sur tous les changements de mentalité et de comportements que suppose le recours généralisé à l'usage des outils du numérique sur des réseaux dont les failles techniques viennent souvent aggraver les failles humaines.

M. Gilles Babinet, responsable des enjeux de l'économie numérique pour la France *(French Digital Champion)*, Commission européenne. - Ce débat d'aujourd'hui est essentiel. Je vais vous faire des commentaires directement liés aux enjeux de sécurité, en particulier sur ce qui se fait au niveau européen, puis je ferai des commentaires plus généraux sur les sujets de la donnée.

En matière de sécurité, plusieurs initiatives existent ou ont existé au niveau européen. Ces éléments de normalisation peuvent être le fait directement de l'Europe, ou le fait d'agences de normalisation qui n'y sont pas directement rattachées, mais dont l'impact sur la façon de structurer les réseaux est très conséquent. Je pense à l'*European Telecommunications Standards Institute (ETSI)* par exemple. Ils peuvent aussi être le fait de la correspondance entre des organismes techniques liés à la création de formats de sécurité sur Internet en particulier. Ces travaux sont principalement techniques, ils n'ont pas de nature à proprement parler juridique (recherche d'algorithme, de modèles d'échanges les plus performants entre les systèmes au sens large).

D'une façon générale, l'Europe se réveille un peu en retard en matière de sécurité. Les grandes sociétés de conseil font assez régulièrement des comparaisons en matière de processus de sécurité dans les entreprises, je pense à l'étude de *Capgemini*, par exemple, il y a deux ans. Elles montrent clairement que **les sociétés américaines accordent plus d'attention à la sécurité que les sociétés européennes**. Et au sein de l'Europe, il y a de grandes différences entre les pays.

Malheureusement, la France n'a pas investi beaucoup, même s'il y a un rattrapage dans ce domaine. J'en tiens pour preuve un exercice que j'ai lancé avec le journal *Les Échos* il y a deux mois, qui consiste à mesurer l'agilité numérique des entreprises du CAC 40. Le sondage comporte une centaine de questions et à ce jour, j'ai pris connaissance de vingt-six formulaires. Sans révéler de noms, je peux vous dire que **la prise de conscience est extrêmement récente** et qu'elle se traduit par **un accroissement important des budgets consacrés à la sécurité**. Approximativement, pour les entreprises dont nous avons dépouillé les résultats, la croissance des budgets en matière de sécurité entre 2012 et 2013 est de l'ordre de 40 %. Le budget moyen se situe aux alentours de 70 millions d'euros. Ce sont des montants importants qui sont affectés à la fois aux processus technologiques et aux formations des cadres dirigeants, des cadres intermédiaires et des équipes en général.

Deux affaires publiques, que l'on peut évoquer, ont réveillé les consciences puisque, semble-t-il, il y a eu des fuites importantes au sein d'*Airbus* et d'*Areva*, alors qu'une attention forte était donnée à la sécurité. En tout cas, dans l'une de ces deux entreprises, ce n'est pas en soi les processus techniques qui ont failli, mais une **formation insuffisante des équipes** qui n'étaient pas éveillées au risque de faille dans la sécurité.

À l'échelle européenne, je peux également vous dire qu'il y a la volonté d'une sorte de souveraineté de la sécurité européenne. Mme Neelie Kroes s'est exprimée à cet égard, elle y est sensible et pense qu'il faut absolument une coordination européenne à cet égard. Au-delà, il existe des financements européens qui sont affectés à une trentaine de projets, dont quelques-uns ont une taille significative.

Je pense en particulier au financement des réseaux quantiques. Ceux-ci ont une caractéristique : **sur la partie transport, ils sont impossibles à espionner**, c'est-à-dire que l'on ne peut pas extraire de la donnée sans que ce soit visible dans le réseau. Les travaux qui sont menés à cet égard sont assez prometteurs. Cela ne résout pas tout, parce qu'il peut y avoir des failles humaines ou des failles de traitement. Je ne parle pas d'ordinateur quantique, mais juste de transmission de données. Mme Neelie Kroes s'est encore récemment exprimée sur ce sujet. C'est intéressant de voir que l'Europe peut être chef de file dans ce domaine, c'est ce qui semble être le cas aujourd'hui.

Je ne suis pas un spécialiste de *Prism*. Je lis la même chose que vous dans la presse et je me garderai bien de faire des commentaires de comptoir. En revanche, sur l'accord commercial transatlantique TAFTA *(Trans-Atlantic Free Trade Agreement)*, je peux vous dire objectivement qu'il a été très mal vécu au sein de la Commission européenne, laquelle l'a perçu comme une trahison. D'ailleurs, cela a ralenti les discussions. Et sans connaître aucunement ce qui se dit en matière de traité transatlantique pour les données, puisque par définition ces négociations sont secrètes, je crois savoir que cela a permis aux Européens d'être beaucoup plus attentifs à cette notion et donc assez exigeants.

Je voudrais aussi vous dire que depuis l'affaire *Prism*, des initiatives sont prises par différents pays. En particulier, l'initiative allemande me semble assez intéressante à certains égards. Elle comporte plusieurs aspects.

Il y a d'abord **cette idée selon laquelle il faut que les données soient localisées dans des pays européens. Je trouve cette initiative infondée. Cela n'a pas de sens au plan technique**. Ce qui est important, c'est la sécurité que l'on assure à ces données et la façon dont on les traite. La localisation technique des données n'a aucun sens. Je peux vous dire que, dans bien des cas, les administrateurs des nuages numériques (*clouds*) ont eux-mêmes du mal à savoir où se trouvent les données. Pour des raisons techniques de sécurité des données, mais aussi pour des besoins de performance, ces données sont répliquées. Dans certaines grandes entreprises, les expériences ont montré que **les mêmes données sont localisées dans plus de trente endroits à la fois**. De fait, imposer une localisation géographique, cela créerait, d'une part, des contraintes supplémentaires dans la gestion de ces données, et, d'autre part, cela limiterait la performance des réseaux et donc des acteurs propriétaires de ces données.

Le nuage numérique européen est une initiative très populaire dont on entend beaucoup parler. Je regrette que l'argent investi par la France dans cette idée de « nuage souverain » n'ait pas été investi en sécurité des données. Cela m'aurait semblé beaucoup plus pertinent. Je me suis déjà exprimé à ce titre, j'en profite pour le redire.

Les Allemands ont également pris l'initiative d'émettre leurs normes de sécurité. Ils ont recommandé que ce soit une norme nationale largement répandue. J'ai émis exactement la même idée auprès du ministère du redressement productif. J'aurais beaucoup apprécié que ce soit une norme européenne, mais **il est possible de créer, ou en tout cas d'utiliser les normes existantes « adaptées »**, pour faire en sorte que ce soient des normes européennes ou nationales et qu'elles soient très sûres.

On sait, par exemple, qu'il y a des failles très importantes dans le *SSL*, une norme massivement utilisée et que l'on continue malgré tout à utiliser. Comme c'est une norme vieillissante, il a tendance à disparaître, mais c'est une norme percée qui continue à être utilisée.

Voilà les commentaires que je voulais vous faire sur ce qui se passe en Europe. D'une façon plus générale, et comme vient de le dire Mme Falque-Pierrotin, tout cela repose très largement sur le droit, un droit qui soit le plus constant possible et dont l'assiette géographique soit la plus large possible.

Il faut garder à l'esprit deux modèles anthropologiques qui s'affrontent. Le modèle anglo-saxon, une culture de la *common law* facilite à mon sens très largement l'expérimentation. Il considère que l'innovation est une notion intrinsèquement prioritaire, il faut d'abord expérimenter et on verra après. Bien que j'aie de très nombreuses critiques à son égard, c'est le modèle qui prédomine dans les *GAFA* (*Google, Amazon, Facebook, Apple*). Le modèle tente un tas de choses et il essaie de préserver une contrepartie implicite, c'est-à-dire qu'on vous rend un service de la plus grande valeur, souvent gratuitement, et en contrepartie, vous acceptez les conditions. On considère que votre droit, c'est de ne plus les accepter. Évidemment, on peut juger cela assez inégal. Il n'empêche qu'aujourd'hui des milliards de gens acceptent ce contrat implicite sous cette forme.

Cela doit nous faire réfléchir. Sans vouloir défendre nécessairement ce modèle anglo-saxon, je pense que le modèle qui consiste à avoir une régulation *ex ante, a priori*, est problématique dans certains cas, dans la mesure où certaines sociétés vont chercher à s'en affranchir. J'ai été surpris, dans le cadre des auditions que j'ai menées sur le CAC 40, qu'un certain nombre de sociétés m'avouent avoir décidé d'héberger leurs données en dehors de l'Europe, voire de les faire héberger avec une sorte d'isolation juridique, pour s'affranchir des contraintes de régulation européenne. C'est quand même lié aussi à des enjeux de sécurité et cela nous pousse à y réfléchir.

Au-delà, j'observe que tous ces principes de régulation sont jugés éminemment complexes et ils sont confiés à des autorités administratives. Il y a une difficulté à avoir un débat citoyen de bonne qualité sur ce sujet. Lorsque vous êtes dans des zones extrêmement exploratoires et innovantes, le risque est d'avoir une régulation mal calée, qui finalement impacte la capacité d'innovation ou même d'inclusion sociale des nations.

Je pense en particulier au système de santé. Les systèmes de santé numériques recèlent des opportunités extraordinaires. Je ne cesse de le dire à une époque où les finances publiques sont en grand péril. On devrait accélérer notre mutation vers ce système de santé. Mais nous sommes tous conscients qu'il comporte également des risques très importants pour les citoyens. Pour caricaturer, une société d'assurance qui découvrirait dans un traitement de données que quelqu'un va avoir un cancer n'a aucun intérêt objectif à l'assurer. Cela est bien compris par tous. Pour autant, les croisements de données ont des capacités prédictives, des capacités d'augmentation de la qualité de prescription, de diagnostic, qui sont absolument incroyables. J'écris actuellement un livre sur ce sujet. Je pense qu'une des raisons qui ont ralenti notre capacité à faire émerger une médecine digitale du XXI[e] siècle, c'est un *a priori* qui consiste à croire que l'on ne peut rien faire sans que la régulation soit parfaitement calée.

Le risque, qui est à mon sens aujourd'hui avéré, c'est finalement que les gens en viennent à confier leurs données à *Apple* par exemple, lequel vient de faire une annonce en ce sens. La qualité et la capacité de traitement de ces sociétés vont devenir tellement importantes à court terme, en quelques années, qu'il est probable que toute cette partie de traitement et de diagnostic soit progressivement extraite du système de santé publique pour être confiée à des acteurs privés. Ceux-ci vont récupérer des quantités de données incroyables qui seront affranchies dans une certaine mesure du droit européen parce que ce sera une exigence citoyenne. Les citoyens vont vouloir utiliser ces services. Il y a là quelque chose qui devrait nous pousser à réfléchir en matière de sécurité. Toutes ces données qui partent à l'extérieur des institutions et des entreprises européennes, c'est finalement une perte de souveraineté.

Je finirai par un mot sur le droit à l'oubli, qui a été abordé. Selon l'arrêté de la Cour de justice de l'Union européenne, ce droit donne la possibilité de modifier les données vous concernant. Là aussi, j'ai beaucoup d'inquiétudes. J'ai rencontré une association d'archivistes qui m'a dit que, dans une certaine mesure, c'est une **possibilité de réécriture de l'histoire**. Évidemment, je me place avant tout du côté des citoyens et des individus, mais je pense que, dans bien des cas, des gens qui ont été justement critiqués pourraient demander la modification des données qui les regardent.

De mon point de vue, cela reflète malgré tout un manque d'agilité numérique des institutions en général qui ont du mal à comprendre les enjeux. Finalement, il me semble que l'ensemble de la régulation et l'harmonisation de la régulation ne doivent pas passer nécessairement par des analyses techniques, mais plus par des analyses éthiques et d'usages en général. Cela est également vrai dans le domaine de la sécurité, où **ce n'est pas la technologie qui résout les problèmes, mais davantage la formation des gens**.

Pour conclure, je dirais qu'**il faut accélérer la prise de conscience à l'égard de l'ensemble de cette formidable révolution digitale**. C'est le point principal de mon intervention. C'est la seule façon pour accroître la sécurité et finalement, pour arriver à l'émergence d'une Europe numérique et l'inclusion citoyenne dans cette nouvelle ère.

Document n° 3 : L'ENA sur le chemin escarpé de la formation à l'open data- www.lagazettelescommunes.com- 21/05/2015 -Sabine Blanc

L'école nationale d'administration (ENA) a organisé au mois de mai une formation inédite sur le "partage et l'utilisation des données publiques numériques". Un premier "galop d'essai" qui reflète les difficultés persistantes pour que le sujet, aussi porté politiquement soit-il, infuse réellement dans les administrations.

Voilà plus de quatre ans que l'open data est porté politiquement au plus haut niveau, et de plus en plus avec la récente création du poste d'administrateur général des données. A gauche comme à droite, l'open data est loué. Quand il s'agit de rentrer dans le dur, c'est nettement plus laborieux, comme en témoigne le faible nombre de participants à la première formation continue sur le sujet montée par l'ENA en mai : six, déjà sensibilisés au sujet.

"C'est un galop d'essai", indique Jérôme Lartigau, conseiller pédagogique à l'ENA. Nous sommes persuadés que la donnée est primordiale et nous espérons qu'il y aura d'autres sessions." Primordiale, mais pas au point que la prestigieuse école ouvre ses données.

Issus de services en administration centrale -Éducation nationale, Développement durable… -, les "pionniers" ont eu droit à une (re)mise à niveau sur les fondamentaux du "partage et de l'utilisation des donnée publiques numériques", pour reprendre l'intitulé exact, qui renvoie à la gouvernance globale de la donnée. Ces cours théoriques n'ont rien de superflu, tant ce sujet brasse des problématiques complexes.

Droit d'auteur, propriété intellectuelle, données personnelles…

"Qui est propriétaire de la donnée ?", lance Lancelot Pecquet. "Celui qui produit la donnée", avance déjà Isabelle Leleu, cheffe de service adjointe du service central d'hydrométéorologie et d'appui à la prévision des inondations (Schapi) au ministère du Développement durable. La question en amène d'autres qui conduisent sur les rives escarpées du droit d'auteur, de la propriété intellectuelle, des données personnelles.

Dans le cas des données publiques, "cela renvoie à la question des biens communs", indique Lancelot Pecquet. En clair, une donnée publique appartient à tout le monde, à partir du moment où le cadre légal est respecté, comme la non-divulgation de données personnelles.

Un subtil équilibre entre tout le dispositif législatif encourageant l'ouverture des données depuis la loi Cada de 1978, et la loi Cnil de 1978 qui protège pour sa part des dérives liées à leur utilisation.

Autre sujet qui agite dans les chaumières administratives : celle du financement. L'occasion de revenir sur le rapport Trojette de 2013 portant sur les redevances sur les données publiques. La crainte de voir un apport d'argent disparaître, voire de causer des coûts en plus, fait partie des arguments avancés par les administrations sollicitées pour ne pas ouvrir les données.
"Il faut faire la différence entre les entités à qui on demande de trouver leurs fonds et les ministères, estime un des participants. Cela rejoint le débat sur le financement des services publics, il revient au politique de trancher ; les opérateurs, cela leur est égal, tant qu'on leur donne l'équivalent en fonds."

A lire aussi Le rapport Trojette habille pour l'hiver les redevances sur les données publiques

Le Graal mouvant de l'anonymisation

La question du financement semble toutefois une galéjade à côté de celle de l'anonymisation des données. "D'après une étude de l'UE, il existe toujours un risque résiduel plus ou moins important de réidentification, relève Lancelot Pecquet, il peut s'avérer délicat de trouver une réponse satisfaisante."
"C'est un gros problème pour nos enquêtes, nous avons 1400 variables, une seule suffit à réidentifier", illustre Florence Ryk, chargée d'études et d'enquêtes au département entrées et évolutions dans la vie active (DEEVA) du centre d'études et de recherche sur les qualifications (Céreq) et correspondante informatique et libertés (CIL) de l'établissement. Nous en retirons un maximum quand nous passons les données aux chercheurs."

Si le risque est réel, il ne faut pas pour autant verser dans des hypothèses anxiogènes et peser les avantages et les inconvénients par rapport au risque. Au passage, grince Benjamin Ooghe-Tabanou, administrateur de l'association Regards citoyens qui a assuré un session de la formation, l'État vend déjà des données personnelles, comme le fichier des cartes grises.

Un objet de communication

De façon plus globale, c'est l'intérêt même de l'ouverture des données publiques qui est interrogée. Le portail controversé de l'Enseignement supérieur et de la Recherche, qui ne fait que doublonner les données de data.gouv.fr, le portail national, a animé la discussion.
"C'est un objet de communication", tranche Benjamin Ooghe-Tabanou. » C'est vrai que quelques jeux de données peuvent avoir un faible nombre de téléchargements, mais le plus important c'est l'utilisation qu'on en fait. Un jeu de données très peu téléchargé peut déboucher au final sur une super killer application.", veut croire Jean-Renaud Daclin, chef de projet fonctionnel au ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche.
"Mais il n'y a pas besoin d'un outil de communication, répète Benjamin Ooghe-Tabanou. On est dans le second 'effet kiss cool' : 'on nous avait promis d'énormes retombées !', disent les administrations. On n'a rien promis ! L'intérêt, ce sont les externalités positives, c'est un pari. Sinon, l'open data n'intéresse pas la plupart des gens."

"Il est vrai que l'open data est difficile à cerner et doit encore se concrétiser", note l'un des participants. "Il est possible de modéliser la valeur ajoutée qui n'est d'ailleurs pas forcément économique", note Lancelot Pecquet.
Récemment, la Sunlight foundation, une association américaine qui promeut davantage de transparence dans la démocratie, s'est attelée à évaluer différemment l'impact de l'open data, partant du constat que "les preuves fortes de l'impact à long terme des initiatives d'ouverture des données publiques sont incroyablement rares".

Problèmes de formatage

La partie théorique a été complétée par un volet qui se voulait plus pratique, et qui l'a été… en théorie. Des difficultés intéressantes à affronter car elles reflètent la réalité du quotidien des administrations. Dans la vie rêvée des praticiens de l'open data, un joli fichier CSV – c'est-à-dire impeccablement formaté pour être ouvert en trois clics sur n'importe quelle machine – est mis à disposition dans un licence ouverte.

Fin praticien de l'open data, tendance pure et dure, Benjamin Ooghe-Tabanou a plus pesté sur les bugs divers rencontrés – format bizarre, navigateur obsolète, etc… – qu'il n'a montré comment utiliser un fichier. "Le problème dans vos administrations, c'est que vous n'avez pas la main sur vos machines, qui ne sont pas toujours à jour", critique le jeune informaticien.

Didier Sarfati, responsable du bureau des systèmes d'information (BSI) du conseil général de l'environnement et du développement durable (CGEDD) propose de manipuler des données sur la qualité de service dans les transports, en l'occurrence la ponctualité. "Mon regard de citoyen, c'est qu'il n'est pas du tout pratique de cliquer sur plein de boutons pour accéder à quatre lignes de données. Il devrait y avoir sur data.gouv tout le fichier mis en ligne chaque mois, en plus de ce web service."

"Il faut donc une personne pour s'en charger", remarque un participant. La réaction fuse : "Chez Regards citoyens, tout est automatisé, le robot ne signale que les erreurs." Et bonne nouvelle, data.gouv dispose maintenant d'une API [1] permettant d'automatiser la publication sur sa plate-forme. Heureusement car "le formulaire de publication de data.gouv n'est vraiment pas drôle", se réjouit Benjamin Ooghe-Tabanou.

Faute de pouvoir faire quelque chose avec ces données de transport, Florence Ryk propose celle du Céreq sur le parcours des jeunes après la sortie du système scolaire. Au bout de 10 minutes, le gros fichier de 21 Mo s'ouvre enfin sur des lignes illisible pour un humain : les variables sont des nombres, il faut donc ouvrir le dictionnaire des variables pour voir la correspondance.

Trop compliqué en si peu de temps, d'autant plus qu'elles sont disponibles sur un pdf, l'enfer absolu de la réutilisation puisque ce format n'est pas lisible de façon automatique par un ordinateur. La réalisation d'une "visualisation amusante" attendra encore. A la fin, on se rabattra sur… un fichier de La Gazette des communes, pas très sexy, mais formaté. Au moins Benjamin Ooghe-Tabanou peut-il montrer comment marche Raw, un des outils de visualisation de données qu'il a présentés. "Je vous rappelle que cette formation est expérimentale", plaisante Lancelot Pecquet.

Monsieur Jourdain de l'open data

Tout comme monsieur Jourdain, les participants reconnaissent que leurs administrations font déjà de l'open data sans le savoir. Et c'est peut-être pour cette raison que cela passe, tant que ce que le mouvement implique en termes de changement de mentalités n'est pas surligné à grand renfort de communication.

"L'enjeu, c'est la conduite du changement face à l'ouverture des données, analyse Jean-Renaud Daclin. Détenir l'information c'est détenir une forme de pouvoir. Cette perte peut représenter une crainte pour les services sans compter que cela peut amener un sentiment de désappropriation et de dévalorisation de son propre travail au profit d'autres personnes. Il ne faut pas négliger également la crainte politique qui est aussi bien réelle car en rendant libre nos données nous ne maîtrisons plus sa diffusion et son interprétation par d'autres, or nous sommes là pour valoriser l'action du ministère."

C'est aussi des stratégies d'ouverture qui sont à réfléchir, pour rassurer au mieux les parties prenantes, comme l'explique Isabelle Leleu : "Nous travaillons à la cartographie des zones inondables en temps réel. Nous pouvons impliquer les acteurs locaux, qui comprendront mieux les données. Et nous allons

d'abord la mettre à disposition des gestionnaires de crise puis du grand public, quand les données et la méthodologie seront consolidées." Elle souligne que si les équipes sont sensibilisées à l'open data, le manque se fait surtout sentir en matière de veille sur un sujet qui évolue vite. Et de déplorer aussi dans l'ensemble "le manque de démonstration volontariste dans les ministères", regret qui n'a rien d'isolé.

Document n ° 4 - 10 conseils pour la sécurité de votre système d'information – www.cnil.fr - 12 octobre 2009

La loi "informatique et libertés" impose que les organismes mettant en œuvre des fichiers garantissent la sécurité des données qui y sont traitées. Cette exigence se traduit par un ensemble de mesures que les détenteurs de fichiers doivent mettre en œuvre, essentiellement par l'intermédiaire de leur direction des systèmes d'information (DSI) ou de leur responsable informatique.

1. Adopter une politique de mot de passe rigoureuse

L'accès à un poste de travail informatique ou à un fichier par identifiant et mot de passe est la première des protections. Le mot de passe doit être individuel, difficile à deviner et rester secret. Il ne doit donc être écrit sur aucun support. La DSI ou le responsable informatique devra mettre en place une politique de gestion des mots de passe rigoureuse : un mot de passe doit comporter au minimum 8 caractères incluant chiffres, lettres et caractères spéciaux et doit être renouvelé fréquemment (par exemple tous les 3 mois). Le système doit contraindre l'utilisateur à choisir un mot de passe différent des trois qu'il a utilisés précédemment. Généralement attribué par l'administrateur du système, le mot de passe doit être modifié obligatoirement par l'utilisateur dès la première connexion. Enfin, les administrateurs des systèmes et du réseau doivent veiller à modifier les mots de passe qu'ils utilisent eux-mêmes.

2. Concevoir une procédure de création et de suppression des comptes utilisateurs

L'accès aux postes de travail et aux applications doit s'effectuer à l'aide de comptes utilisateurs nominatifs, et non « génériques » (compta1, compta2...), afin de pouvoir éventuellement être capables de tracer les actions faites sur un fichier et, ainsi, de responsabiliser l'ensemble des intervenants. En effet, les comptes « génériques » ne permettent pas d'identifier précisément une personne. Cette règle doit également s'appliquer aux comptes des administrateurs systèmes et réseaux et des autres agents chargés de l'exploitation du système d'information.

3. Sécuriser les postes de travail

Les postes des agents doivent être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité (10 minutes maximum) ; les utilisateurs doivent également être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau. Ces dispositions sont de nature à restreindre les risques d'une utilisation frauduleuse d'une application en cas d'absence momentanée de l'agent du poste concerné. Par ailleurs, le contrôle de l'usage des ports USB sur les

postes « sensibles », interdisant par exemple la copie de l'ensemble des données contenues dans un fichier, est fortement recommandé.

4. Identifier précisément qui peut avoir accès aux fichiers

L'accès aux données personnelles traitées dans un fichier doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées. De cette analyse, dépend « le profil d'habilitation » de l'agent ou du salarié concerné. Pour chaque mouvement ou nouvelle affectation d'un salarié à un poste, le supérieur hiérarchique concerné doit identifier le ou les fichiers auxquels celui-ci a besoin d'accéder et faire procéder à la mise à jour de ses droits d'accès. Une vérification périodique des profils des applications et des droits d'accès aux répertoires sur les serveurs est donc nécessaire afin de s'assurer de l'adéquation des droits offerts et de la réalité des fonctions occupées par chacun.

5. Veiller à la confidentialité des données vis-à-vis des prestataires

Les interventions des divers sous-traitants du système d'information d'un responsable de traitement doivent présenter les garanties suffisantes en terme de sécurité et de confidentialité à l'égard des données auxquels ceux-ci peuvent, le cas échéant, avoir accès. La loi impose ainsi qu'une clause de confidentialité soit prévue dans les contrats de sous-traitance. Les éventuelles interventions d'un prestataire sur des bases de données doivent se dérouler en présence d'un salarié du service informatique et être consignées dans un registre. Les données qui peuvent être considérées « sensibles » au regard de la loi, par exemple des données de santé ou des données relatives à des moyens de paiement, doivent au surplus faire l'objet d'un chiffrement.

« A noter » : l'administrateur systèmes et réseau n'est pas forcément habilité à accéder à l'ensemble des données de l'organisme. Pourtant, il a besoin d'accéder aux plates-formes ou aux bases de données pour les administrer et les maintenir. En chiffrant les données avec une clé dont il n'a pas connaissance, et qui est détenue par une personne qui n'a pas accès à ces données (le responsable de la sécurité par exemple), l'administrateur peut mener à bien ses missions et la confidentialité est respectée.

6. Sécuriser le réseau local

Un système d'information doit être sécurisé vis-à-vis des attaques extérieures.

Un premier niveau de protection doit être assuré par des dispositifs de sécurité logique spécifiques tels que des routeurs filtrants (ACL), pare-feu, sonde anti intrusions, etc. Une protection fiable contre les virus et logiciels espions suppose une veille constante pour mettre à jour ces outils, tant sur le serveur que sur les postes des agents. La messagerie électronique doit évidemment faire l'objet d'une vigilance particulière. Les connexions entre les sites parfois distants d'une entreprise ou d'une collectivité locale doivent s'effectuer de manière sécurisée, par l'intermédiaire des liaisons privées ou des canaux sécurisés par technique de « tunneling » ou VPN (réseau privé virtuel). Il est également indispensable de sécuriser les réseaux sans fil compte tenu de la possibilité d'intercepter à distance les informations qui y circulent : utilisation de clés de chiffrement, contrôle des adresses physiques des postes clients autorisés, etc. Enfin, les accès distants au système d'information par les postes nomades

doivent faire préalablement l'objet d'une authentification de l'utilisateur et du poste. Les accès par internet aux outils d'administration électronique nécessitent également des mesures de sécurité fortes, notamment par l'utilisation de protocoles IPsec, SSL/TLS ou encore HTTPS.

« A noter » : Un référentiel général de sécurité, relatif aux échanges électroniques entre les usagers et les autorités administratives (ordonnance 2005-1516), doit voir le jour prochainement (voir projet sur le site www.ssi.gouv.fr). Il imposera à chacun des acteurs des mesures de sécurité spécifiques.

7. Sécuriser l'accès physique aux locaux

L'accès aux locaux sensibles, tels que les salles hébergeant les serveurs informatiques et les éléments du réseau, doit être limité aux personnels habilités. Ces locaux doivent faire l'objet d'une sécurisation particulière : vérification des habilitations, gardiennage, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs, etc. La DSI ou le responsable informatique doit veiller à ce que les documentations techniques, plans d'adressages réseau, contrats, etc. soient eux aussi protégés.

8. Anticiper le risque de perte ou de divulgation des données

La perte ou la divulgation de données peut avoir plusieurs origines : erreur ou malveillance d'un salarié ou d'un agent, vol d'un ordinateur portable, panne matérielle, ou encore conséquence d'un dégât des eaux ou d'un incendie. Il faut veiller à stocker les données sur des espaces serveurs prévus à cet effet et faisant l'objet de sauvegardes régulières. Les supports de sauvegarde doivent être stockés dans un local distinct de celui qui héberge les serveurs, idéalement dans un coffre ignifugé. Les serveurs hébergeant des données sensibles ou capitales pour l'activité l'organisme concerné doivent être sauvegardés et pourront être dotés d'un dispositif de tolérance de panne. Il est recommandé d'écrire une procédure « urgence - secours » qui décrira comment remonter rapidement ces serveurs en cas de panne ou de sinistre majeur. Les supports nomades (ordinateurs portables, clé USB, assistants personnels etc.) doivent faire l'objet d'une sécurisation particulière, par chiffrement, au regard de la sensibilité des dossiers ou documents qu'ils peuvent stocker. Les matériels informatiques en fin de vie, tels que les ordinateurs ou les copieurs, doivent être physiquement détruits avant d'être jetés, ou expurgés de leurs disques durs avant d'être donnés à des associations. Les disques durs et les périphériques de stockage amovibles en réparation, réaffectés ou recyclés, doivent faire l'objet au préalable d'un formatage de bas niveau destiné à effacer les données qui peuvent y être stockées.

9. Anticiper et formaliser une politique de sécurité du système d'information

L'ensemble des règles relatives à la sécurité informatique doit être formalisé dans un document accessible à l'ensemble des agents ou des salariés. Sa rédaction requiert l'inventaire préalable des éventuelles menaces et vulnérabilités qui pèsent sur un système d'information. Il convient de faire évoluer régulièrement ce document, au regard des modifications des systèmes et outils informatiques utilisés par l'organisme concerné. Enfin, le paramètre « sécurité » doit être pris en compte en amont de tout projet lié au système d'information.

10. Sensibiliser les utilisateurs aux « risques informatiques » et à la loi "informatique et libertés"

Le principal risque en matière de sécurité informatique est l'erreur humaine. Les utilisateurs du système d'information doivent donc être particulièrement sensibilisés aux risques informatiques liés à l'utilisation de bases de données. Cette sensibilisation peut prendre la forme de formations, de diffusion de notes de service, ou de l'envoi périodique de fiches pratiques. Elle sera également formalisée dans un document, de type « charte informatique », qui pourra préciser les règles à respecter en matière de sécurité informatique, mais aussi celles relatives au bon usage de la téléphonie, de la messagerie électronique ou encore d'internet. Ce document devrait également rappeler les conditions dans lesquelles un salarié ou un agent peut créer un fichier contenant des données personnelles, par exemple après avoir obtenu l'accord de son responsable, du service juridique ou du CIL de l'entreprise ou de l'organisme dans lequel il travaille.

Ce document doit s'accompagner d'un engagement de responsabilité à signer par chaque utilisateur.

A noter : veiller à ce que les utilisateurs nettoient régulièrement leurs vieux documents et messages électroniques sur leurs postes. De même, nettoyer régulièrement le répertoire d'échange partagé entre les différents services afin qu'il ne se transforme pas en espace « fourre-tout » (fichiers personnels des agents mélangés avec des dossiers sensibles)

Document n° 5 : Protection de l'information - Enjeux, gouvernance et bonnes pratiques - http://www.cigref.fr/cigref_publications - 2008

Dans le cadre de ses groupes d'échanges de pratiques, le CIGREF a retenu un axe de travail autour de la protection de l'information, en termes d'usages des systèmes d'information.
Le pilotage de ce groupe de travail a été assuré par Jean-Pierre Gagnepain, DSI d'Air Liquide.
Le CIGREF s'est intéressé cette année à ce thème car l'information est au cœur des actifs immatériels de l'entreprise. Et trop souvent le discours ambiant porte sur les aspects techniques et contenant de la sécurité au détriment de ses aspects organisationnels et contenu.
Il convient de définir au préalable ce que l'on entend par protection de l'information. En effet la protection de l'information, ce n'est pas seulement la confidentialité ou la valorisation de l'information. Le groupe de travail s'est intéressé au terme de protection de l'information

1- Définition

La protection de l'information est une démarche consciente visant à protéger, au sein de l'entreprise étendue, ce qui vaut la peine d'être protégé, tant au niveau des données que des supports d'information. Cette démarche implique un système de gestion, une identification des informations sensibles, une analyse de risques, des acteurs, avec des rôles et responsabilités et un programme de réduction des risques.
En effet, la collecte, la valorisation et la diffusion de l'information tant interne qu'externe constituent un élément clé de la compétitivité des entreprises. Les entreprises doivent également chercher à limiter au maximum le risque de diffusion d'informations confidentielles, que cette diffusion soit volontaire ou accidentelle.
Par ailleurs, les entreprises sont de plus en plus confrontées à des exigences légales en matière de conservation de données (données personnelles, données financières, archivage légal...) à des fins de conformités ou de contrôle, ou à valeur probante. L'ensemble de ces tendances pose, de manière sous-jacente, la question de la protection de l'information. Confidentielle, ou ouverte, structurée ou non, maîtrisée ou libre, l'information est un actif qu'il convient de protéger techniquement, juridiquement, humainement. On entend par actif, tout ce qui a de la valeur pour l'entreprise. Ce document vise l'ensemble des personnes concernées et en charge de la protection de l'information : dirigeants, responsables métiers, responsables sécurité, responsable intelligence économique, documentalistes, salariés.

2. Objectifs poursuivis

Les objectifs du groupe de travail ont été les suivants :
•Identifier et caractériser les enjeux liés à la protection de l'information en entreprise ;
•Comprendre les modèles d'organisation, les acteurs, les méthodes et les démarches ;
•Mieux positionner la démarche de protection de l'information au sein de l'entreprise en adoptant une approche de type gouvernance (rôles et acteurs) et en nouant un dialogue stratégique avec les métiers (implication, sensibilisation, responsabilisation, appropriation) ;
•Identifier des bonnes pratiques fortes et lister les précautions minimales à prendre ou à préparer ;
•Avoir une approche équilibrée entre les enjeux majeurs et les pratiques. La littérature sur la protection de l'information est ancienne, riche et abondante. La démarche suivie par le groupe de travail n'a pas été de réinventer la matière mais plutôt de la simplifier, d'avoir une approche transversale, en mettant l'accent sur la démarche, la sensibilisation et les bonnes pratiques.

Ce groupe de travail a cherché également à capturer les retours d'expérience les plus pertinents et à l'intérieur de ceux-ci, les « invariants », les éléments communs aux entreprises, notamment sur les aspects gouvernance, classification de l'information et sensibilisation. Ce groupe de travail n'a pas cherché à être exhaustif mais plutôt à être pertinent, en fournissant des éléments à la fois descriptifs

Le rapport s'est intéressé aux thèmes suivants :
•Les enjeux, les risques et les grands axes ;
•La démarche, l'organisation et la gouvernance ;
•La sensibilisation et l'implication des acteurs ;
•Les bonnes pratiques. Ce qui paraît critique (et perfectible) aujourd'hui dans une entreprise c'est :
1) de prendre conscience de ses enjeux et de ses risques ;
2) de mettre en place une démarche de gouvernance structurée et cohérente ;
3) de sensibiliser l'ensemble des acteurs et de promouvoir une culture de protection de l'information,
4) de conduire des actions concrètes et sélectives de réduction des risques.

3. Les enjeux, les risques, les grands axes

3.1. Les enjeux de la protection de l'information

L'information est aujourd'hui unanimement considérée comme un actif stratégique pour l'entreprise. En même temps, il s'agit d'un actif intangible, dont la valeur est difficilement mesurable et dont la prise de conscience pourrait être amplifiée chez les dirigeants. On se retrouve donc face à un paradoxe dans lequel l'accès à l'information est jugé stratégique alors que sa protection est jugée non prioritaire.

Longtemps on a considéré que la démarche de protection de l'information « papier » était suffisante, que le fait de ne pas faire transiter d'information sensible par des moyens électroniques, voire de chiffrer ponctuellement les documents électroniques ou les transmissions, était suffisant. Or il n'en est rien. Il existe en effet un certain nombre de tendances de fond et de ruptures d'ordre économique, réglementaire et sociologique, qui obligent à repenser de façon plus globale la protection de l'information. Parmi les évolutions internes on peut citer les tendances suivantes :
•L'explosion des services dématérialisés et des volumes d'information (structurée mais surtout non structurée) circulant dans les entreprises et sur Internet. Cette volumétrie croissante des contenus oblige à repenser et à industrialiser la démarche de protection de l'information ;
•L'environnement décentralisé des entreprises et l'hétérogénéité des niveaux de « sécurité » interne qui peuvent justifier la mise en place d'un référentiel de protection de l'information.
Parmi les évolutions externes on peut mentionner :
•La tendance à la convergence des usages domestiques et professionnels des SI.Wifi, messageries instantanées, réseaux sociaux, blogs, wikis...sont d'utilisations courantes dans la sphère privée mais souvent incompatibles avec les usages et les besoins dans l'entreprise. Ceci oblige à revoir les règles d'usages des SI (chartes) mais aussi à redéfinir plus précisément la valeur de ces systèmes d'information pour l'entreprise ;

•L'émergence de l'entreprise étendue, impliquant un changement des modèles d'affaire, des relations avec les clients, les partenaires, les fournisseurs, les salariés et conduisant à étendre le périmètre de protection de l'information au-delà des frontières traditionnelles de l'entreprise ;
•L'exigence de transparence et de reporting accru avec un renforcement des contraintes légales, réglementaires, contractuelles. Cette tendance conduit d'un côté à publier davantage d'informations mais d'un autre côté à contrôler en amont beaucoup plus finement leur origine, et véracité et en aval les destinataires de l'information ;
•La complexité et l'interaction croissante avec l'environnement, ce qui se traduit par exemple par une diversification et une dangerosité croissante des menaces, obligeant les entreprises à repenser leur politique de protection de l'information et à se préparer au changement.

3.2. Les risques en entreprise

Les évolutions internes et externes examinées ci-dessus sont porteuses de nouveaux risques.
Afin d'avoir une approche globale, efficace et cohérente, il est nécessaire d'identifier et d'intégrer les risques en amont de la démarche de protection de l'information. Les entreprises sont confrontées à des risques variés, complexes et croissants. Le CIGREF a déjà abordé la gestion des risques et la place du DSI dans la démarche dans un précédent rapport.

L'objectif ici n'est pas de refaire une nouvelle étude sur le sujet, mais plutôt de voir en quoi les risques impliquent d'avoir une démarche de protection de l'information. Cette démarche de protection doit s'inscrire en complément d'une politique de gestion des risques. On distingue généralement plusieurs types de risques : les risques financiers, opérationnels, de conformité et d'atteinte à l'image.
Les risques liés aux usages IT font partie des risques opérationnels. On peut classer les risques liés aux usages IT de différentes façons, par exemple :
•Les risques informationnels ;
•Les risques liés aux applications ;
•Les risques liés aux développements ;
•Les risques liés à la maintenance ;
•Les risques liés aux infrastructures, serveurs ;
•Les risques liés aux projets ;
•Les risques liés aux fournisseurs.
Les critères pris en considération pour l'analyse des risques IT sont classiques :
•Disponibilité ;
•Intégrité ;
•Confidentialité ;
•Continuité ;
•Preuve / Traçabilité / Auditabilité. Ce que l'on peut dire des risques aujourd'hui en entreprise, c'est qu'il est indispensable de répertorier ces risques, de les hiérarchiser, de les relier à des processus, et de mettre en place un modèle de gouvernance approprié afin de les gérer tant d'un point de vue performance financière, conformité, continuité, image et protection de l'information...
•Associer le Correspondant Informatique et Libertés (CIL) le cas échéant (quand il est nommé) dans la démarche de protection de l'information et vérifier qu'elle est compatible avec la réglementation en vigueur (notamment la durée de conservation des données).

4. Les bonnes pratiques RH

•Impliquer les RH dans la démarche, dans la définition, la mise en œuvre et le contrôle ;
•S'assurer de la définition et du respect des engagements de confidentialité sur les postes clés ;
•Instiller la sensibilisation sécurité dans les fonctions et dans la démarche qualité ;
•Intégrer la sensibilisation à la protection de l'information dans l'évaluation, dans le Droit Individuel à la Formation (DIF) et dans l'intéressement ;
•Utiliser le e-learning (sans forcément commencer par la sécurité)

Document n ° 6 : La sécurisation des données est un enjeu- http://www.toolinux.com - 13/03/2015

La sécurisation des données est un enjeu colossal à l'heure du cloud, notamment pour les entreprises et collectivités locales. Quatre éléments essentiels doivent absolument être pris en compte, selon Yann Duverdier (JVS-Mairistem).

Sauvegarde

Les entreprises et les collectivités doivent faire face à un environnement toujours plus hétérogène et l'utilisation de plus en plus fréquente de l'informatique dématérialisée en fait partie. De nombreuses entreprises gèrent donc aujourd'hui des environnements physiques, des environnements virtuels ainsi que des environnements Cloud. De nombreuses entreprises recherchent une méthode efficace pour simplifier leurs processus de sauvegarde. Il peut être intéressant de penser la préservation des données au cœur même des logiciels ou avec les services Cloud.

Mesures :

- Possibilité de revenir à une situation antérieure, si erreur lors d'une procédure lourde telle que la préparation du budget.

- « Scheduler » : messages de recommandations au cœur des logiciels lors d'opérations particulières (ex. avant de commencer le budget, « nous vous conseillons de faire un archivage »).

Sécurité des données

Un exemple : 19.000 attaques de sites web suite aux attentats de Charlie Hebdo, y compris ceux des collectivités locales. Les collectivités et les entreprises ont souvent peu conscience des enjeux liés à la sécurité des données. Mais la sécurité est un travail d'équipe et il faut que les prestataires de Cloud ou de logiciels et leurs clients travaillent main dans la main pour proposer une sécurité optimum. Ce n'est pas au fournisseur de gérer la sécurité de son client, car ce dernier en est en fait le seul maître. Le fournisseur de Cloud met à disposition des outils permettant la mise œuvre d'une politique de sécurité, mais c'est au client de les utiliser à bon escient et de prendre conscience de la dangerosité de mettre à disposition des données informatiques, y compris en interne. 60% des piratages trouvent leur source en interne.

Mesures :

- Mettre en place des droits d'accès aux données restreints, gérer finement les profils d'utilisateurs.

- Mettre en place une charte informatique pour éduquer en interne et informer sur ce qu'il est possible de faire ou non

- Ne pas hésiter à prendre conseil auprès de son prestataire informatique.

Usages de l'informatique

Les risques viennent souvent d'une méconnaissance de l'informatique et du web. Il faut être vigilant et ne pas « sortir » n'importe quelles données de la collectivité ou de l'entreprise. Attention également à ne pas télécharger n'importe quoi.

Bien souvent, les entreprises et les communes ne savent pas si leurs sauvegardes sont bonnes. Elles sont formées par leur prestataire, mais elles ne se soucient pas vraiment, ne vérifient pas. Il n'y a pas de test de restauration, ce qui engendre parfois de mauvaises surprises …

Mesures :

- Formation, « éducation », aider à faire prendre conscience.

- Rappeler que les données ne doivent pas être sauvegardées que sur le poste mais aussi et surtout sur le serveur.

Importance de l'information/formation

Avant de sécuriser les réseaux, il faut éduquer les utilisateurs, mais aussi les cadres sur les enjeux, risques et bonnes pratiques.

Par exemple, méconnaissance de la différence entre un virus et un malware. Un virus s'installe à votre insu sur votre machine et vient corrompre un programme existant. En revanche, un malware est interprété par le système comme un programme installé par l'utilisateur : en cliquant sur une PJ, en installant un petit programme, etc. Ainsi les antivirus sont inutiles face à cette menace ! Seule la vigilance de l'utilisateur peut le protéger :

Mesures :

- Etre vigilant sur l'ouverture de PJ quand on ne sait pas de qui vient l'email

- Se méfier des emails étrangers

- Ne pas aller sur n'importe quel site et installer n'importe quel programme

- Ne pas hésiter à se tourner vers son prestataire informatique en cas de question.

Yann Duverdier, Directeur Business Development chez JVS-Mairistem.

Document n° 7 : Cadre stratégique commun du Système d'Information de l'Etat Synthèse-Février 2013

-1.OBJET ET DESTINATAIRES

Le cadre stratégique est un document d'orientation fixant les objectifs de transformation du système d'information de l'Etat sous forme de cibles à atteindre et de dispositifs à mettre en œuvre à l'échéance de 5 ans, en partant des principaux enjeux de l'Etat. Elaboré sous le pilotage de la DISIC en y associant les responsables des systèmes d'information des ministères, il s'adresse principalement aux décideurs des ministères concernés par les systèmes d'information (secrétaires généraux, directeurs métiers, responsables des systèmes d'information), pour orienter la stratégie d'évolution des systèmes d'information ministériels
et interministériels, pour préciser la gouvernance des SI de l'Etat et pour définir des modalités opérationnelles de mise en œuvre de la stratégie.

2. « D'OU PART-ON?»LE SYSTEME D'INFORMATION EXISTANT:DES LIMITES ET DES ATOUTS

Les systèmes d'information sont omniprésents dans la sphère

publique, les fonctions les plus régaliennes de l'Etat (défense, diplomatie, sécurité intérieure, ...) dépendent de façon cruciale des moyens de communication et de partage de l'information. La performance globale de l'administration est intimement liée à la qualité et à l'efficience de son système d'information. De nombreuses initiatives de l'administration ont permis d'atteindre cet état de développement des usages.
Mais la capacité d'évolution du système d'information est fortement contrainte par plusieurs facteurs:
•Dans un contexte de restriction budgétaire croissante, la capacité d'investissement est obérée par des coûts récurrents qui représentent la grande majorité des dépenses et des ressources humaines dans le domaine des systèmes d'information. La valeur ajoutée par le système d'information n'est pas perçue.
•L'évolution des compétences des agents de l'administration, indispensable dans un domaine en mouvement permanent, est limitée par un morcellement des modalités de gestion, basées en partie sur des dispositifs réglementaires obsolètes. L'attractivité des postes est réduite, les leviers de motivation sont insuffisants, et une concurrence se développe avec le secteur privé sur certains profils rares.
•Les fondements du système d'information (les infrastructures
et les systèmes internes à l'administration) n'ont pas évolué au même rythme que son interface avec l'usager dans le cadre du développement de l'administration électronique. Les projets de simplification se heurtent à des conceptions très cloisonnées (dès la définition juridique des concepts) qui rendent impossible ou très complexe l'automatisation des échanges de données.

•La fonction SI dans les ministères n'est pas encore suffisamment en prise avec les enjeux stratégiques: positionnée comme un centre de coût, concentrée sur des activités de production ou de développement, elle n'est pas utilisée comme un levier de transformation.
•La faible agilité des organisations et des systèmes d'informations, l'absence de cadre technique et financier pour la mise en commun de solutions informatiques, conduit le système d'information à freiner les réformes d'organisation, ou à recréer des structures autonomes réalisant des choix insuffisamment coordonnés pour répondre à des besoins similaires.
Ses atouts sont nombreux et constituent un point d'appui indispensable pour les travaux à venir:
•Les systèmes d'informations des administrations, bien qu'en partie sous
-traités, restent sous maîtrise des équipes internes, ce qui permet de disposer de nombreuses compétences indispensables, et de ne pas dépendre de contrats de long terme difficiles à faire évoluer;
•Les retours d'expérience sont nombreux sur de premières actions de transformation, aussi bien dans le développement de l'administration électronique, que la mise en place d'infrastructures communes, d'applications transverses et de solutions interministérielles sur le territoire;
•La prise de conscience à l'échelle interministérielle du caractère stratégique du SI progresse: les actions conduites par la D
ISIC depuis 2011 et l'engagement des ministères auprès d'elle en
témoignent; la gouvernance des systèmes d'information a progressé dans les ministères.

3. «POURQUOI?»-SE TRANSFORMER EST UNE NECESSITE

Continuer à faire évoluer les systèmes d'information est nécessaire pour ré pondre aux enjeux publics de demain: il s'agit d'un outil de production de l'administration, qui doit délivrer des services plus performants aux usagers, faciliter et accompagner les réformes de l'Etat, rendre possible les politiques publiques transverses à plusieurs administrations, s'intégrer dans une dimension européenne.
C'est d'autant plus nécessaire qu'il n'y a pas d'alternative: les technologies évoluent, sont adoptées par les agents et les usagers de l'administration, et finissent par s'imposer. Ce sont des leviers sur lesquels l'Etat peut s'appuyer pour conduire sa transformation, à condition de développer la confiance dans les outils numériques, d'assurer l'évolution nécessaire des compétences, de mettre en place les mesures d'accompagnement adaptées.
Enfin, transformer le système d'information répond à l'impératif de maîtrise des dépenses publiques, dans une logique double:
•il faut optimiser les coûts de fonctionnement du système d'information, à chaque fois que possible, notamment en s'appuyant sur des comparaisons à l'état de l'art,
•il faut savoir investir dans le système d'information à chaque fois qu'il crée une valeur pertinente et qu'il permet de réduire d'autres dépenses.

Pour entrer dans l'ère de l'«Etat numérique»,
la transformation doit être piloté e au plus haut niveau, afin de faire prendre en compte les enjeux stratégiques liés au numérique pour l'Etat, afin d'organiser la fonction SI pour anticiper et accompagner les réformes, afin de sélectionner les investissements les plus stratégiques et les mettre en commun, afin de mettre en place une gestion des ressources humaines adaptée au besoin de l'administration dans le domaine des systèmes d'information, afin d' «urbaniser» le système d'information pour faciliter l'interopérabilité, le partage des ressources et la valorisation des données.

4. «VERS OU?»-UNE CIBLE AMBITIEUSE ET REALISTE A 5ANS

Trois principaux axes de transformation, regroupant les objectifs, les moyens à mettre en œuvre ou les cibles à atteindre, orientent les transformations ministérielles et interministérielles:

•Le SI crée une valeur croissante pour ses utilisateurs; en particulier, il s'agit:
-d'analyser et d'optimiser les processus métier en s'appuyant sur les opportunités de développement du SI, en impliquant les utilisateurs, en supprimant les ruptures de chaînes dématérialisées, pour améliorer le service rendu tout en réduisant les coûts de fonctionnement;
-de valoriser, en interne comme en externe, le patrimoine de données de l'Etat, avec la mise en place d'une gouvernance des données;
-de simplifier et renforcer l'interaction «multicanal» entre l'Etat et les usagers du service public.

•Le SI de l'Etat est construit de façon efficiente; en particulier, il s'agit:
-d'organiser la mise en cohérence, voire la mise en commun, des services transverses (infrastructures, mais également les services applicatifs courants: messagerie, collaboratif, accès distant au SI, logistique, ...) en s'appuyant sur une urbanisation du système d'information de l'Etat;
-de converger vers un réseau interministériel de l'Etat, exploité par une structure interministérielle;
-de moderniser et rationaliser les infrastructures de production informatique (consolidation, virtualisation, industrialisation des processus, orientation service) et d'expérimenter le «cloud computing»;
-de faire converger les cadres d'architecture et renforcer les règles d'interopérabilité.

•La fonction SI de l'Etat est pilotée et alignée sur les enjeux de politiques publiques; en particulier, il s'agit:
-D'articuler la planification stratégique des évolutions du système d'information avec la programmation budgétaire;
-De définir des pratiques de gestion des ressources humaines cohérentes à l'échelle interministérielle, inscrites dans une perspective de 5 à 10 ans des besoins;
-De progresser dans la maîtrise des risques (sécurité des systèmes, pilotage des grands projets);
-D'optimiser la relation avec les fournisseurs;
-De prendre en compte les enjeux d'exemplarité (accessibilité, Environnement).

Le renforcement des mesures prises en matière de protection des systèmes d'information et de communication de l'Etat, dans toutes les dimensions de la cyber sécurité, est indispensable; il fait l'objet, sous pilotage de l'ANSSI,de travaux spécifiques, complémentaires du présent cadre stratégique, destinés à définir la politique de sécurité des systèmes d'information de l'Etat (PSSIE).

5. «COMMENT?»-UNE GOUVERNANCE, DES NORMES ET DES PROJETS FEDERATEURS

La mise en œuvre de cette transformation doit s'appuyer sur une organisation et une gouvernance adaptées.
La direction interministérielle des systèmes d'information et de communication (DISIC), «DSI de l'Etat», en est le pivot. Elle anime la planification stratégique à l'échelle interministérielle pour identifier les
investissements pertinents créateurs de valeur, sources d'économies dans le fonctionnement de l'administration, ou nécessaires à l'optimisation des coûts de fonctionnement du SI. Elle pilote la modernisation de la gestion des ressources humaines SIC, ainsi que les travaux d'urbanisation et de standardisation, renforce la gestion financière dans le domaine SI, organise la maîtrise des risques des

projets majeurs, renforce la stratégie achat avec le service des achats de l'Etat (SAE), et pilote les projets majeurs de mutualisation. La DISIC s'appuie sur le réseau des DSI ministériels dont le positionnement stratégique est encore à renforcer.
La transformation s'appuie sur des instances stratégiques (conseil des SIC) associant les secrétaires généraux et des instances exécutives (comité technique des SIC) associant les DSI. La transformation concerne également les opérateurs de l'Etat: le volet «SI» sera intégré par les ministères dans l'exercice de la tutelle sur leurs opérateurs.
La transformation des SI de chaque ministère est coordonnée et appuyée par le SGMAP, dans le cadre du suivi des plans ministériels de modernisation et de simplification. Elle est outillée par des «contrats de progrès» ministériels, permettant à la DISIC et aux DSI ministériels d'adresser l'ensemble des objectifs du présent cadre stratégique avec des actions concrètes et des engagements réciproques.

CONCOURS INTERNE OUVERT LES 20 ET 21 AOUT 2015 POUR LE RECRUTEMENT D'UN CADRE SPECIALISTE TECHNIQUE DU CADRE DES POSTES ET TELECOMMUNICATIONS DE LA NOUVELLE-CALEDONIE

---------⏮⏭--------

EPREUVE ECRITE D'ADMISSIBILITE : NOTE DE SYNTHESE

DUREE : 4 HEURES

COEF : 4

SUJET

Ce dossier comporte 32 pages y compris la page de garde.

note de synthèse à partir d'un dossier « Objets connectés »

I –Objet de l'épreuve – liste des documents

Vous êtes cadre spécialiste technique et sollicité par le comité exécutif pour la rédaction d'une note de synthèse à son attention sur l'évolution récente en matière d'objets connectés et d'internet des objets.

Dossier fourni

N° Doc.	Intitulé du document	nbre pages
[1]	La solution se trouve en partie dans le problème, Alain Louchez et Valerie Thomas, ITU News n°1 2014	4
[2]	Internet des objets, big data et 5G ! Des opportunités majeures pour l'Europe - Roberto Viola, Les cahiers de l'ARCEP, oct. 2014	2
[3]	Quel avenir pour la carte SIM ? La carte SIM : un concentré de technologie de plus en plus performant, Olivier Pitou , Les cahiers de l'ARCEP, oct. 2014	2
[4]	Les télécoms et les grandes ruptures technologiques, MN Jego-Laveissière, P. Louette Les cahiers de l'ARCEP, oct. 2014	1
[5]	Les prévisions des principaux analystes du secteur, ITU News n°1 2015	3
[6]	Les usages de l'internet augmentent, la vigilance des internautes aussi ! Baromètre 2015 ACSEL-CDC	1
[7]	Objets connectés : Orange acquiert la start-up Ocean, FABIENNE SCHMITT - LES ECHOS | LE 16/04/2015	1
[8]	Qualcomm prêt pour la bataille de l'Internet des objets, Romain Gueugneau, Les Echos, 18/05/2015	2
[9]	Et si la voiture connectée saturait les réseaux mobiles ? B.Solivellas, www.cnetfrance.fr, 25/05/2015	1
[10]	Interview Delphine Asseraf – Allianz : « Un assureur est légitime à tirer de la valeur des objets connectés », X.Biseul, www.itespresso, 1 juin 2015	2
[11]	Les constructeurs auto font monter Apple et Google à bord, M. Amiot, Les Echos, 3/06/2015	2
[12]	Toshiba et Microsoft s'allient dans l'Internet des objets, R. Loukil, www.usine-digitale.fr, 5 juin 2015	1
[13]	Sigfox, LoRa, Qowisio : la bataille pour les réseaux bas débit est lancée, P. Manière, www.latribune.fr, 09/06/2015	3
[14]	L'ÉLECTRONIQUE SE MOBILISE POUR RÉPONDRE AUX ENJEUX DE L'INTERNET DES OBJETS, J.Marouani, www.electroniques.biz, 25 juin 2015	2
[15]	L'IdO aide les industriels à explorer le futur, fr.plc.com, juillet 2015	2
[16]	Internet des objets: la bataille des futurs standards de communication est engagée, S.Meunier, www.france24.com, 17 juillet 2014	2

II – Rappels et règles à suivre

Il vous incombe de vérifier le dossier fourni vis-à-vis de la liste détaillée ci-dessus.

Il vous est rappelé que vous ne devez en aucun cas faire appel à des éléments externes aux documents fournis, y compris pour la conclusion.

Les renvois aux documents seront précisés en employant la numérotation fixée au tableau ci-dessus.

Votre note devra comporter entre 4 et 6 pages manuscrites et se terminer par une conclusion.

ITU NEWS N° 1 2014 > Les déchets électroniques et l'Internet des objets

La solution se trouve en partie dans le problème

Par Alain Louchez et Valerie Thomas

https://itunews.itu.int/Fr/4866-La-solution-se-trouve-en-partie-dans-le-probleme.note.aspx

L'Internet des objets (IoT) était à l'honneur cette année au CES, le Salon international de l'électronique grand public organisé par la Consumer Electronics Association, à Las Vegas, aux États-Unis, du 7 au 10 janvier 2014. En substance, on entend par Internet des objets l'intégration de n'importe quel objet, quelle que soit sa taille ou sa nature, dans l'espace de communication.

Grâce à la convergence de nombreuses technologies qui tombe à point nommé, il est aujourd'hui possible de se connecter à n'importe quel objet ou de communiquer avec lui au moyen d'une interface, partout et à tout moment. Cette évolution fait le bonheur des développeurs d'applications. Mais étant donné la place croissante qu'occupe l'électronique dans le tissu économique et dans les habitudes de la société, la gestion de ces appareils au-delà de leur durée de vie utile va devenir nécessaire, à la fois pour protéger l'environnement et pour assurer la durabilité de notre approvisionnement en matériaux.

L'Internet des objets, source de déchets électroniques

Dans son rapport intitulé «Stratégie nationale pour une gestion responsable dans le domaine de l'électronique», le Groupe spécial interorganisation américain pour une gestion responsable dans le domaine de l'électronique (Interagency Task Force on Electronics Stewardship) reconnaît que *«ces technologies sont devenues indispensables à notre mode de vie et à la croissance de notre économie». Il alerte toutefois sur le fait que «le développement de ces technologies posent de plus en plus la question de la protection de la santé humaine et de l'environnement contre les effets néfastes d'une prise en charge et d'une élimination inappropriées de ces produits.»*

Mercy Wanjau, juriste principale au sein de la Commission des communications du Kenya, a déjà fait observer en 2011 (voir les Nouvelles de l'UIT, N° 9, 2011) que «les déchets électroniques [étaient] aujourd'hui l'un des flux de déchets à plus forte croissance». Aujourd'hui, d'après les estimations de l'Université des Nations Unies relayées par l'UIT, 67 millions de tonnes d'équipements électriques et électroniques ont été mis sur le marché en 2013. La même année, 53 millions de tonnes de déchets électroniques (déchets d'équipements électriques et électroniques) ont été éliminés dans le monde. Avec l'explosion de l'Internet des objets, la production de déchets électroniques va inévitablement s'accélérer.

En conséquence, une attention particulière est accordée aux déchets électroniques non seulement au niveau national (par exemple, le Congrès américain a adopté le 24 juillet 2013 un texte sur les déchets électroniques toxiques, à savoir la loi sur le recyclage responsable des équipements électroniques), mais également au niveau international. Par exemple, l'UIT travaille en collaboration avec le Secrétariat de la Convention de Bâle sur le contrôle des mouvements transfrontières des déchets électroniques dangereux et sur l'élimination de ces déchets. L'Union travaille également avec l'Université des Nations Unies, en coopération avec l'Initiative StEP (Solving the E-waste Problem, «Initiative pour la résolution du problème des déchets électroniques») et le Centre pour l'environnement et le développement pour la région arabe et l'Europe (CEDARE), à sensibiliser aux dangers que représentent ces déchets et à promouvoir l'intégration de la gestion

des déchets électroniques dans les politiques nationales relatives aux technologies de l'information et de la communication (TIC).

L'UIT tient une page web de référence complète sur les déchets électroniques et a publié un Kit pratique sur la gestion des équipements TIC en fin de vie. Ce Kit a été élaboré en partenariat avec plus de 50 acteurs — sociétés travaillant dans le domaine des TIC et organisations de protection de l'environnement – et a été à l'origine de l'élaboration de nouvelles normes techniques, telles que la Recommandation UIT–T L.1000 «Solution universelle d'adaptateur de puissance et de chargeur pour les terminaux mobiles et les autres dispositifs TIC portatifs». Cette norme définit les spécifications techniques pour un chargeur universel compatible avec un grand nombre de dispositifs électroniques grand public, qui permet de réduire les déchets et améliore le côté pratique pour les utilisateurs. Lorsque cette norme sera pleinement mise en œuvre dans le monde entier, elle permettra d'éviter quelque 82 000 tonnes de chargeurs redondants et d'éviter au moins 13,6 millions de tonnes d'émission de CO_2 par an.

Si les gouvernements suivent de près les incidences de l'IoT sur la société, notamment sur la sécurité et la confidentialité des données, ses conséquences sur la durabilité de l'environnement ne semblent pas traitées avec le même degré d'urgence.

Les équipements électroniques utilisés tout au long de la chaîne de valeur de l'IoT finiront en déchets. Un article rédigé par Elizabeth Chamberlain et Kyle Wiens de la communauté iFixit, publié le 9 janvier 2014 sur le site Internet TreeHugger, commente une étude récente menée par Huabo Duan et ses collègues de l'Institut de technologie du Massachusetts intitulée «Caractérisation quantitative des flux internes et transfrontières de déchets électroniques — Analyse de la génération, de la collecte et de l'exportation aux États-Unis («Quantitative characterization of domestic and transboundary flows of used electronics —Analysis of generation, collection, and export in the United States»), publiée le 15 décembre 2013. Les auteurs de cet article craignent que l'essor des éléments informatisés de base de l'IoT ne constitue un facteur de plus entravant les efforts déployés pour tenter de gagner la bataille contre les déchets électroniques, puisque *«à mesure que vont se multiplier les objets informatisés — réfrigérateurs, jouets, équipements électroménagers, et accessoires par exemple — des formes de déchets électroniques moins évidentes vont faire leur apparition sur le marché. En effet, s'il est facile de faire le lien entre un écran cathodique géant et les déchets électroniques, la relation ne saute pas aux yeux pour les cartes d'anniversaire musicale. Personne ne se pose de questions avant de les jeter et pourtant elle font partie des déchets électroniques.»*

La fabrication d'équipements IoT respectueux de l'environnement devrait devenir la principale priorité. Des chercheurs de l'Université Catholique de Louvain, en Belgique (juin 2013), ont clairement expliqué l'urgence de ce constat: *«La conception que l'on a de l'Internet des objets (IoT) exige le déploiement de billions de nœuds capteurs sans fil (WSN, wireless sensor nodes) dans notre environnement. Le déploiement d'un si grand nombre de systèmes électroniques ne pourra être durable que si l'on adopte une approche fondée sur la conception écologique. Cette approche demande de réduire au maximum 1) l'énergie grise et l'empreinte carbone de la production de WSN, 2) l'écotoxicité des déchets de WSN, et 3) le trafic Internet associé à la génération de données.»*

La gestion de l'environnement grâce à l'Internet des objets

Les technologies de l'Internet des objets, telles que les communications de machine à machine (M2M) sont déjà utilisées pour améliorer la protection de l'environnement, par exemple pour la collecte des ordures, le

recyclage des huiles, le recyclage des ampoules, la réduction des émissions de CO_2, le contrôle de la pollution auditive, la gestion du gaspillage de l'eau, et même le retrait de la graisse de cuisine dans les restaurants.
Lors d'un Atelier sur l'IoT organisé à Pékin, en Chine, en août 2013, Li Haihua, Ingénieur principal à l'Académie chinoise de recherches dans le domaine des télécommunications relevant du Ministère de l'industrie et des technologies de l'information, et Directeur adjoint du Département de l'Internet des objets et des Services et Ressources, a indiqué qu'en Chine «l'Internet des objets est utilisé pour la surveillance automatique de plus de 15 000 sources de pollution majeures».
Dans un article intitulé «Intégrer les technologies de l'Internet des objets dans la gestion de l'environnement en Afrique du Sud», présenté en avril 2012 à la 2e Conférence internationale sur les sciences de l'environnement et le génie, Nomusa Dlodlo, chercheur principal au Conseil pour la recherche scientifique et industrielle à l'Institut Meraka de Pretoria, met en évidence la corrélation entre l'IoT et la gestion de l'environnement dans de nombreux domaines.

L'Internet des objets et la gestion des déchets électroniques

Puisque la mise au rebut des composants électroniques utilisés dans les objets reliés à l'IoT constituent une source importante de déchets électroniques, les fabricants d'équipements IoT doivent de plus en plus tenir compte des dangers liés à l'utilisation de matériaux dangereux pour produire les dispositifs en question. Les produits devraient être conçus et fabriqués de manière à minimiser leur impact sur l'environnement pendant leur cycle de vie. Les problèmes environnementaux devraient également faire partie intégrante du processus de fabrication intelligente qui a une relation symbiotique avec l'Internet des objets. Par exemple, le Georgia Tech Manufacturing Institute, qui entretient des liens étroits avec le Partenariat pour des technologies de fabrication avancées des États-Unis (United States Advanced Manufacturing Partnership), considère que l'environnement doit être la préoccupation centrale de la production industrielle moderne.
Le suivi des déchets électroniques présente des avantages. En 2011, le projet BackTalk mis au point par le Senseable City Lab de l'Institut de technologie du Massachusetts a apporté des explications sur les «chemins sinueux empruntés par les déchets électroniques», en pointant des pertes d'efficience économique flagrantes. La mise en place d'un meilleur suivi à distance améliorerait la précision des données sur les déchets électroniques; par exemple, l'Agence de protection de l'environnement des États-Unis *«a reconnu qu'il était nécessaire d'adopter une approche scientifique pour obtenir de meilleures informations sur les flux de déchets électroniques qui partent des États-Unis.»*
Actuellement les activités visant à définir des normes, des protocoles et des spécifications dans l'espace IoT sont axées sur l'interopérabilité, parce qu'il n'existe pas de langue commune entre les machines et les objets sur un grand nombre de marchés. Aucune considération particulière n'a encore été donnée pour intégrer la composante environnementale dans les normes relatives à l'IoT.

Et maintenant?

Si les objets reliés à l'IoT étaient dotés non seulement d'un moyen permettant leur localisation grâce au système mondial de positionnement de suivi (GPS) mais également d'une sorte d'identification électronique universelle, le recyclage, la réutilisation et la gestion de la fin de vie des équipements seraient grandement facilités. Ce suivi pourrait aider à régler le problème des coûts de collecte et de recyclage, et offrir de nouvelles opportunités au secteur privé, comme la récupération des métaux rares. Il favoriserait également la mise en œuvre de réglementations limitant l'utilisation de certaines substances dangereuses. Des systèmes

d'identification tels que le Code de produit universel (UPC) et le Numéro international normalisé des livres (ISBN) sont largement utilisés; un système analogue pourrait certainement être mis en place pour les dispositifs électroniques.

Certains outils sont déjà disponibles. Un outil d'aide à l'achat axé sur l'environnement appelé EPEAT aide les acheteurs à trouver, comparer et choisir les produits les plus respectueux de l'environnement et fournit aux fabricants des critères environnements pour la conception et l'élaboration des produits. En outre, l'e Stewards Initiative a créé une certification pour les recycleurs électroniques qui intègre les exigences de la norme ISO 14001 sur le management environnemental. Elle propose également un grand nombre de services d'appui pour une utilisation et une gestion efficaces des équipements électroniques.

Le déploiement à grande échelle des technologies IoT est imminent. Les possibilités attrayantes qu'ouvrent ces technologies masquent des conséquences non désirées, y compris le problème des déchets électroniques. Les décideurs doivent se préoccuper de la composante environnementale. Il faut agir maintenant.

À propos des auteurs

Alain Louchez est Directeur général du Centre pour le développement et l'application des technologies de l'Internet des objets (CDAIT) au Georgia Institute of Technology.

Valerie Thomas est professeur associée à l'Anderson Interface Chair in Natural Systems à la H. Milton Stewart School of Industrial and Systems Engineering, et occupe également un poste à la School of Public Policy au sein du Georgia Institute of Technology.

"L'Internet des objets – Grandes tendances et enjeux de la normalisation", tel était le thème d'un atelier organisé par l'UIT en février 2014. On trouvera des renseignements plus détaillés à l'adresse suivante: http://www.itu.int/en/ITU-T/Workshops-and-Seminars/iot/201402/Pages/default.aspx.

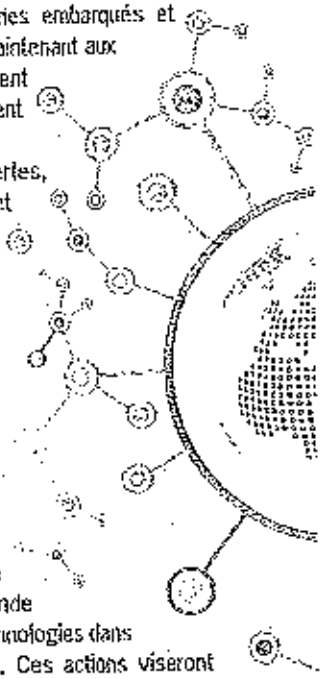
Internet des objets, big data et 5G :

Par Roberto VIOLA, directeur général adjoint de la DG Connect au sein de la Commission européenne

Quelles technologies clés pour favoriser l'innovation et la croissance en Europe ? Dans le secteur des télécommunications, l'internet des objets, le big data et la 5G devraient être les facteurs déclencheurs de profonds changements. Ils représentent des opportunités majeures et nous possédons en Europe de réels atouts pour être à la pointe dans ces domaines. La Commission européenne est pleinement engagée dans cette réflexion qui peut stimuler le développement de ces secteurs d'avenir.

Internet des objets : l'Europe à la pointe

L'internet des objets recouvre la connexion des objets à l'internet au moyen de capteurs pour récupérer et exploiter des données du monde physique. L'évolution constante des technologies de l'internet couplée à la baisse continue des coûts de l'électronique permettent aujourd'hui d'envisager le déploiement de tels systèmes à grande échelle. L'internet des objets est donc pressenti comme la prochaine révolution de l'internet.



Le big data, cet énorme patrimoine d'information, encore largement inexploité, est comparable à une nouvelle source d'énergie renouvelable à disposition de la société du XXIème siècle.

De nombreux bénéfices économiques et sociétaux sont attendus. Dans la santé, l'avènement de capteurs biométriques connectés permet de repenser le suivi médical des patients et leur traitement "en continu". L'optimisation en temps réel des transports publics, l'émergence de services autour des données de consommation d'énergie ou environnementales sont d'autres exemples typiques. De multiples nouveaux services peuvent donc être envisagés, notamment pour les villes intelligentes.

Le nombre d'objets connectés d'ici 2020 est estimé entre 20 et 50 milliards. Le déploiement d'objets intelligents dans les différents secteurs de l'économie pourrait avoir un impact entre 2 et 5 trillions d'euros par an sur l'économie mondiale [1]. Pour les fournisseurs de technologies (logiciel embarqué, capteurs, services de communication et d'information), l'impact est estimé à 309 milliards d'euros en 2020 [2]. Le développement d'écosystèmes autour des objets connectés devient donc un enjeu économique majeur, suscitant de nombreuses initiatives industrielles.

Eu égard aux nombreuses annonces sur les objets connectés en provenance des Etats-Unis (Apple, Google, Cisco) ou d'Asie (Samsung, Huawei), il est légitime de se demander si l'Europe ne va pas rater le tournant du web 3.0, comme cela fût le cas lors de l'arrivée des smartphones. Il serait toutefois erroné de penser que les jeux sont faits. Les chaînes de valeurs de l'internet des objets sont beaucoup plus complexes que celles construites autour des smartphones, et le nombre d'acteurs concernés beaucoup plus important. L'Europe possède des sociétés de pointe dans tous les secteurs de la chaîne de valeur de l'internet des objets, sur lesquelles elle peut s'appuyer pour catalyser le déploiement de ces systèmes intelligents.

L'Europe a déjà investi plus de 100 millions d'euros en R&D dans les systèmes et plateformes pour objets connectés. Elle est déjà en première ligne pour les systèmes embarqués et les capteurs. La Commission s'attelle maintenant aux barrières qui s'opposent au déploiement massif du marché [3]. En ce sens, il convient de prendre en compte :

- la disponibilité de plates-formes ouvertes, vecteurs du développement de l'internet des objets, permettant le déploiement d'applications interopérables ;
- le besoin dérivé de standards ouverts ;
- la sécurité de bout en bout ;
- le niveau de protection et de confidentialité, pour garantir le respect de la vie privée et permettre la confiance des citoyens dans ces nouvelles applications.

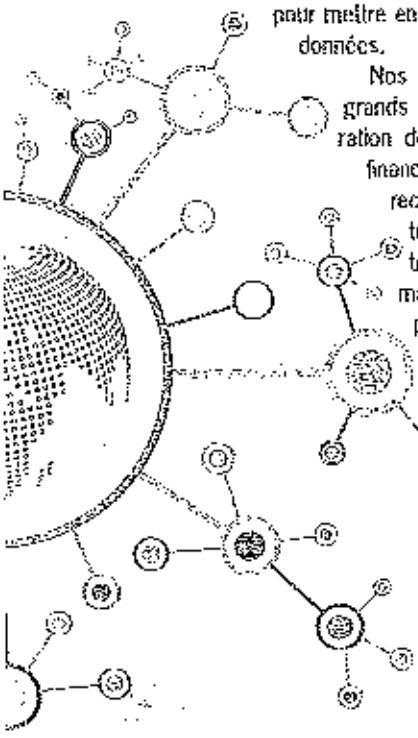
La Commission européenne propose de soutenir le déploiement de pilotes à grande échelle, afin de valider les technologies dans un nombre de secteurs clés. Ces actions viseront à faciliter l'émergence d'écosystèmes autour de l'internet des objets. C'est une extraordinaire opportunité de croissance pour la France et l'Europe.

Big data : un énorme patrimoine encore inexploité

Il est difficile de ne pas être fasciné par le thème du big data (données massives). A l'heure actuelle, le monde produit 1,7 million de milliards d'octets de données par minute (l'équivalent de 360 000 DVD), soit plus de 6 mégaoctets de données par personne chaque jour. Cet énorme patrimoine d'information, encore largement inexploité, est comparable à une nouvelle source d'énergie renouvelable à disposition de la société du XXIème siècle : pour améliorer notre capacité à anticiper des événements futurs en utilisant les masses de données des faits du présent ; pour fournir des outils qui nous guident dans notre vie quotidienne ; pour améliorer la qualité de nos décisions stratégiques tant sur le plan politique que dans le secteur industriel ; pour permettre une production de qualité fondée sur une meilleure compréhension des processus de production et des besoins ou souhaits des consommateurs.

Au-delà des aspects d'amélioration et de gains d'efficacité, certains avancent même que le big data transformera notre façon de produire, de faire de la recherche et même de penser. Au lieu d'essayer d'établir de simples liens de cause à effet – l'action X produit l'effet Y – le big data permettra l'identification de corrélations par le biais de calculs de probabilités.

des opportunités majeures pour l'Europe



Encouragée par la France à se saisir de ce sujet majeur, la Commission européenne a fait du *big data* une des ses priorités. Notre ambition vise à transformer l'économie européenne pour que ses fondements reposent sur l'exploitation des masses de données, pour mettre en œuvre une véritable économie des données.

Nos actions se regroupent selon deux grands axes : soutien financier et amélioration des conditions-cadre. Notre soutien financier vise à cofinancer les projets de recherche et d'innovation d'infrastructures importantes permettant le traitement et l'échange de données massives (à travers le réseau européen GÉANT, par exemple) et de créer des espaces clos permettant l'expérimentation. Il est également prévu de mettre en place un partenariat public-privé « données massives » pour financer des idées plus avancées dans des domaines comme la médecine personnalisée ou la logistique alimentaire, ainsi que l'établissement d'une grande coalition en faveur des emplois numériques et le lancement de l'initiative « *Ouvrir au monde extérieur les systèmes d'éducation* » afin de remédier aux inadéquations de compétences.

> Le déploiement d'objets intelligents dans les différents secteurs de l'économie pourrait avoir un impact compris entre 2 000 et 5 000 milliards d'euros par an sur l'économie mondiale.

5G : des initiatives importantes, face aux Etats-Unis et à l'Asie

Sur les dix-huit derniers mois, les travaux relatifs à la 5G ont connu un essor considérable. La Commission a pleinement anticipé ce mouvement en lançant une série de projets 5G exploratoires[14] dès 2012, puis en signant fin 2013 le partenariat public-privé 5G avec l'association industrielle représentant les acteurs de la recherche européenne[15], doté d'une enveloppe budgétaire de 700 millions d'euros dans le cadre du programme communautaire Horizon 2020. Neelie Kroes a aussi encouragé les industriels à travailler ensemble pour aboutir à une définition globale de la 5G d'ici la fin 2015[16].

Des initiatives 5G importantes ont aussi été lancées en Corée du Sud, au Japon, en Chine et aux Etats-Unis. Si la définition de la 5G n'est pas encore établie, les axes majeurs de recherche, et leur motivation, sont clairs :

- l'augmentation continue du trafic mobile, d'environ 80 % par an. D'ici 10 à 15 ans, le trafic global pourrait être multiplié par 1000. L'industrie travaille dans quatre directions pour permettre l'extension des capacités : la densification des réseaux avec des cellules plus petites ; l'utilisation de nouvelles bandes de fréquences (millimétriques), l'augmentation de l'efficacité spectrale avec de possible nouvelles formes d'onde, l'utilisation optimisée par délestage du trafic sur d'autres réseaux d'accès ;
- la possibilité de servir des débits proches de ceux des réseaux fixes, jusqu'à 1 Gb/s ;
- l'émergence de l'internet des objets dans des domaines industriels divers (énergie, transport, santé…). La 5G doit pouvoir servir tous les besoins de communication de secteurs professionnels divers. Pour les applications nécessitant des réponses instantanées aux évènements, des temps de latence de l'ordre de la milliseconde seront nécessaires, ce qui n'est pas disponible aujourd'hui ;
- la possibilité de mettre en œuvre des fonctions réseaux sous forme logicielle. En virtualisant ces fonctions, le réseau devient un « nuage » (*cloud*), ce qui permet aussi leur partage entre fournisseurs de services. De nombreux bénéfices sont attendus de cette transformation, notamment en termes de coûts de gestion de réseaux et de gains d'énergie.

Les bandes au-dessus de 3,4 GHz sont sous utilisées à ce jour, mais les scénarios de la 5G font apparaître que la densification des réseaux et l'émergence de services à très haut débit (télévision ultra haute définition 4K ou 8K) peuvent justifier l'usage de spectre au-delà de 6 GHz, avec des bandes continues de plusieurs centaines de MHz.

Le sujet de la 5G est prioritaire en Asie et sera débattu lors de la CMR[17] 2015, pour définir s'il est porté à l'ordre du jour de la CMR 2018. L'Europe doit rapidement développer une position commune sur ce sujet, acceptable par l'industrie satellitaire qui est potentiellement impactée par des réseaux mobiles terrestres dans les bandes millimétriques. Avec l'accélération des travaux sur la 5G, les sujets "spectre" et "normes" deviennent très importants dans un proche avenir. La Commission européenne est prête à jouer un rôle moteur et constructif dans ces domaines.

http://europa.eu/

[13] www.mckinsey.com/insights/business_technology/disruptive_technologies
[14] www.gartner.com/newsroom/id/2636073
[15] http://www.internet-of-things-research.eu/
[16] http://5g-ppp.eu/projects/
[17] http://5g-ppp.eu/
[18] Congrès Mondial des Mobiles 2014, Barcelone, http://europa.eu/rapid/press-release_SPEECH-14-155_en.htm
[19] Conférence Mondiale des Radiocommunications http://www.itu.int/en/ITU-R/conferences/wrc/2015/Pages/default.aspx

quel avenir pour la carte SIM ?

La carte SIM : **un concentré de technologie de plus en plus performant**

Par Olivier PIOU, directeur général Gemalto

Lorsque j'ai rejoint cette industrie, au début des années 1990, je n'imaginais pas à quel point ce petit micro processeur révolutionnerait nos vies au quotidien. En effet, si sa vocation première vise à authentifier un abonné sur un réseau cellulaire, pour lui permettre de téléphoner, d'envoyer des SMS ou de partager des photos, elle ouvre un panel d'opportunités bien plus large!

Si l'on s'intéresse aux usages mobiles déjà déployés à travers le monde, on s'aperçoit combien les applications que renferme ce concentré de technologie facilite la vie de nos semblables, voire la transforme. Au Kenya, par exemple, un service de transfert d'argent via le mobile est disponible : m-pesa. Grâce à n'importe quel mobile, il est possible de transférer et de recevoir de l'argent 24 h sur 24, 7 jours sur 7, sans besoin d'accéder à une connexion internet. Grâce à des identifiants sécurisés dans la SIM, l'opérateur offre à des personnes sans compte bancaire les mêmes services que ceux offerts par une banque.

La SIM devient multi-applicative et multi-clients

Les usages du mobile évoluent vers toujours plus de simplicité et de rapidité. L'arrivée de la technologie sans contact NFC et son déploiement aux États-Unis et en Asie sont la preuve de la mutation de l'industrie du mobile. Grâce à son portefeuille mobile, il est aujourd'hui possible de payer directement depuis son téléphone, d'activer ses coupons de réduction et de cumuler des points de fidélité dans son enseigne favorite aux États-Unis. De l'autre côté de la planète, les voyageurs hongkongais n'ont maintenant plus besoin de valider leur ticket de transport version papier, puisque leur titre ou abonnement est directement chargé dans leur téléphone. En approchant leur *smartphone* de la borne de transport, compatible avec la technologie sans contact, ils valident leur ticket, de façon complètement sécurisée.

Les investissements de Gemalto en recherche et développement ont permis à la carte SIM d'être de plus en plus performante. Connectée à des solutions logicielles déployées dans des centres informatiques spécialisés, elle est aujourd'hui capable d'héberger et de gérer des services et applications multiples, qui requièrent un fort niveau de sécurité. A l'instar d'un immeuble divisé en appartements où chaque locataire voudrait préserver son intimité, les cartes SIM modernes offrent à différentes industries l'opportunité d'héberger leurs services de façon cloisonnée, hermétique et totalement sécurisée. Ainsi, la SIM devient multi-applicative et multi-clients, permettant à une banque, un opérateur de transport, un organisme de santé, ou une université, d'offrir leurs applications au plus grand nombre d'abonnés. Elle se positionne donc *de facto* comme l'élément sécurisé de référence du portefeuille mobile.

Certifiée par les autorités bancaires, au même titre qu'une carte de crédit, la SIM peut capitaliser sur les infrastructures sans contact EMV sécurisées déjà déployées massivement dans la plupart des pays. Elle permet d'offrir une véritable interopérabilité grâce à la conjugaison de différents standards (ETSI, Global Platform, 3GPP, recommandations GSMA...) à même de garantir l'adoption par le plus grand nombre. Ainsi, l'ensemble des 800 opérateurs mobiles dénombrés dans le monde peuvent déployer des services de paiement ou de transport sur un nombre toujours croissant de mobiles, qu'ils soient chinois, européens, américains, taïwanais, coréens, avec des systèmes qui restent compatibles les uns avec les autres.

De nouveaux usages autour de l'internet des objets

Avec l'évolution du monde numérique, de nouveaux usages apparaissent autour de l'internet des objets, amenant la SIM à étendre son rôle au-delà du mobile. A se transformer dans sa taille, sa durabilité, ses fonctionnalités. Elle change de forme, soit être amovible mais également soudée à l'appareil, elle peut s'intégrer dans les voitures, les montres, les lunettes, les vêtements... En résumé, la SIM, ce concentré de logiciel dans une puce toujours indépendante du reste de l'appareil, dont les qualités fonctionnelles et sécuritaires sont aujourd'hui prouvées et éprouvées, évolue pour s'intégrer avec des objets de la vie courante. Elle permet aussi la création de nouvelles applications dans différents domaines tels que :

> La SIM, ce concentré de logiciel dans une puce toujours indépendante du reste de l'appareil, dont les qualités fonctionnelles et sécuritaires sont aujourd'hui prouvées et éprouvées, évolue pour s'intégrer avec des objets de la vie courante.

- l'automobile (avec l'appel d'urgence en cas d'accident – « e-call » – qui relie le véhicule endommagé à une centrale d'intervention),
- la santé (avec la « santé mobile », qui permet à un malade d'avoir un équipement à domicile relié automatiquement aux services hospitaliers via un réseau mobile, pour le suivi et une intervention médicale éventuelle en cas de signe alarmant)
- et plus largement les objets connectés qui vont étendre les possibilités de communication entre un réfrigérateur, un compteur d'eau ou d'électricité, une montre, etc... et une plateforme dans le *cloud* permettant de généraliser en toute sécurité les projets de « villes intelligentes » ou bien la prise en charge à distance d'un certain nombre de personnes isolées ou de malades chroniques.

Suite p. 49

[3]

Suite de la p. 45

OLIVIER PIOU

La protection des données personnelles : une priorité

La confidentialité des données est ainsi au cœur du débat : l'authentification de l'individu et la sécurisation de ses données personnelles sont exigées de toute part. Elles sont ici garanties par la SIM grâce à un système sophistiqué de technologies de cryptage et de connectivité vers des serveurs distants, qui ne permet qu'aux intéressés, prestataires de services et individus, d'accéder à ces informations.

Ainsi, que nous soyons parent, patient, élu, entrepreneur, consommateur..., je suis convaincu que la protection de nos données les plus sensibles, comme nos identifiants, nos comptes bancaires, photos, vidéos, reste une priorité. Nous sommes amenés à partager notre monde numérique avec nos communautés personnelles et professionnelles via le *cloud*, mais nous souhaitons toujours protéger notre intimité, nos secrets et contrôler qui peut y avoir accès. Connectivité et sécurité ne s'opposent pas. Elles sont complémentaires et coexistent. Et elles peuvent coexister pacifiquement à condition de disposer d'une plateforme multi applicative simple et sécurisée telle que la SIM.

La convergence des industries du mobile est en marche. La France est un acteur incontournable dans ce processus, engagée dans l'innovation, capable d'exporter ses savoir-faire et technologies, dont bon nombre de pays ont fait l'acquisition. C'est ensemble, opérateurs télécoms, institutions bancaires, fournisseurs de services, opérateurs de transport, industriels, organismes de régulation, que nous construirons le monde numérique de demain. Connecté. Libre. Et sécurisé.

www.gemalto.com/france

212

[4]

Les télécoms et les grandes ruptures technologiques

Par Marie-Noëlle JEGO-LAVEISSIERE, directrice exécutive innovation, marketing et technologies, et Pierre LOUETTE, directeur général adjoint, Orange

Le secteur et les marchés des télécoms sont coutumiers des ruptures technologiques, qui apportent des services innovants aux consommateurs et aux entreprises, tout en rebattant les cartes de la concurrence entre les acteurs. En leur temps, la télématique puis l'arrivée d'internet, de la téléphonie mobile, de l'ADSL sont venus créer des usages nouveaux, qui eux-mêmes ont engendré des opportunités nouvelles pour l'ensemble de l'économie.

Les grandes ruptures d'aujourd'hui viennent du monde du logiciel et de l'internet : le *cloud*, le *big data*, la virtualisation des infrastructures envahissent les télécoms et révolutionnent l'architecture des réseaux. L'internet des objets – montres, appareils photo, lunettes, voitures, etc. – pénètre notre quotidien et crée de nouveaux modes de connectivité et de médiation. Les interfaces de programmation (souvent désignée par le terme API pour *Application Programming Interface*), deviennent un moyen simple de lier applications et ressources réseau et *cloud*. Ces mutations rendent les réseaux plus flexibles, modulables et ouverts, avec pour conséquence un foisonnement de services innovants.

Opportunités économiques

Ces avancées, comme celles qui les ont précédées, sont naturellement sources d'opportunités économiques énormes. Pour les opérateurs télécoms, elles tendent également à accroître fortement le niveau de concurrence, en permettant l'entrée dans leur cœur de métier de nouveaux acteurs venus notamment du monde du logiciel ou de l'internet. C'est par exemple le cas pour les services de communication qui ont été bouleversés ces dernières années par des géants comme Skype, Whatsapp ou encore Wechat. Plus largement, c'est toute la chaîne de fourniture de l'accès réseau qui est potentiellement affectée.

Les avancées technologiques tendent à accroître fortement le niveau de concurrence, en permettant l'entrée, dans le cœur de métier des opérateurs, de nouveaux acteurs venus notamment du monde du logiciel ou de l'internet. Plus largement, c'est toute la chaîne de fourniture de l'accès réseau qui est potentiellement affectée.

Tout l'enjeu est d'être en mesure de développer les *business models* de demain, économiquement viables, à partir des innovations d'aujourd'hui. Les acteurs qui seront les mieux à même de prendre leur place dans les révolutions en cours sont ceux qui seront capables d'investir au bon moment dans les bonnes technologies et les bonnes compétences. Les grands gagnants seront aussi les entreprises capables de diffuser rapidement leurs innovations et d'y faire adhérer le marché, dans un monde où la taille critique, l'audience et la relation client seront plus que jamais des actifs essentiels.

Rôle de la régulation

Encore faut-il que les acteurs soient en mesure de le faire... Or, en ce qui concerne les opérateurs télécoms français, la destruction de valeur intervenue sur le marché depuis deux ans a laminé leurs marges. Les conséquences sur leur niveau d'investissement en sont désormais très visibles, notamment dans les observatoires publiés par l'Autorité. La régulation a aussi un rôle à jouer dans la capacité des acteurs à investir, en garantissant un traitement équitable à l'ensemble des services qui sont en concurrence. Cela nécessite d'embrasser l'écosystème numérique dans son ensemble et non plus de raisonner selon des logiques sectorielles largement dépassées par la réalité des marchés.

Le mythe du garage californien est une réalité. Aux opérateurs de repenser leurs relations avec les entreprises les plus innovantes et, parfois, de remettre en cause leurs modes de fonctionnement.

Les velléités récurrentes de limiter la possibilité, pour les acteurs, de déployer des services innovants, parfois au nom d'un concept de neutralité mal compris et surtout appliqué de façon sélective, sont également un frein considérable à l'investissement. Le projet de règlement communautaire en cours d'examen, qui ne prévoit rien moins que d'interdire aux opérateurs télécoms d'opérer des services gérés, est à ce titre inquiétant.

Révolution culturelle

De leur côté, les opérateurs doivent aussi mener une révolution culturelle : l'innovation n'est plus exclusivement produite en interne. Elle est de plus en plus le fruit de co-innovations avec des petites structures tierces, qui développent des innovations de rupture, non seulement sur le plan technologique, mais aussi sur celui des services. Le mythe du garage californien est une réalité. Aux opérateurs de repenser leurs relations avec les entreprises les plus innovantes, et, parfois, de remettre en cause leurs modes de fonctionnement.

C'est tout le sens de la démarche d'Orange, qui s'inscrit résolument dans l'écosystème numérique global. Cette démarche passe par la refonte de nos processus de recherche et d'innovation, afin de les rapprocher du temps du marché. Elle passe aussi par une politique d'ouverture volontariste, via des partenariats variés, à la fois avec des géants industriels, des instituts de recherche et des *start-ups*. Orange renforce son soutien à l'écosystème numérique, notamment avec les accélérateurs Orange Fab, par lesquels sont passées plus de 40 *start-ups* à ce jour. Cela passe enfin par le développement d'une stratégie d'investissement ambitieuse, afin d'anticiper et d'accompagner les ruptures.

www.orange.fr

[5]

ITU NEWS N° 1 2015 > Analyses du secteur

Les prévisions des principaux analystes du secteur

https://itunews.itu.int/Fr/5684-Les-previsions-des-principaux-analystes-du-secteur.note.aspx

Le début de l'année est toujours le moment que choisissent de nombreux instituts de recherche et de grands cabinets de conseil pour publier leurs prévisions concernant les télécommunications. Le présent article donne un court résumé de quelques unes des principales tendances qui se dégagent des projections pour cette année.
Pour 2015, de nombreux grands instituts de recherche annoncent que les logiciels pour mobile de prochaine génération, l'informatique en nuage, l'Internet des objets et, bien sûr, les médias sociaux et les mégadonnées vont se développer. Plusieurs analystes ont également étudié les répercussions des nouveautés technologiques pour les entreprises et les consommateurs.
Le phénomène de convergence est très net, puisque beaucoup prévoient que les télécommunications déborderont sur le domaine des technologies de l'information, alors même que les questions liées aux réseaux de télécommunication empiètent de plus en plus sur les domaines des technologies de l'information et de l'Internet (le débat actuel sur la neutralité des réseaux en était une bonne illustration). Selon les projections de l'International Data Corporation (IDC), le cumul des dépenses relatives aux technologies de l'information et aux télécommunications dans le monde augmentera de 3,8% au cours de l'année 2015, pour atteindre quelque 3 800 milliards USD sur l'année.
Ainsi, nombre des prévisions de l'IDC concernant les télécommunications en 2015 portent sur l'évolution du rôle des entreprises de télécommunication dans un secteur en pleine convergence et sur les choix que ces entreprises feront pour se lancer dans les interfaces API, les services à valeur ajoutée, la publicité ciblée sur mobile ou les services de sécurité gérés, et pour adopter la virtualisation des réseaux afin d'accroître leurs marges bénéficiaires.
Ces prévisions vont dans le sens de nombre des conclusions du Sommet des hautes personnalités sur l'avenir organisé par l'UIT, à l'occasion duquel un éminent orateur a suggéré que dans l'avenir, chaque entreprise pourrait dans la pratique devenir un fabricant de logiciels d'une manière ou d'une autre (voir l'article consacré à ITU Telecom World 2014).
Ovum et Infonetics s'intéressent tous deux au ralentissement de la progression des recettes de télécommunication, en particulier en Europe. Selon Infonetics, les recettes générées par les services mobiles dans le monde au premier semestre de 2014 ont augmenté de seulement 0,5% par rapport à la même période en 2013. Toutefois, Infonetics reste positif puisque les services de données mobiles (messagerie textuelle et large bande mobile) ont progressé dans toutes les régions, grâce à l'augmentation de l'utilisation des téléphones intelligents, et l'entreprise prévoit que le marché des données continuera d'être florissant en 2015. Selon Ovum (la branche recherche d'Informa), le nombre d'abonnements mobiles augmentera pour atteindre 8,5 milliards d'ici à la fin de 2019. L'UIT prévoit que le nombre d'internautes dépassera les 3 milliards en 2015. Selon les prévisions de WeAreSocial/Internet World Stats, le mobile contribuera à porter le taux de pénétration de l'Internet au-delà de 50% de la population mondiale fin 2016, avec quelque 2,7 milliards de «connexions» par smartphone dans le monde (on ne sait en revanche pas très bien s'il s'agit du nombre d'abonnements ou de téléphones utilisés). Dans son rapport faisant autorité intitulé «Les Prédictions du secteur des Technologies, médias et télécommunications (TMT)», Deloitte prévoit qu'en 2015, 1,4 milliard de téléphones intelligents seront vendus dans le monde et que les ventes de ce type de téléphones dépasseront les

ventes cumulées d'ordinateurs personnels, de téléviseurs, de tablettes et de consoles de jeux, que ce soit en nombre d'unités vendues ou en montant des recettes. Le cabinet Gartner prévoit qu'en raison de la multiplication des dispositifs mobiles, on s'intéressera davantage aux besoins des utilisateurs dans différents contextes et environnements, plutôt qu'aux seules caractéristiques et fonctionnalités des dispositifs. Gartner prévoit en outre que les téléphones et les objets connectés portables feront partie intégrante d'un environnement informatique de plus en plus vaste (électronique grand public et écrans connectés compris). L'homme ne sera pas le seul à être de plus en plus connecté. De nombreux analystes s'accordent à dire que nous entrons dans l'ère de l'Internet des objets (IoT), dont ils prévoient une forte progression. Selon Deloitte, 1 milliard de dispositifs IoT sans fil seront commercialisés en 2015, soit une augmentation de 60% par rapport à 2014, ce qui signifie qu'il y aura une base de 2,8 milliards d'objets connectés installés d'ici à fin 2015. L'IDC prévoit que les dépenses liées à l'IoT dépasseront 1 700 milliards USD, soit une augmentation de 14% par rapport à 2014 (ces dépenses pourraient même atteindre 3 000 milliards USD d'ici à 2020). Contrairement à de nombreux analystes qui prévoient que l'Internet des objets sera essentiellement constitué de réseaux de capteurs sans fil, l'IDC pense que «l'Internet des objets industriel» fonctionnera pour l'essentiel dans un environnement de lignes fixes dans l'avenir proche, puisque selon le cabinet, plus de 90% du trafic lié à l'Internet des objets industriel devrait passer par les réseaux de lignes fixes.

Dans son rapport annuel, Ericsson Consumer Lab se penche sur l'IoT du point de vue du consommateur et laisse entendre que les consommateurs souhaitent que la technologie et la connectivité soient intégrées dans tous les aspects de leur quotidien. Ericsson pense en outre que 2015 sera une année charnière dans le domaine de la télévision, puisque l'entreprise prévoit que pour la première fois, les consommateurs regarderont davantage de vidéos en streaming que de programmes de télévision classiques. Pour PC Mag, les objets connectés portables devraient «probablement» devenir la catégorie d'objets technologiques la plus populaire en 2015.

Le mot «intelligence» revient lui aussi très souvent, même si les avis divergent concernant ce qui, ou pour être plus précis, concernant les éléments qui deviennent plus intelligents. Pour l'IDC, ce sont les réseaux. Pour d'autres, c'est notre environnement connecté tout entier. Pour GP Bullhound, banque d'investissement spécialisée dans les entreprises technologiques, ce sont les dispositifs intelligents de l'IoT qui sont de plus en plus intelligents, grâce aux innovations dans le domaine des logiciels et à une meilleure utilisation des données. Selon GP Bullhound, les dispositifs connectés portables (par exemple, les bracelets Fitbit et Jawbone) se sont avérés utiles pour suivre l'activité des personnes dans le monde réel et générer des données, mais ils exigent généralement de trop nombreuses manipulations de la part des consommateurs pour être véritablement «intelligents». Dans le cas de dispositifs plus sophistiqués, des applications fonctionneront en permanence en arrière-plan, en tenant compte du contexte, et collecteront des données auprès de multiples sources, s'adapteront, apprendront et se mettront à jour de manière automatique et, dans certains cas, prendront des mesures sans que l'utilisateur ait à intervenir ou à donner d'instructions.

Certains observateurs vont même plus loin, en laissant entendre que les schémas d'écoulement du trafic mobile et les charges des réseaux évoluent en réponse à des demandes de service faites par les réseaux (comme c'est le cas avec les téléphones intelligents via les réseaux LTE (évolution à long terme), par exemple). Les opérateurs mobiles devront peut-être revoir l'architecture, la topologie et les fonctionnalités de leurs réseaux pour acheminer efficacement le trafic 4G, tout en offrant une bonne expérience client et en augmentant leurs marges bénéficiaires. Deux choses sont en tous cas certaines: l'innovation et l'évolution des

réseaux de télécommunication/TIC se poursuivent à un rythme soutenu et il est impossible de s'ennuyer lorsqu'on est un observateur ou un acteur du secteur des télécommunications!

---

1 "Forrester Predictions"http://www.forrester.com/Forrester-Predictions-2015/-/E-MP1161?intcmp=mkt:$social:predictions.

2 "Top Tech Predictions for 2015", PC Mag. 29 December 2014, available from:http://www.pcmag.com/article2/0,2817,2474114,00.asp

3 http://www.mis-asia.com/tech/networking/idc-announces-predictions-for-telecoms-industry-for-2015/

4 http://telecomworld.itu.int/daily-highlights-1/future-every-company-will-become-software-company/

"Ovum Telecoms, Media and Entertainment Outlook 2015", available

from:http://info.ovum.com/uploads/files/Ovum_Telecoms_Media_and_Entertainment_Outlook_2015.pdf

5 http://www.lightwaveonline.com/articles/2015/01/datacom-to-telecom-sluggish-in-2014-says-infonetics.html?cmpid=StrackId

6 http://wearesocial.sg/blog/2015/01/digital-social-mobile-2015/.

7 http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/tmt-pred15-full-report.pdf

8 "Gartner Identifies the Top 10 Strategic Technology Trends for 2015", available from Gartner at:http://www.gartner.com/newsroom/id/2867917 Information about Gartner Symposium/ITxpo in Orlando, is available at:www.gartner.com/us/symposium. Video replays of keynotes and sessions are available on Gartner Events on Demand at:www.gartneronlemand.com.

9 http://www.ericsson.com/res/docs/2014/consumerlab/ericsson-consumerlab-10-hot-consumer-trends-2015.pdf.

9 http://www.cgbullhound.com/wp-content/uploads/2015/01/CB-Bullhound-Technology-Predictions-2015.pdf

C67

Les usages de l'internet augmentent, la vigilance des internautes aussi !

http://www.fftelecoms.org/articles/les-usages-de-l-internet-augmentent-la-vigilance-des-internautes-aussi

40% des internautes français ont confiance dans l'usage d'internet, l'intérêt pour les objets connectés se confirme

Malgré un recul du niveau global de confiance, les usages internet des français ne faiblissent pas, selon une étude ACSEL-CDC : 89% des internautes pratiquent le e-commerce, 89% l'e-administration, 86% la banque en ligne et 77% utilisent les réseaux sociaux. De nouveaux usages apparaissent : 10% des internautes possèdent un objet connecté.

La protection des données personnelles et la sécurité des données bancaires et des comptes utilisateurs comptent parmi les principales préoccupations des internautes français. A cet égard, l'étude ACSEL-CDC souligne que l'existence de garanties techniques de sécurisation des données constitue, avec la crédibilité du site utilisé, l'un des leviers majeurs de la confiance numérique.

En parallèle, les internautes français se révèlent de plus en plus vigilants quant aux données et informations qu'ils sont prêts à partager, en particulier avec les acteurs privés et via les réseaux sociaux. Ils développent peu à peu des stratégies de protection de leurs données personnelles : 84% ont déjà eu une action concrète en de protection en naviguant sur internet, 70% ont déjà effacé des cookies, ou des fichiers temporaires.

Les internautes font preuve d'une maturité et d'un recul croissants vis-à-vis de l'internet qui ne freinent pas pour autant leurs usages : e-commerce, banque en ligne, e-administration et réseaux sociaux restent fortement utilisés et l'intérêt pour les objets connectés connaît un essor fulgurant. 10% des internautes sont équipés d'un objet connecté et 20% ont des projets d'équipement. La maison connectée (4% équipés, 14% « en projet »), la voiture connectée (5% équipés, 11% « en projet ») et les bracelets ou montres connectés sont plébiscités. Ici encore, la problématique de la protection de la vie privée et des données personnelles constitue le sujet majeur de préoccupation : 61% des utilisateurs sont gênés par le stockage en ligne de ces données.

[7]

Objets connectés : Orange acquiert la start-up Ocean

FABIENNE SCHMITT - LES ECHOS | LE 16/04/2015

http://www.lesechos.fr/16/04/2015/LesEchos/21920-099-ECH_objets-connectes_-orange-acquiert-la-start-up-ocean.htm

L'entreprise est spécialisée dans la géolocalisation de véhicules. Elle permet à l'opérateur de se renforcer dans les objets connectés.

Orange l'a récemment annoncé : il veut réaliser 600 millions d'euros de chiffre d'affaires dans les objets connectés en 2018, soit six fois plus que l'an dernier. L'opérateur met ce programme en application, en s'offrant la start-up Ocean, spécialisée dans la gestion de flottes et la géolocalisation de véhicules.

Créée en 2003 et pilotée par Philippe Rivière depuis 2007, Ocean est une société rentable de 70 salariés qui réalise 10,2 millions de chiffre d'affaires. Son rapprochement avec Orange lui permet de s'adosser à un groupe mieux à même de financer ses développements futurs. L'opérateur télécoms a déjà développé en interne une activité de gestion de flottes de véhicules, via sa filiale Orange Business Services. Ocean vient la renforcer : avec sa nouvelle jeune pousse, il passe de 60.000 à plus de 100.000 véhicules gérés et totalise 5.000 clients. Il revendique désormais la position de leader du marché. *« L'idée, c'est d'être très puissant en France pour se développer à l'international, en particulier en Europe et en Asie »*, affirme Béatrice Felder, directrice d'Orange Applications for Business. La plate-forme d'Ocean doit aussi permettre à Orange de développer de nouveaux services liés à l'Internet des objets, par exemple dans le domaine agricole (bennes, citernes...).

Montée en puissance

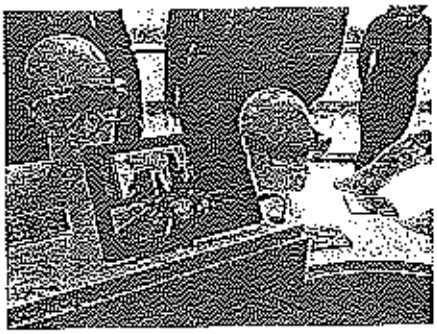
L'acquisition s'inscrit dans la stratégie de montée en puissance du groupe sur le prometteur marché des objets connectés et dans le domaine du « Machine to Machine ». Orange gère plus de 1,3 million d'objets connectés dans les domaines de la santé, des villes intelligentes et de la maison connectée, en plus des transports. L'opérateur a notamment développé Homelive, un service qui permet à l'utilisateur de piloter sa maison depuis son mobile. *« On estime qu'il y aura plus de 25 milliards d'objets connectés aux réseaux dans le monde en 2020. La connectivité sera en quelque sorte l'oxygène des objets connectés »*, avait martelé Stéphane Richard, PDG d'Orange, lors de la présentation de son plan stratégique à la mi-mars.

[8]

Qualcomm prêt pour la bataille de l'Internet des objets

ROMAIN GUEUGNEAU / JOURNALISTE | LE 18/05 À 16:23, MIS À JOUR À 16:37

http://www.lesechos.fr/tech-medias/hightech/0217480719?-qualcomm-pret-pour-la-bataille-de-linternet-des-objets-1120366.php



L'américain lance des produits dédiés aux objets connectés. Il espère tirer près de 2 milliards de dollars de revenus de ce nouveau segment.

C'est le nouveau territoire de conquête des géants de la tech. Après la révolution du smartphone, voici venue celle de l'Internet des objets. Voitures, compteurs d'eau, montres ou électroménager : d'ici quelques années, la plupart de ces appareils seront connectés au réseau. Un gigantesque marché se dessine et les estimations vont bon train : entre 25 et 50 milliards d'objets pourraient être connectés d'ici à 2020, pouvant représenter jusqu'à 3.000 milliards de dollars !

Qualcomm a des arguments à faire valoir dans la bataille qui se profile. Peu connu du grand public, le californien est un géant du mobile. Il équipe la grande majorité des smartphones et tablettes en processeurs, modems et autres composants pour la connectivité (wifi, bluetooth, LTE...). « *Nous maîtrisons l'ensemble des technologies nécessaires pour faire avancer ce marché et profiter des immenses opportunités de croissance* », explique Derek Aberle, le président de Qualcomm, qui dévoilait la vision du groupe sur l'Internet des objets lors d'une conférence à San Francisco, la semaine dernière.

Plus d'un milliard de dollars de revenus

Selon le dirigeant, il ne suffit pas de connecter tous ces appareils au réseau pour les rendre plus intelligents, il faut aussi les rendre plus puissants, notamment en les équipant de processeurs. « *Une grande partie de ces objets devra être capable de communiquer directement entre eux, sans avoir à passer par le réseau, pour éviter de le saturer* », souligne Derek Aberle.

Si l'Internet des objets est encore un marché du futur, Qualcomm en profite déjà. Le groupe de San Diego a engrangé plus d'un milliard de dollars de revenus l'an dernier en composants dédiés à d'autres produits que des smartphones ou des tablettes (sur un total de 26,5 milliards). Et cela pourrait représenter plus de 10 % du chiffre d'affaires de la division puces cette année (soit environ 2 milliards).

Produits dédiés

Dans le portefeuille de produits du groupe, il n'existe pourtant aucun composant dédié. Les montres connectées de LG et Samsung embarquent ainsi des processeurs Snapdragon de Qualcomm initialement conçus pour les smartphones. Seuls quelques ajustements ont été réalisés pour s'adapter à la résolution de l'écran. Cela va bientôt changer.

A San Francisco, Qualcomm a dévoilé deux produits spécialement conçus pour l'Internet des objets et notamment la maison connectée : économes en énergie, ils pourront être embarqués dans des appareils comme un four ou une lampe, par exemple. Le groupe a aussi fait la démonstration d'un nouveau protocole de communication permettant aux objets de dialoguer directement entre eux - si la porte du réfrigérateur reste ouverte, un message d'alerte s'affiche sur le téléviseur du salon.

Cabines téléphoniques transformées en bornes Wifi

Travaillant avec une quinzaine de constructeurs, Qualcomm équipe déjà depuis plusieurs années les voitures en solutions de connectivité (3G, 4G...). Il lancera l'an prochain des processeurs intégrés dans les véhicules, permettant de faire tourner des applications de divertissement mais surtout d'analyser les multiples données des caméras et capteurs positionnés un peu partout dans et autour du véhicule.

Le groupe va aussi accentuer ses efforts dans les programmes de « smart cities ». Il travaille pour l'instant sur une vingtaine de projets dans le monde. Il a notamment été sélectionné par la ville de New York pour transformer 7.500 anciennes cabines téléphoniques en bornes wifi.

Qualcomm n'est pas le seul géant des puces à vouloir jouir davantage des promesses de l'Internet des objets. Intel et Broadcom sont également sur les rangs, tout comme Samsung . La semaine dernière, le groupe coréen avait aussi choisi San Francisco pour présenter une nouvelle gamme de processeurs destinée à être embarqués dans tous les objets connectés... La bataille ne fait que commencer.

[9]

Et si la voiture connectée saturait les réseaux mobiles ?

http://www.cnetfrance.fr/cartech/et-si-la-voiture-connectee-saturait-les-reseaux-mobiles-39819734.htm

La voiture connectée annonce une petite révolution dans l'automobile mais elle pourrait avoir une conséquence fâcheuse : saturer les réseaux de téléphonie mobile.

- Par Benoît Sollvellas @B_Solivellas
- lundi 25 mai 2015 à 10:30

Vidéo à la demande, musique en streaming, partage d'informations sur les conditions routières ou sur la météo,...la voiture connectée va devenir très gourmande en bande passante sur les réseaux de téléphonie mobile.

Encore marginale aujourd'hui, la voiture communicante deviendra la norme ces prochaines années. Le cabinet d'analyses Gartner estime que d'ici à 2020, 250 millions de voitures connectées seront en circulation. Résultat, d'ici 2023, Machina Research estime que ces autos s'accapareront la moitié des connexions M2M (entre terminaux, c'est à dire hors communications entre personnes physiques). Et la surcharge ne sera pas évidente à supporter pour les opérateurs de téléphonie. D'ici 10 ans, certaines antennes relais pourraient ainsi connaître une augmentation de 97% de demande de connexion.

Les opérateurs devront donc s'organiser d'autant que les projets de nouvelles applications sont chaque jour un peu plus larges. Parmi les derniers projets en date figurent **l'ouverture à distance pour les livraisons** ou la **recherche de places de stationnement disponibles**.

Interview Delphine Asseraf — Allianz : « Un assureur est légitime à tirer de la valeur des objets connectés »

Xavier Biseul, 1 juin 2015, 19:10
http://www.itespresso.fr/interview-delphine-asseraf-allianz-assureur-legitime-tirer-valeur-objets-connectes-96867.html

Internet des objets, Pay how you drive, mobilité… Delphine Asseraf, Directrice digital d'Allianz France, aborde tous ces sujets.

Boîtier qui évalue votre comportement au volant, détecteur de fumée connecté à la maison…

Allianz veut mettre des objets connectés partout. Une façon pour l'assureur de renforcer son rôle de prévention et de personnaliser ses services. Explications de sa directrice digital.
En un an, Allianz France a multiplié les annonces autour des objets connectés. L'assureur a tout d'abord commencé par donner des cours de conduite avec TomTom puis s'est associé à Nest pour offrir un détecteur de fumée à ses nouveaux clients. Enfin, plus récemment, il déclinait son application mobile pour l'Apple Watch.

Une frénésie autour des objets connectés qui rappelle celle menée par son concurrent Axa. Les deux géants de l'assurance en France se collent d'ailleurs à la culotte avec des communiqués publiés parfois à quelques jours d'intervalle. Mais, dans cette course contre la montre, la compagnie d'origine allemande cultive sa différence.
Alors que le coach de conduite d'Axa repose sur une appli mobile (Axa Drive Coach) Allianz associe appli et boîtier. De même, Allianz va se lancer dans le « pay how you drive » - la prime du contrat auto varie en fonction du comportement au volant – mais uniquement à la baisse alors que le produit que vient de lancer Direct Assurance (filiale d'Axa) prévoit aussi une majoration en cas de mauvaise conduite.

Décryptages de Delphine Asseraf, Directrice digital d'Allianz France.

ITespresso.fr : Pourquoi un assureur s'intéresse aux objets connectés ?
Delphine Asseraf : Au-delà du phénomène de mode, nous pensons qu'il y a une véritable légitimité pour un assureur d'en tirer de la valeur ajoutée. En connaissant plus finement et plus régulièrement les usages de nos assurés, nous pouvons agir dans le domaine de la prévention.
Le dispositif « Allianz conduite connectée » ne requiert aucune installation complexe et aucune interaction pendant la conduite par exemple. C'est un partenaire de conduite qui vous protège en observant votre comportement sur la route sur la base d'indicateurs simples et efficaces que sont l'accélération, le freinage, la tenue de route dans les virages.

A partir de là, le système vous donne des conseils pour rendre la route plus sûre. Avec des défis pour s'améliorer. C'est une sorte de bracelet connecté de la voiture qui, sur le principe du « quantified self », pose un constat objectif et livre des pistes de progression.

Le dispositif ne repose pas uniquement sur une application mobile mais sur un boîtier qui a fait ses preuves – celui de TomTom. Un boîtier qui se branche directement sur le port diagnostic du véhicule.

ITespresso.fr : Allez-vous proposer le « pay how you drive » ?
Delphine Asseraf : Oui, nous allons le proposer dès cette année, toujours avec TomTom. Les assurés qui ont un comportement vertueux au volant se verront appliquer une réduction de leur prime. A la différence d'autres acteurs du marché, nous ne discriminerons pas les conducteurs qui auront de mauvais scores. Nous sommes avant tout dans la prévention.
Dans le même esprit, Allianz a offert un détecteur de fumée Nest aux clients souscrivant un contrat d'assurance habitation.

Pour Allianz France, il s'agit aussi de mettre du sens à ces innovations et c'est le deuxième axe de notre stratégie : l'assistance. Le boîtier TomTom comprend un appel d'urgence qui en cas de choc contacte le conducteur puis, en l'absence de réponse, les services d'urgence.

Nous prenons les devants de l'eCall (*) qui sera obligatoire pour les véhicules neufs à partir du 31 mars 2018, tout en pouvant équiper le parc de voitures existant.

ITespresso.fr : Quel est l'apport des mobiles dans cette stratégie ?
Delphine Asseraf : Les objets connectés permettent de rendre l'assurance plus personnalisée, plus en phase avec les usages de nos clients.
Notre application sur l'Apple Watch permet, par exemple, de trouver un de nos partenaires santé et de s'y rendre en prenant le meilleur itinéraire. Cela peut se faire en situation de mobilité sans avoir un smartphone en main.

Enfin, notre stratégie porte sur le renforcement de la relation-client. Avec notre application mobile, nous pouvons faire de la pédagogie au quotidien en livrant des conseils via des notifications. Cette appli mobile s'enrichit de nouvelles fonctionnalités tous les trimestres.

Les services permettent de tisser une relation durable avec son assureur sans que les contacts ne se limitent aux moments des sinistres qui fort heureusement n'ont pas lieu tous les jours, même si Mon Allianz Mobile permet de déclarer un sinistre de A à Z en prenant des photos.

ITespresso.fr : Comment Allianz s'intègre dans l'écosystème de l'innovation ?
Delphine Asseraf : Allianz France a noué des partenariats avec des acteurs de l'économie collaborative. Pour Drivy qui fait de la location entre particuliers, Allianz France se substitue à l'assureur habituel du propriétaire le temps de la location. Nous proposons aussi aux chauffeurs professionnels d'Uber une offre auto qui répond aux besoins spécifiques des VTC.
Allianz a aussi récemment ouvert sa première promotion de start-up au sein de son accélérateur à Nice : des jeunes pousses prometteuses dans les domaines du big data, des objets connectés, du stade connecté et des FinTech. Elles bénéficieront d'un accompagnement personnalisé par un réseau d'experts et de mentors, internes et externes.

Pour Allianz, cet écosystème est un autre moyen d'appréhender les nouveaux usages. Nous ne nous interdisons pas de co-construire des offres avec des start-up et de les développer en France et à l'international.

(*) eCall : appels d'urgence (112)

(**) VTC : voiture de transport avec chauffeur

[4]

Les constructeurs auto font monter Apple et Google à bord

MAXIME AMIOT / JOURNALISTE | LE 03/06 À 06:00, MIS À JOUR À 10:12

http://www.lesechos.fr/journal20150603/lec2_finance-et-marches/021106877165-les-constructeurs-auto-font-monter-apple-et-goo

Grâce aux systèmes Car Play (ci-dessus) et Android Auto, le conducteur pourra déporter son écra musique et d'autres applications.

Les premiers modèles intégrant les systèmes des deux géants du numérique arrivent sur le marché.

Après des mois de buzz intensif, les premières voitures compatibles avec les systèmes d'exploitation d'Apple et Google commencent à arriver sur le marché. Du côté de PSA, Car Play, le système embarqué d'Apple, « *sera accessible en fin d'année sur une demi-douzaine de modèles* », dont l'ensemble de la gamme DS (DS3, DS4, DS5) ainsi que des modèles Peugeot et Citroën, indique aux « Echos » Gaël Colin, en charge des technologies embarquées chez PSA. Quant à Android Auto, la solution de Google, « *elle sera intégrée dès 2016* » sur les nouveaux modèles du groupe, ajoute Gaël Colin. Dans les deux cas, les solutions seront déployées sur l'ensemble des gammes des trois marques du groupe, à partir du segment B (citadines).

PSA rejoint ainsi d'autres constructeurs très actifs sur le sujet. La semaine dernière, Hyundai annonçait l'arrivée d'Android Auto sur sa berline Sonata, vendue aux Etats-Unis. De même, à partir de cet été et jusqu'en 2016, General Motors déploiera Car Play et Android Auto sur 15 modèles de la marque Chevrolet. En Europe, Opel, propriété de GM, ouvrira le bal en fin d'année, avec la nouvelle Astra. Celle-ci intégrera les deux systèmes avant qu'ils ne soient déployés sur le reste de la gamme en 2016. Enfin, chez Audi, on annonce que les solutions seront aussi disponibles d'ici à la fin de l'année sur le nouveau Q7.

Mirror Link, la 3e solution

Grâce à un raccord USB, Car Play et Android Auto permettent au conducteur ou à son passager de déporter leur écran de smartphone sur l'écran de bord, et de profiter ainsi de la navigation, de la musique et autres applications. Le tout piloté par les systèmes de reconnaissance vocale d'Apple et Google. D'autres contenus pourront être proposés au fil du temps, à condition d'être certifiés par Apple et Google et d'être sans risque pour la sécurité. Le début d'un raz de marée ? Pour le cabinet IHS, les deux systèmes devraient équiper, d'ici à 2020, plus de 30 millions de voitures chacun dans le monde. Mais si les géants du numérique ont fait leurs preuves en termes d'ergonomie, ils devront lever certaines limites. Tandis que Car Play n'est accessible qu'aux utilisateurs d'iPhone 5 ou d'iPhone 6, Android Auto ne s'adresse qu'aux propriétaires de smartphone embarquant la dernière version d'Android, baptisée « Lollipop » (Android 5.0), qui reste encore marginale.

Certains misent du coup sur une troisième solution, Mirror Link, qui propose le même type de services (déport de l'écran), mais sur un éventail de smartphones plus large (plus de 1.000 modèles certifiés). « *Il faut pouvoir proposer différentes solutions, sans exclusivité aucune* », indique Gaël Colin, de PSA, qui propose Mirror Link sur ses citadines C1, 108 ou sur la nouvelle DS5.

L'attractivité de ces solutions dépendra de leur ergonomie, de la richesse des contenus et du coût pour l'utilisateur. Du côté d'Audi, on précise que l'option pour profiter d'Apple Car Play et d'Android Auto sera commercialisée entre 500 et 700 euros. Chez PSA, l'option Mirror Link coûte 250 euros. Dernière interrogation : le risque pour les constructeurs de laisser le contrôle de l'écran à des acteurs extérieurs. Ce n'est pas un hasard si Renault et Nissan n'ont toujours pas annoncé de modèles intégrant les solutions.

[12]

L'USINEDIGITALE
LE MEDIA DE LA TRANSFORMATION NUMÉRIQUE

Toshiba et Microsoft s'allient dans l'Internet des objets

RIDHA LOUKIL Publié le 05 juin 2015 à 10H16
http://www.usine-digitale.fr/article/toshiba-et-microsoft-s-allient-dans-l-internet-des-objets.N333651

Les deux groupes veulent combiner les dispositifs électroniques du premier et le cloud du second pour simplifier aux entreprises la mise en place d'applications d'internet des objets. Ils comptent démarrer dès cette année par les secteurs de transport et logistique.

Toshiba et Microsoft s'allient dans l'Internet des objets © CC jeferrb

Toshiba et Microsoft s'associent pour développer conjointement des solutions complètes d'internet des objets. Les deux groupes veulent combiner leurs savoir-faire complémentaires pour s'adresser de bout en bout à ce marché prometteur.

Le groupe japonais fournit des dispositifs électroniques comme les processeurs d'applications, les capteurs, les enregistreurs de conduite de véhicule ou les technologies de stockage de données, pour transformer les produits en objets connectés. De son côté, l'éditeur américain propose des services sur son cloud Azure pour la collecte, le stockage, l'exploration et l'analyse des données issues de ces objets. L'un de ces services le plus avancé est l'apprentissage statistique à partir des big data ou Machine Learning, dont le rôle est de prévoir le futur à partir de données du passé. Les deux partenaires espèrent simplifier la mise en place d'applications en combinant leurs savoir-faire.

DES SOLUTIONS PACKAGÉES ET À L'ÉTAT DE L'ART

La surveillance des ascenseurs à des fins de maintenance prédictive illustre l'intérêt de cette alliance. Elle a besoin d'un côté de capteurs, processeurs et autres composants électroniques pour relever les données de fonctionnement des engins, et de l'autre, de services cloud pour suivre en temps réel et à distance les machines. Grâce à l'analyse des données avec le Machine Learning, il devient possible de prévoir où et quand les pannes vont se produire, et d'anticiper ainsi les interventions de maintenance. C'est ce que l'ascensoriste allemand ThyssenKrupp fait en s'appuyant sur le cloud Azure de Microsoft.

L'offre disponible aujourd'hui pour l'internet des objets est fragmentée entre une multitude d'intervenants sur la chaîne de valeurs : fournisseurs de composants électroniques, éditeurs de logiciels, opérateurs cloud, etc. En joignant leurs forces, Toshiba et Microsoft espèrent accélérer l'adoption de l'internet des objets en offrant des solutions packagées de bout en bout qui simplifient la mise en oeuvre d'applications. Ils prévoient de démarrer cette année par les secteurs de transport et logistique. Avec la promesse des solutions à l'état l'art sur le plan technologique, rentables, évolutives et faciles d'usage.

L'Internet des objets est perçu comme un nouvel Eldorado. Selon la dernière étude du cabinet IDC, il représenterait une opportunité business de 1700 milliards de dollars dans le monde à l'horizon 2020. De quoi aiguiser bien des appétits. General Electric, Schneider Electric, Cisco, IBM, SAP, Qualcomm, Intel, Microsoft, Samsung... Tous les grands industriels, et pas seulement du numérique, se positionnent sur ce marché. Mais l'alliance entre Toshiba et Microsoft est la première du genre.

[13]

Sigfox, LoRa, Qowisio : la bataille pour les réseaux bas débit est lancée

Par Pierre Manière | 09/06/2015, 18:15

http://www.latribune.fr/technos-medias/sigfox-lora-qowisio-la-bataille-pour-les-reseaux-bas-debit-est-lancee-482685.html

Anne Lauvergeon et Ludovic Le Moan, respectivement présidente du conseil d'administration et PDG de Sigfox, veulent faire de leur solution un standard. (Crédits : Reuters)

Spécialistes de l'Internet des objets, ces sociétés développent des technologies de réseaux et de capteurs sans fil qui permettent de surveiller automatiquement les compteurs à gaz, de développer des parkings intelligents, de mieux maîtriser l'éclairage public, de détecter les incendies ou encore de mieux gérer le trafic routier. Engagées dans une course de vitesse pour déployer leurs solutions et les imposer, ces pionniers jouent des coudes en France et à l'international.

Les réseaux bas débit sans fil ont le vent en poupe. Et pour cause : il s'agit d'un des principaux moteurs de la révolution à venir de l'Internet des objets. Les enjeux sont colossaux : demain, la plupart des objets, mais aussi une large part des équipements publics (les routes, les voies ferrées, les lampadaires...) disposeront de capteurs capables de renvoyer des informations sur leurs usages ou leur environnement. Ainsi, un capteur géolocalisé et enterré sous une bretelle d'autoroute pourra, par exemple, renvoyer des informations sur le trafic. Un autre, installé sur un compteur d'eau, permettra de récupérer très facilement des données liées à la consommation. Placé sur un point haut, un capteur pourra mesurer la qualité de l'air.

Cette révolution est à nos portes. Selon le cabinet Idate, il y aura quelque 80 milliards d'objets connectés à travers le monde d'ici 2020 ! Connecter ces objets, et leur permettre de communiquer entre eux pour récolter des informations ou leur en envoyer, s'avère donc crucial. C'est là qu'interviennent les réseaux bas débit, un créneau où la France est pour l'heure très bien placée. Les sociétés Sigfox et Qowisio, ainsi que la technologie LoRa (mise en place par l'entreprise iséroise Cycleo, rachetée par l'Américain Semtech), sont actuellement engagées dans une course de vitesse pour imposer leurs solutions dans l'Hexagone et à travers le monde.

Qowisio à l'assaut du marché français

Concrètement, elles développent des systèmes à base d'antennes, de capteurs et de serveurs, pour collecter et envoyer des informations ou des ordres aux objets ou infrastructures ciblés. De manière générale, ces technologies insistent sur la grande autonomie des capteurs, dont la faible consommation d'énergie leurs permet de vivre plusieurs années. Une obligation, puisqu'on imagine mal, par exemple, remplacer tous les mois un dispositif enterré sous la chaussée. Leurs solutions sont toutes peu coûteuses, en raison, notamment, du nombre de capteurs à installer. En outre, elles mettent toutes l'accent sur la fiabilité en termes de connectivité. Mieux, les antennes disposent d'une très grande portée, jusqu'à plusieurs dizaines de kilomètres, permettant de déployer un réseau plus facilement et efficacement.

Sur ce créneau, l'heure est aux grandes manœuvres. Cette semaine, Qowisio a levé 10 millions d'euros. Après avoir déployé 18 réseaux privés à l'étranger, cette pépite française souhaite faire son nid dans l'Hexagone. A *La Tribune*, Cyrille Le Floch, son PDG, explique qu'il va notamment travailler avec une enseigne de grande distribution basée à Anger, dont il conserve l'anonymat. L'objectif est ici d'améliorer la logistique : *« On va mettre en place un suivi des palettes de produits pour pouvoir les géolocaliser entre les magasins et la centrale d'achat »*, explique-t-il. Pour séduire ses clients, Cyrille le Floch revendique une solide expérience à l'international. *« On a travaillé avec de gros opérateurs télécoms en Europe et dans les pays émergents »*, avance-t-il. Pour l'un d'entre eux, il a notamment glissé ses capteurs au niveau des antennes-relais, pour vérifier qu'elles étaient bien alimentées en électricité.*« Ainsi, si le réseau tombe en panne, l'opérateur sait immédiatement quelle installation pose problème. »* Il peut donc y envoyer ses équipes techniques sans perdre de temps. D'autres applications apparaissent prometteuses, surtout du côté des économies d'énergie. *« En mettant des capteurs dans les lampadaires, on pourra gérer l'éclairage public de manière beaucoup plus fine qu'aujourd'hui. »*

Sigfox séduit les investisseurs

Mais Qowisio n'est pas tout seul. Loin de là. Pour s'imposer, elle doit faire face à un concurrent particulièrement vorace : Sigfox. Véritable pionnier du secteur, cette société toulousaine revendique la place de « leader mondial de la connectivité des objets ». Elle a déjà développé moult applications. Parmi elles, la startup a participé à Fastprk : l'an dernier à Moscou, elle a déployé plus de 11.000 capteurs pour donner, via une appli mobile, des informations sur l'état de stationnement en temps réel. But de l'opération : désengorger le centre-ville de la capitale russe, célèbre pour sa très mauvaise circulation.

En février dernier, Sigfox a levé pas moins de 100 millions d'euros auprès d'investisseurs renommés (la banque publique Bpifrance ou le fonds Partech Ventures) et d'industriels intéressés (comme GDF Suez, Air Liquide, ou l'opérateur espagnol Telefonica). Grâce à cette manne, Sigfox veut accélérer son déploiement à l'international, et notamment aux Etats-Unis. L'enjeu est de taille : *« Cette levée de fonds salue notre parcours et met en lumière le potentiel de Sigfox dans la course à venir pour le standard mondial de la connectivité par messages courts »*, estimait Ludovic Le Moan, le PDG de la société, dans la foulée de sa levée de fonds.

LoRa séduit Bouygues Telecom et Orange

Dans son collimateur figure la technologie concurrente LoRa (pour Long Range), qui séduit elle aussi de nombreux acteurs. Dans l'Hexagone, Bouygues Telecom a choisi cette solution pour déployer son réseau. Destinée principalement à des clients industriels, celui-ci vise à séduire des

grands groupes comme Primagaz ou Veolia, d'après une source interne. *« En mettant des puces dans les bouteilles de gaz, on pourra par exemple savoir lorsqu'elles sont presque vide, tout sachant précisément où elles se trouvent,* poursuit cette même source.*Ainsi, on pourra mieux gérer et anticiper les approvisionnements. »* De quoi économiser de précieux deniers sur la logistique...

Orange a lui aussi opté pour LoRa. Depuis peu, l'opérateur historique a lancé un projet pilote à Grenoble, avec une vingtaine d'entreprises. Nicolas Demassieux, directeur des Orange Labs et de la recherche du groupe, égrène différents usages : « On s'intéresse à tous les aspects liés à la consommation de l'énergie, à la mesure de l'humidité, ou aux applications liées à la localisation d'équipements comme les bus ou les trains... »

« Aujourd'hui, certains font beaucoup de bruit... »

Confronté à cette concurrence, Sigfox n'apprécie guère qu'on marche sur ses plates-bandes. Fin mai, Ludovic Le Moan a fusillé le choix de LoRa par Bouygues Telecom de manière bien peu courtoise :

« Je suis persuadé que Bouygues Telecom va échouer dans l'Internet des objets. Je suis même prêt à le parier. Ils sont enfermés dans leur histoire, leur héritage, ils ne peuvent pas aller vite pour réellement 'disrupter' le marché. Ce n'est pas la bonne approche. Si j'étais le PDG de Bouygues Telecom, je serai plutôt allé voir Sigfox plutôt que de m'en faire un rival », a-t il jugé lors de laConnected Conference, *selon le site usine-digitale.fr.*

Chez Bouygues Telecom, on assure que le choix de LoRa a été mûrement réfléchi. *« C'est la meilleure technologie »*, assure notre source. *« Aujourd'hui, il y a des gens qui font beaucoup du bruit. C'est sans doute qu'ils sont nerveux... »*, nous dit-on. Réponse du berger à la bergère. Reste que la bataille ne fait que commencer.

L'ÉLECTRONIQUE SE MOBILISE POUR RÉPONDRE AUX ENJEUX DE L'INTERNET DES OBJETS

RÉDIGÉ PAR JACQUES MAROUANI JEUDI, 25 JUIN 2015 13:09

http://www.electroniques.biz/index.php/economie/vie-de-la-profession/item/54494-l-electronique-se-mobilise-pour-repondre-aux-enjeux-de-l-internet-des-objets

Six des grands acteurs de l'Internet des objets se sont exprimés lors de notre soirée de remise des "Electrons d'or" : Laurent Vernat, directeur du marketing d'Intel Europe de l'ouest, Patrizio Piasentin, directeur de Silicon Labs pour l'Europe du sud, Stuart Lodge, vice-président de Sigfox, Alain Dantec, vice-président de Semtech, Philippe Cola, architecte cœur de réseau et services, à la direction technique de Bouygues Telecom, et Thierry Sachot, directeur général d'Eolane et président de la toute nouvelle Cité de l'objet connecté.

Dans le cadre de la soirée de remise des "Electrons d'or" qui s'est tenue le mercredi 24 juin à Paris, une conférence portant sur le thème de l'Internet des objets et des défis qui en découlent pour l'électronique, a réuni six des grands acteurs de ce domaine : Laurent Vernat, directeur du marketing d'Intel Europe de l'ouest, Patrizio Piasentin, directeur de Silicon Labs pour l'Europe du sud, Stuart Lodge, vice-président de Sigfox, Alain Dantec, vice-président de Semtech, Philippe Cola, architecte cœur de réseau et services, à la direction technique de Bouygues Telecom, et Thierry Sachot, directeur général d'Eolane et président de la toute nouvelle Cité de l'objet connecté.

"Tout objet peut devenir intelligent. Nous avons devant nous un marché colossal et exponentiel qui s'appuie sur trois piliers : les capteurs, dont le coût a été divisé par 2 en 10 ans, la bande passante dont le coût a été divisé par 40 en 10 ans et la puissance de calcul dont le coût a été divisé par 60 en 10 ans. Une croissance importante qu'il faudra gérer, car le potentiel est très important. A ce jour, 85% des outils industriels ne sont pas encore connectés. 15 milliards d'objets seront connectés d'ici fin 2015, mais il seront au nombre de 50 milliards d'ici 2020, selon IDC. Quant au flux de données à stocker et à analyser, il pourrait atteindre 44 zettaoctets, soit 44000 milliards de Go, selon cette même source(*). Il faudra filtrer, analyser et agréger les données avant l'envoi dans le cloud", explique Laurent Vernat.

Réaliser des objets faible consommation

"Il y a de plus en plus d'acteurs dans le domaine de l'Internet des objets. Nous avons déjà été témoins de nombreuses "success stories". Nous avons des objets connectés de types très divers : montres, thermostats, alarmes, compteurs, etc... Nous évaluons pour notre part le nombre d'objets connectés sans intervention humaine à 8 milliards d'unités d'ici 2020 dont 3,7 milliards pour les applications grand public, 0,4 milliard pour les transports, 0,3 milliard pour le domaine de la santé, 1,7 milliard pour les infrastructures de bâtiments et 1,5 milliard pour les industries dans les villes de demain. Le principal défi : comment réaliser des objets faible consommation ? Trois standards couvrent plus de 90% des applications sans fil basse consommation : Zigbee, Bluetooth et les fréquences 2,4 GHz et inférieures au GHz", précise Patrizio Piasentin.

"Le marché de l'Internet des objets nécessite un énorme effort de créativité, des modèles collaboratifs, des partenariats reliant l'industrie avec les start-up. C'est un levier de création de valeur. L'Internet des objets remplit un rôle sociétal dans des domaines variés tels que l'énergie, la santé, les problèmes alimentaires. Il faudra répondre à des enjeux économiques tout en analysant les besoins en matière de sécurité", souligne Stuart Lodge.

Premier déploiement d'un réseau national dédié à l'Internet des objets

Alain Dantec a, quant à lui, rappelé l'historique de LoRa, solution concurrente de celle de Sigfox, née à la suite de l'acquisition en 2012 de la start-up grenobloise Cycleo par Semtech. Une histoire qui pose la problématique du positionnement stratégique des sociétés de semi-conducteurs dans le contexte du marché prometteur de l'Internet des objets. Elles devront passer d'un modèle de fabricant de semi-conducteurs à celui d'offreur de solutions. *"LoRa offre un compromis en termes de débit et de portée. En 2014, les grands déploiements M2M ont eu lieu pour Veolia avec des applications de télérelevés de compteurs d'eau, puis, cette année, avec la création de LoRa Alliance et le premier déploiement d'un réseau national dédié à l'Internet des objets avec Bouygues Telecom. Nous avons un écosystème complet avec une technologie performante et évolutive, des composants et modules pour les terminaux et l'infrastructure, un protocole de communication LoRaWan, des solutions d'infrastructure avec des passerelles et de gestion du réseau, des opérateurs offrant une large couverture et la possibilité de roaming (KPL, Belgacom, Suisscom en Europe), et enfin, des pourvoyeurs de services"*, détaille Alain Dantec. *"LoRa est une solution prête pour l'Internet des objets, déjà mise en oeuvre sur de multiples réseaux privés, et dont les performances ont été démontrées sur de nombreux réseaux privés à Grenoble, et aux Etats-Unis, en Californie et sur la côte est"*, ajoute-t-il.

Relever le défi de la sécurité

Bouygues a testé la solution LoRa pendant 16 mois. Cette évaluation a permis de qualifier la propreté de bande 868 MHz, l'effet de charge et des interférences, l'ingénierie radio en fonction du nombre de sites et d'antennes par site, le taux de couverture en intérieur, la localisation sans GPS. Philippe Cola précise que les deux solutions techniques Sigfox et LoRa ont été comparées, et que suite à l'expérimentation sur le site pilote de Grenoble, c'est la technologie LoRa qui a été retenue. *"Pour nous, l'Internet des objets est une continuité de services. Bouygues vend du service et non une technologie. Le grand défi à relever est celui de la sécurité et se conçoit dès la conception du réseau"*, souligne-t-il.

Enfin, Eolane est revenu sur le lancement de la Cité de l'objet connecté, née de l'un des 34 chantiers de la Nouvelle France Industrielle. Elle est portée par un groupe d'entreprises industrielles partenaires réunies autour d'Eolane. *"Devant la compétition internationale et face à l'accélération des cycles de production, l'innovation ne peut se faire avec succès qu'en réunissant l'ensemble des savoir-faire de conception, industrialisation et intégration"*, explique Thierry Sachot. La cité de l'objet connecté réunit des compétences et des métiers (concepteurs, assembleurs, sous-traitants de l'électronique, du numérique, de la plasturgie et de la mécanique) pour offrir une fluidité et une rapidité nécessaires à l'innovation. Elle propose des équipements pour réaliser des maquettes pour 300 € par mois et par personne (400 € en y adjoignant un bureau). Ensuite, la phase industrialisation du produit sera réalisée au cas par cas sous forme de devis.

(*) Etude intitulée "The digital universe of opportunities : rich data and the increasing value of the internet of things", publiée par IDC pour le compte d'EMC, un spécialiste américain du stockage.

L'IdO aide les industriels à explorer le futur

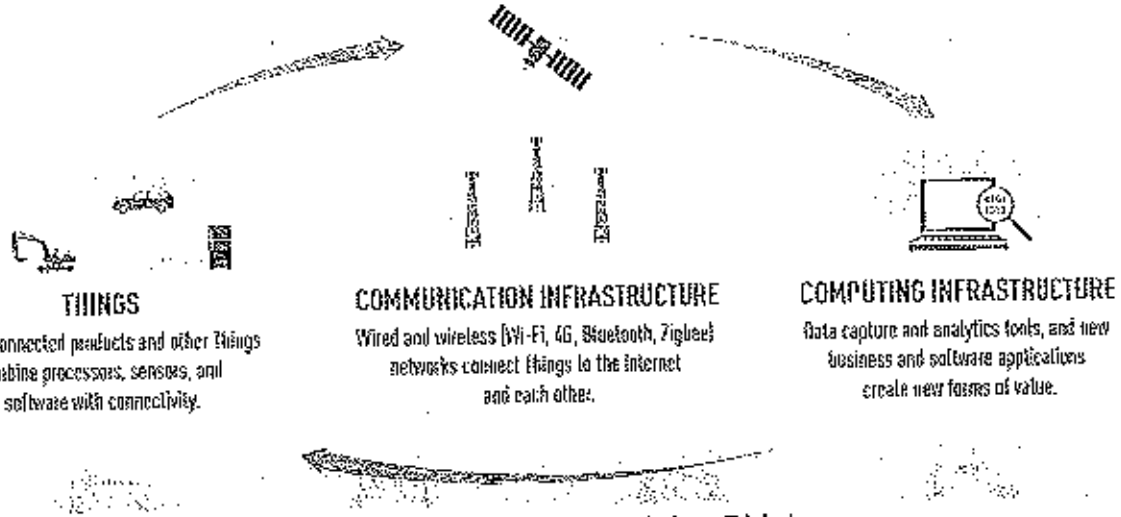
http://fr.ptc.com/internet-of-things juillet 2015

L'expression « Internet des Objets » a été créée pour décrire le nombre croissant de produits intelligents et connectés. Elle reflète les nouvelles opportunités que représentent ces objets.
Le nombre d'objets connectés à Internet dépasse d'ores et déjà la population mondiale. La tendance devrait même s'accélérer pour atteindre les 50 milliards d'appareils connectés d'ici à la fin de la décennie. Pour les fabricants, les répercussions de ce phénomène émergent qu'est l'« Internet des objets » sont immenses.
Selon un rapport récent du McKinsey Global Institute :

- L'Internet des Objets (IdO) représentera une valeur ajoutée potentielle de 6,2 billions de dollars par an pour l'économie mondiale d'ici 2025.
- Il prévoit en outre qu'à cette date, 80 à 100 % des fabricants auront adopté les applications IdO.
- L'impact économique potentiel pourrait atteindre 2,3 billions de dollars pour la seule industrie manufacturière mondiale.

La convergence des forces de marché et l'innovation des technologies opérationnelles a permis le développement de l'Internet des objets.
Pour saisir la balle au bond, les fabricants ont un besoin urgent de repenser presque toute leur activité, de la création des produits à leur exploitation, sans oublier leur maintenance. Quant aux autres, ils verront leur avantage concurrentiel actuel mis à mal.
L'IdO inclut trois composants fondamentaux :

- Des produits intelligents et connectés, des systèmes de produits et d'autres **objets**.
- Ces « objets » sont reliés via des **infrastructures de communication** de type Internet.
- Les infrastructures de communication sont reliées à des **infrastructures informatiques** qui créent de nouvelles formes de valeur.



Les produits intelligents et connectés dans l'Internet des Objets
L'expression « Internet des Objets » a été créée pour décrire le nombre croissant de produits connectés à l'Internet. Elle reflète les nouvelles opportunités que représentent ces objets. Toutefois, cette expression n'aide pas vraiment à comprendre le phénomène et ses implications. L'Internet, qu'il implique des personnes ou des choses, est simplement un vecteur, c'est le mécanisme qui sert à transmettre des informations. Le moteur de la transformation, ce

n'est pas l'Internet, mais la nature changeante des « objets », en d'autres termes, les produits eux-mêmes.

Ce sont les **fonctionnalités** inédites de ces produits intelligents et connectés, ainsi que les données qu'ils génèrent, qui marquent l'avènement de cette nouvelle ère de la concurrence.

- Les produits peuvent accéder à l'environnement et le **surveiller**. Lorsque la pluie commence à tomber, une voiture peut relever ses vitres.
- Une pièce de rechange peut arriver sur site avant même qu'un problème soit signalé parce son **état était suivi**.
- La **commande à distance et en temps réel** d'aéronefs peut offrir aux troupes un « œil dans le ciel » qui les aide à assurer leur sécurité.

Il serait simpliste, voire dangereux, de dire que l'Internet des Objets « change tout ». En même temps que l'Internet lui-même, les produits intelligents et connectés offrent en effet une gamme infinie et nouvelle de possibilités technologiques. Cependant, les règles de la concurrence et l'avantage concurrentiel demeurent les mêmes. Pour naviguer dans le monde des produits intelligents et connectés, encore faut-il comprendre, plus que jamais, les règles qui le sous-tendent.

« La stratégie IdO de PTC et les fonctionnalités liées de gestion du cycle de vie permettront aux entreprises de toutes sortes de proposer de nouveaux produits et services innovants, ainsi que de créer une véritable gestion du cycle de vie en boucle fermée. »

— **Peter Bilello, CIMdata**

Internet des objets: la bataille des futurs standards de communication est engagée

[16]

17 juillet 2015 - 14H05

© AFP/Archives / Par Septime MEUNIER | La première brosse à dents connectée, exposée à Las Vegas le 5 janvier 2014

PARIS (AFP) - http://www.france24.com/fr/20150717-internet-objets-bataille-futurs-standards-communication-est-engagee

Les futurs standards de communication connectant le vaste ensemble de l'internet des objets ne sont pas encore définis et font l'objet d'une âpre bataille, aux enjeux tant techniques et économiques que politiques.

"La communication sur internet se base sur une couche IP (protocole internet, ndlr) qui harmonise à un certain niveau tous les standards existants, mais l'internet des objets possède des protocoles propres à certains métiers et usages, loin de garantir une communication unifiée et sécurisée entre des équipements hétérogènes", résume David Fxcoffier, responsable innovation chez Sogeti.

Pacemaker, voiture, caméra, compteur d'eau, alarme, montre, station météo, drone, brosse à dent, ampoule, maillot de bain: la nature très variée des objets connectés a poussé des entreprises de secteurs divers à former plusieurs alliances internationales.

Officialisé en avril dernier, le consortium LoRa regroupe une soixantaine d'entreprises mondiales parmi lesquelles Cisco ou IBM, et, en France, Bouygues Telecom et Schneider Electric.

Face à elle, la start-up tricolore Sigfox, basée à Toulouse, collabore avec des opérateurs comme Telefonica, SK Telecom et NTT Docomo, entrés à son capital lors d'une levée de fonds de 100 millions d'euros en février.

"Ce sont les deux seuls systèmes matures, mais nous sommes en avance: nos premiers réseaux sont déjà installés, capables dès maintenant de gérer plusieurs milliards d'objets, et ne vont pas tarder à être rentables", assure Christophe Fourtet, co-fondateur en 2009 de Sigfox.

"LoRa est plus performant notamment en termes de flexibilité du réseau", réforque Olivier Roussat, PDG de Bouygues Telecom.

Alors que s'affrontent près d'une dizaine de projets concurrents (Zigbee, Thread, Weightless...), l'Union internationale des télécommunications (UIT), agence des Nations unies, est censée superviser ce processus, en allouant des bandes spécifiques pour les différents usages.

"Au final c'est le marché qui décide, et il ne faudra pas un seul standard, mais au minimum deux ou trois", juge Anne Bouverot, directrice générale de la GSMA, association qui regroupe plus de 800 opérateurs télécoms dans le monde.

"Une chose est sûre, aujourd'hui il est beaucoup plus facile de trouver un financement pour faire de l'internet des objets voire même pour créer son propre réseau qu'à l'époque où on a commencé", affirme Christophe Fourtet.

- La Chine en pointe -

Selon une étude d'avril de l'institut Machina Research, le potentiel du marché mondial de l'internet des objets pourrait atteindre 4.300 milliards de dollars en 2024, une perspective qui aiguise bien des appétits.

"Même si c'est un peu tôt encore, nous regardons en permanence quels types de protocoles en développement les consommateurs voudraient utiliser, pour que nos clients puissent se concentrer sur le fait de construire les applications au lieu de faire le travail de base", explique ainsi Werner Vogels, directeur de la technologie d'Amazon.

Le géant américain du commerce en ligne a acquis en mars 2lemetry, une start-up basée à Denver qui a développé une plate-forme agnostique et décentralisée de gestion des données issues de l'internet des objets.

"Nous faisons partie de consortiums à la fois aux Etats-Unis et en Europe car il est très important que nous travaillions tous sur un standard aussi global que possible, sinon on court le risque d'une fragmentation", prévient Luka Mucic, directeur financier du groupe allemand du logiciel professionnel SAP.

"L'interopérabilité est un enjeu majeur pour répondre aux nouveaux usages dans les bâtiments", renchérit Pierre Laroche, directeur innovation et systèmes du fabricant de matériel électrique Legrand.

"Il faut faire en sorte que les systèmes puissent fonctionner entre eux, et donc au travers d'alliances, comme Confluens, nous mettons en place des langages communs entre marques", détaille-t-il.

Pour Vincent Bonneau, expert de l'Idate, l'IoT aura d'abord un modèle économique viable au travers des applications industrielles.

"Or il y quand même une grosse pression politique à chaque fois dans le choix des technologies comme cela a été le cas en France et au Royaume-Uni sur les compteurs électriques, où ni Sigfox ni LoRa n'ont été retenus".

Une solution pourrait venir de Chine qui, selon un rapport de la GSMA publié mardi, "est à l'avant-garde du déploiement de l'internet des objets".

Via des financements alloués dans le cadre de son dernier plan quinquennal, le gouvernement chinois soutient activement le développement de l'IoT, et promeut, au plan international, les normes établies par ses opérateurs.