Forum des Compétences

Réflexions des établissements financiers du

Forum des Compétences

Crédits photo : Public Domain Mark 1.0

« Objets connectés du quotidien utilisés en entreprise » : risques opérationnels et environnement juridique »

Une étude menée avec

ATiPiC AVOCAT

Technologies
Informations
Propriété
Intellectuelle
Commerce

Composition du Groupe de travail du Forum des Compétences

« Objets connectés du quotidien utilisés en entreprise » : risques opérationnels et environnement juridique

Alicia BERE	Crédit Mutuel-Arkea
Franck BICHET	BNP Paribas Cardif
Xavier BOIDART	Crédit Agricole Assurances
Régis BOURDONNEC	BNP Paribas Cardif
Patrick BRUGUIER	Banque de France
Laurent CHAILLEY	Banque de France
François COUPEZ	Cabinet ATIPIC Avocat
Vianney DERMY	Crédit Agricole Assurances
Jean-Christophe DOUCEMENT	La Banque Postale
Mathieu FERTALA	BNP Paribas
Marie-Annick LE PAGE	Crédit Mutuel-Arkea
Sabine MARCELLIN	Crédit Agricole CIB
Agnès THUILIERE	La Banque Postale

Avec le soutien, et la collaboration constante de M. Wilfrid GHIDALIA, Secrétaire général du Forum des Compétences.

Les membres du groupe de travail tiennent à remercier la société Digital Security pour ses apports à leur réflexion et en particulier M. Cédric Messeguer et M. Thomas Gayet.

Groupe de travail du Forum des Compétences : Objets connectés du quotidien utilisés en entreprise : risques opérationnels et environnement juridique

Document déposé chez

LOGITAS

Forum des Compétences

Sommaire

Préambule

Les entreprises sont de plus en plus nombreuses à réfléchir à l'utilisation d'objets connectés du quotidien (bracelet, montre, casque, lunettes, etc.) par leurs salariés, quand elles n'ont pas déjà sauté le pas. L'objectif est d'apporter un meilleur service, toujours plus personnalisé et plus efficace, à leurs clients. Les aéroports notamment utilisent de plus en plus ce type de technologie[1], comme celui de Québec[2]. De même, les services de préparation de commandes exploitent de plus en plus des objets connectés (GPS et scanners) afin de déterminer le parcours optimal à suivre dans un entrepôt[3].

Si cette face émergée de l'iceberg promet aux clients des banques et des assureurs l'émergence d'un marketing personnalisé de tous les instants (accès immédiat aux données des clients affichées sur la montre, guidage des personnels *via* leur montre vers l'endroit du lieu de vente où ils sont utiles, etc.), il ne faut pas oublier que ces outils ont un usage beaucoup plus large au sein des entreprises, par exemple pour faciliter la maintenance et le bon fonctionnement des différents services ou optimiser la logistique (casque de réalité virtuelle avec téléassistance, etc.).

Parallèlement, les salariés se dotent de tels outils dans le cadre de leur vie personnelle, pour enregistrer leurs performances sportives, ou tout simplement pour améliorer leur confort de vie par une connectivité toujours renforcée, ces outils pouvant prendre les formes les plus diverses (bracelets, montres, balances, caméras, drones, voitures… voire tatouages si l'on s'intéresse aux travaux de Microsoft et du MIT[4]).

Les chiffres sont là, même si il est difficile de savoir ce que l'on entend exactement par ce terme d'« objet connecté », les prévisions de Gartner annoncent plus de 20 milliards d'objets connectés en 2020[5], alors qu'il n'y en avait que 900 millions en 2009, quand d'autres en prévoient peut-être dix fois plus (cf. IDC avance le chiffre de 212 milliards).

Si l'on regarde le seul marché des montres connectées, des bracelets et des traqueurs d'activité, la croissance du marché en 2015 a dépassé les 67 % ; les quatre premiers acteurs mondiaux, Xiaomi, Apple, Fitbit et Garmin, ont livré à eux seuls plus de 11 millions d'unités en 2016 selon IDC[6], alors que l'ensemble des

[1] L'enquête annuelle pour 2014 réalisée par la SITA (Société Internationale de Télécommunications Aéronautiques) auprès de passagers autour du globe a montré que 77 % des 6 277 passagers interrogés accepteraient avec plaisir l'utilisation d'objets connectés du quotidien (montres, lunettes, etc.) par les personnels de l'aéroport ou de compagnies aériennes si cela permet de mieux les assister pendant leur voyage.

[2] Les directeurs de service reçoivent sur leurs montres connectées des alertes sur la sécurité des lieux (arrivée simultanée de deux avions qui ont été dirigés vers la même porte, attente à une certaine porte, etc.) *via* une vibration, ce qui permet de les prévenir quasi instantanément. Selon le vice-président des technologies de l'information de l'Aéroport de Québec, « *l'employé n'a plus qu'à y jeter un coup d'œil pour connaître l'information critique et prendre une décision sur-le-champ* ». Cf. http://www.journaldequebec.com/2015/06/17/les-premiers-employes-aeroportuaires-au-monde-a-utiliser-lapple-watch-seront-ceux-de-quebec.

[3] Wearable technologies creeps into the workplace : http://www.bloomberg.com/news/articles/2015-08-07/wearable-technology-creeps-into-the-workplace.
Amazon is looking for the perfect warehouse worker. Cf http://www.bloomberg.com/news/articles/2015-05-28/robot-with-a-human-grasp-is-amazon-s-challenge-to-students.

[4] http://www.objetconnecte.com/tatouages-connectes-mit-microsoft-2208/.

[5] http://www.gartner.com/newsroom/id/3598917.

[6] http://fortune.com/2017/09/01/idc-apple-android-smartwatch-wearables/

ventes avoisine les 20 millions d'unités. La France, quant à elle, a lancé un plan industriel « objets connectés » en 2014, et a identifié la problématique comme l'une des 34 priorités de la politique industrielle.

Inéluctablement, la question des usages que ces objets connectés permettent en entreprise se pose aujourd'hui, non seulement vis-à-vis des fonctionnalités qu'ils offrent (enregistrement toujours plus discret et complet, etc.), mais également au regard de la demande possible d'interconnexion avec le système d'information de l'employeur, afin que le salarié puisse utiliser une seule montre ou une seule paire de lunettes à des fins personnelles comme à des fins professionnelles.

Or les problématiques juridiques et sociétales liées à ces usages se révèlent nombreuses, d'autant que l'étude des données collectées par ces objets, ou encore des traitements réalisés, nécessite un focus particulier au regard de la réglementation applicable ainsi que de celle en cours de construction. Surtout, dans la mesure où le taux d'équipement par le grand public croît sans cesse, toutes les tailles d'entreprises sont aujourd'hui concernées. **Les enjeux liés à la sécurité restent encore sous-estimés. Pourtant, ils sont majeurs : la conception faillible de ces objets ouvre la voie à des incidents de sécurité toujours plus nombreux**. Le fondateur de la conférence Black Hat, Jef Moss, a ainsi rappelé le 5 août 2015 que « *presque aucun des fabricants d'appareils n'a de véritable équipe dédiée à la sécurité* » [7] alors qu'une étude IDC prévoit qu'au cours des 2 prochaines années, 90% des réseaux informatiques auront subi au moins une brèche liée à l'internet des objets[8].

De façon plus prosaïque, le piratage en juillet 2015 d'une Jeep via son système d'assistance à la conduite a attiré l'attention sur ce problème, qui est toutefois beaucoup plus large et concerne toutes les fonctionnalités offertes par ces objets (piratage des données de localisation, des données collectées, prise de contrôle des vidéos enregistrées, etc.). L'attention du public n'a depuis fait que croître ; à titre d'exemple, la presse généraliste a largement relayé les révélations au sujet des télécommandes de verrouillage à distance de près de 100 millions de voitures dans le monde, qui n'offriraient qu'une résistance toute relative aux pirates informatiques[9]… ce qui explique le boom des vols sans effraction.

De l'ampoule électrique[10] à l'avion de ligne en vol[11] en passant par la serrure connectée[12] et le pacemaker[13], tout matériel où l'informatique est présente peut se

---

[7] http://www.centrepresseaveyron.fr/2015/08/06/securite-un-piratage-de-voiture-illustre-les-dangers-des-objets-connectes,968709.php

[8] IDC's 2015 Global IoT Decision Maker Survey réalisée en juillet et août 2015 auprès de 2 350 personnes.

[9] http://automobile.challenges.fr/actu-auto/20160811.LQA8419/volkswagen-particulierement-touche-par-le-piratage-des-telecommandes.html, http://www.lefigaro.fr/conjoncture/2016/08/11/20002-20160811ARTFIG00196-les-cles-de-voitures-de-100-millions-de-vehicules-facilement-falsifiables.php

[10] Cf. l'hypothèse de piratage d'un réseau local via les ampoules électriques connectées http://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?ref=technology&_r=1

[11] L'américain Chris Roberts a ainsi démontré avoir pris le contrôle d'un avion en vol, ce qui avait entraîné son interpellation par le FBI dès son atterrissage. Patrick Ky, directeur de l'AESA (Agence Européenne de la Sécurité Aérienne), a par la suite déclaré que « *l'aviation est vulnérable à la cybercriminalité* » (http://www.usinenouvelle.com/article/pirater-le-systeme-de-controle-d-un-avion-c-est-possible-selon-l-agence-europeenne-de-la-securite-aerienne.N355862).

[12] Anthony Rose a démontré à la DefCon de LasVegas le 8 août 2016 que 12 des 16 serrures qu'il avait testées sont très mal (voire pas du tout) sécurisées, cf. http://www.usine-digitale.fr/article/smart-home-les-serrures-

connecter à un réseau externe et est susceptible de poser de graves problèmes de sécurité. Ainsi, pour le directeur de l'Agence européenne de la sécurité aérienne (AESA), Patrick Ky, qui a lui-même fait mener des attaques réussies en situation réelle sur des avions, « *en matière de cybersécurité, n'importe qui peut s'introduire n'importe où. Des hackers ont même réussi récemment à entrer dans le centre de commandes des drones américains* »[14].

D'ailleurs, le Département de la Justice des Etats-Unis a rendu public début septembre 2016 l'existence d'un groupe, créé 6 mois auparavant, dédié à la sécurisation de « l'internet des objets » vis-à-vis d'une exploitation terroriste qui pourrait en être faite. Ce groupe s'intéresse notamment aux voitures autonomes, aux appareils médicaux et aux autres objets connectés liés à la sécurité nationale[15]. Plus récemment, prenant la suite des affaires des *babyphones*[16], c'est le piratage de centaines de milliers d'objets connectés du quotidien (webcams, enregistreurs vidéo, etc.), permis grâce à des failles de sécurité (et la libre diffusion du code source d'un malware qui les exploite), qui a conduit à plusieurs reprises à des attaques d'entreprises, *via* des dénis de service distribués à grande échelle[17]. Certains sénateurs appartenant à ce groupe ont déposé le 1er août 2017 un projet de loi visant à « améliorer la cybersécurité de l'Internet des objets », actuellement en cours d'examen[18].

En parallèle, Shodan.io, le moteur de recherche dédié au référencement d'objets connectés à Internet, connaît toujours plus de connexions, alors qu'il continue à lister tout type d'objets, de ceux du grand public aux systèmes SCADA[19]. Il donne des éléments d'information sur leurs vulnérabilités et l'exploitation de ces dernières.

La vulnérabilité d'un objet connecté peut ainsi soit conduire à l'attaque facilitée du système d'information d'un tiers, soit devenir une porte d'entrée pour altérer le système d'information d'une entreprise, avec des conséquences potentiellement majeures : paralysie des objets connectés (imprimantes, portes, caméras, ordinateurs, etc.), voire de tout ou partie du système d'information, vol de données, chantage (dans le cas de données « retenues en

---

connectees-peuvent-etre-ouvertes-par-n-importe-qui.N422562. D'autres hackers, également à cette DefCon, ont prouvé que sur 23 objets connectés (réfrigérateurs, thermostats, fauteuil roulant, etc.) fabriqués par 21 entreprises différentes, 47 vulnérabilités existaient, dont l'utilisation de mots de passe non chiffrés et programmés « en dur » (http://www.objetconnecte.com/def-con-objets-connectes-failles-140916/).

[13] http://tempsreel.nouvelobs.com/tech/20170831.OBS4051/risque-de-piratage-un-demi-million-de-pacemakers-a-mettre-a-jour.html

[14] http://www.usinenouvelle.com/article/pirater-le-systeme-de-controle-d-un-avion-c-est-possible-selon-l-agence-europeenne-de-la-securite-aerienne.N355862.

[15] http://www.reuters.com/article/us-usa-cyber-justice-idUSKCN11F2FP.

[16] Le collectif Rapid7 a ainsi réalisé en 2015 un rapport très critique concernant la forte vulnérabilité des babyphones, disponible sur https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf. Ce rapport fait écho à un fait divers de 2013, aux Etats-Unis, où la caméra sans-fil installée afin de surveiller un bébé avait été piratée en pleine nuit, le hacker ayant alors littéralement insulté le bébé, réveillant les parents imprudents (http://www.ladepeche.fr/article/2014/04/29/1872578-etats-unis-un-babyphone-pirate-terrifie-toute-une-famille.html).

[17] Plus puissante attaque par DDOS d'OVH, via 145 607 webcams du 18 au 23 septembre 2016, attaque de Dyn le 21 octobre 2016 ayant conduit à rendre difficile, voire impossible l'accès Twitter, Spotify, Reddid, Airbnb, Paypal, le PlayStation Network, Netflix, etc.

[18] https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices

[19] Selon Wikipedia, un système de contrôle et d'acquisition de données (anglais : Supervisory Control And Data Acquisition, sigle : SCADA) est un système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques.

otage » par exemple si elles sont altérées ou chiffrées), impossibilité de poursuivre normalement l'activité, etc.

Sur ces questions, tout le monde est concerné, de l'entreprise à l'utilisateur en passant par le salarié ou le client, compte tenu du caractère transversal de l'utilisation des objets connectés.

Les objets connectés envahissent l'entreprise, soit que cette dernière ait décidé d'en faire usage, soit que les salariés apportent leurs propres objets connectés dans le cadre professionnel. Face à l'imminence de « *cette réalité augmentée du Bring your Own Device*[20] », les entreprises doivent anticiper dès à présent pour leur permettre de connaître plus aisément les différents principes applicables à cette future réalité et d'adapter au mieux la sécurité des systèmes d'information. Le Forum des Compétences a souhaité les y aider. Rappelons que le Forum des Compétences est une association d'établissements financiers qui échangent dans le domaine de la sécurité des systèmes d'information. Ce groupe de réflexion et de recherche réunit des banques, sociétés d'assurance et régulateurs français.

Le Forum des Compétences a ainsi souhaité confier à un groupe de travail le soin de proposer des éléments de réponse, pour anticiper au mieux cette réalité émergente. Le groupe, associant juristes et spécialistes de la sécurité des systèmes d'information de grands établissements de la Place et assisté par le cabinet d'avocats ATIPIC Avocat, a élaboré le présent document de synthèse afin de les y aider.

Ce document est conçu pour apporter un éclairage aux décideurs, aux professionnels de la sécurité de l'information et aux juristes qui participent aux processus de gestion du risque dans les entreprises. Cet éclairage synthétique ne pourra qu'être enrichi par l'expérience et les avis des professionnels de chaque Etablissement concerné lors de la mise en œuvre de projets d'objets connectés spécifiques.

[20] Sur cette question, voir notamment les précédents travaux du Forum des Compétences – *« Les Terminaux personnels en Entreprise – FAQ »*, disponible sur http://www.forum-des-competences.org/index.php?action=download_resource&id=579&module=resourcesmodule&src=%40random5198dba8b1f0b.

Synthèse des conclusions du présent document

Les 6 points à connaître :

- Un objet connecté peut être **défini** comme un objet électronique du quotidien qui, *via* l'ajout de fonctions supplémentaires et en les reliant à un réseau (en permanence ou non), permet de récupérer et de traiter des informations ou d'automatiser des actions de la vie quotidienne ;

- Un objet connecté traite très souvent dans la pratique des données à caractère personnel, ce qui entraîne l'application du très strict **RGPD** (Règlement Général sur la Protection des Données). Si ce sont des **données de santé**, le régime est plus strict que pour d'autres types de données à caractère personnel. Si l'objet connecté traite **d'autres types d'information**, il ne faut pas en déduire qu'aucune réglementation n'est susceptible de s'appliquer à ces données ;

- Les données de **géolocalisation** requièrent également une attention particulière de la part de l'entreprise ;

- **Les objets connectés souffrent fréquemment d'une sécurisation insuffisante mettant en risque leurs utilisateurs** (exploitation indue des données, détournement, etc.) et la sensibilisation des nombreux acteurs du domaine est cruciale pour changer cet état de fait ;

- Les contraintes réglementaires, qui imposent de façon directe ou indirecte cette sécurisation, renforcent la nécessité pour les entreprises de suivre les bonnes pratiques en matière d'analyse des risques et de mise en œuvre de solutions sécurisées. **Les sanctions peuvent aller jusqu'à 4 % du chiffre d'affaires mondial consolidé**…

- Au-delà de la question des données traitées par les objets connectés, l'objet en lui-même, ainsi que la façon dont il est utilisé sont l'objet de règles juridiques à connaître, qui ne sont pas spécifique à un objet connecté mais s'appliquent de façon transversale : question de **l'évaluation des risques de santé** en cas d'usage imposé à un salarié, de **l'impossibilité de brouiller** les émissions de ces objets sans commettre de faute pénal, de la **répression applicable en cas de piratage** de ceux-ci, ou encore la question de la **force probante que l'on peut attendre de leurs enregistrements**).

Les 5 principaux risques :

- le **vol** (notamment à des fins de divulgation), l'écoute ou l'interception de données « à forte valeur » : données de géolocalisation, de bien-être, de santé, données bancaires, etc. ;

- la **falsification** des données échangées ;

- la **mise hors service**, notamment à des fins de chantage ou d'extorsion (blocage du système de climatisation en plein été, du système de démarrage de la voiture, etc.) ;

- la **prise de contrôle** et le **détournement de finalité** de l'objet connecté : minage

de bitcoin, piratage pour mise en réseau parmi d'autres objets connectés permettant une attaque par déni de service distribuée (DDoS), etc. ;

- la **fuite d'informations confidentielles** relatives à l'entreprise ou de données à caractère personnel.

4 recommandations à garder en tête :

- **Réaliser des analyses de risque poussées** en ce qui concerne les scénarios et les conséquences **non seulement pour l'entreprise mais également pour les personnes** dont les données à caractère personnel seraient traitées ;

- **Intégrer l'objectif de sécurité dès le début du projet et pendant toute sa durée en parallèle, si des données à caractère personnel sont traitées, avec la notion de *Privacy by design*, y compris en mode agile** ;

- **Responsabiliser tous les acteurs concernés**, qu'ils soient partenaires ou sous-traitants de l'entreprise, notamment par le biais d'un sourcing exigeant ;

- **Réfléchir aux impacts dès la mise en œuvre d'un projet imposant une large utilisation des objets connectés par les salariés pour l'accomplissement de leur mission… ainsi qu'organiser la cohérence avec l'irruption des objets connectés personnels dans l'entreprise**.

1 - Ce qu'on entend par « objet connecté du quotidien utilisé en entreprise »

Face au « buzz » médiatique autour du terme « objet connecté » ou de celui très proche « Internet des objets », le groupe de travail s'est tout d'abord interrogé sur le cadre précis de la problématique étudiée, et sur la définition des termes employés.

Or, il apparaît que si les tentatives de définition de ces concepts sont nombreuses, les objets connectés n'ont pas de définition officielle du fait de la grande différence entre les objets qui peuvent disposer d'une communication ou d'une connexion. De ce fait, le groupe de travail a décidé de construire sa propre définition à l'occasion de la présente étude, après avoir rassemblé et étudié de nombreuses définitions existantes (indiquées en annexe 2 pour l'information du lecteur intéressé).

Le présent document abordera donc la question des objets électroniques du quotidien qui, *via* l'ajout de fonctions supplémentaires et en les reliant à un réseau (en permanence ou non), permettent de récupérer et de traiter des informations ou d'automatiser des actions de la vie quotidienne. Ces informations sont des données issues du monde physique (pression, température, rythme cardiaque, distance parcourue, localisation, etc.). Par « utilisation dans la vie quotidienne », on entend les catégories suivantes : domotique, santé, bien-être et accessoires (montres, balance, interrupteur lumière, drone, véhicule, tondeuse, vêtement, tatouage…). Cependant, et pour permettre de dégager la spécificité de ces outils, le groupe a

décidé d'exclure de cette définition les ordinateurs tels que le grand public les conçoit (ordinateurs dits fixes ou « desktops » et ordinateurs dits portables ou « laptops ») ainsi que la catégorie de ce que l'on appelle actuellement les « tablettes » ainsi que les « smartphones » dans le format qu'on leur connaît habituellement (3,5 pouces et supérieurs). Le groupe a de même exclu les périphériques informatiques tels qu'on les connaît et conçoit encore classiquement (imprimante, webcam, clavier…).

On le voit, la catégorisation de l'objet de notre étude peut apparaître quelque peu artificielle. **Elle montre surtout que les fonctionnalités informatiques (traitement de l'information, mémorisation, interconnexion entre systèmes, langage informatique commun) nécessitent des supports de taille toujours plus réduite et qu'elles peuvent donc être insérées dans potentiellement n'importe quel objet du quotidien pour le transformer en capteur intelligent et interactif. Cela conduit à évaluer sous un jour nouveau des problématiques qui étaient auparavant physiquement limitées par les objets.**

Notre définition rejoint notamment celle proposée par l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) en ce que les deux approches mettent l'accent sur la communication des objets physiques avec des plateformes de traitement de données[21].

Un premier exemple simple et d'actualité est la commercialisation en automne 2016 de lunettes de soleil connectées par Snap (ex-Snapchat) permettant de filmer des séquences de 10 secondes avec un angle de vue de 105°, intégrant un module de mémoration et des connexions réseau de type Bluetooth ou Wifi[22].

Allant plus loin dans ce processus de miniaturisation, Google s'intéresse à des lentilles corrigeant bien entendu la vision, mais disposant surtout d'un espace de stockage, de radio, de capteurs et d'une batterie. Ces lentilles connectées seraient insérées chirurgicalement *via* une forme de colle. Sony et Samsung travaillent également sur des projets de lentilles, permettant quant à elles de prendre des photographies et des vidéos grâce à un simple clignement de l'œil ou encore disposant de capteurs de mouvement en réalité augmentée.[23]

L'objet de cette étude est volontairement cantonné aux objets connectés du quotidien (lunettes, casques, montres, etc.) ayant une utilisation dans le monde professionnel et en particulier dans l'entreprise, **car c'est l'interaction des deux mondes qui, selon nous, cristallise les problématiques les plus intéressantes.**

Celles-ci seront abordées pour mettre en avant les problématiques juridiques ainsi que celles liées à la sécurité des systèmes d'information.

Enfin, la question de l'insertion ou non de la voiture dans le cadre de cette étude a donné lieu à de nombreux échanges au sein du groupe de travail, notamment en ce

[21] ARCEP, *Préparer la révolution de l'Internet des Objets*, 7 novembre 2016 : « *Dans le cadre de ce rapport, une acception large du terme internet des objets sera retenue, correspondant à un ensemble d'objets physiques connectés qui communiquent via de multiples technologies avec diverses plateformes de traitement de données, en lien avec les vagues du cloud et du big data ».*

[22] http://www.usine-digitale.fr/article/snapchat-devient-snap-inc-et-se-lance-dans-les-objets-connectes.N441637.

[23] cf. Les Echos, le 02/05/2016 : http://www.lesechos.fr/02/05/2016/lesechos.fr/021895327848_google-imagine-des-lentilles-de-contact-implantables-dans-l-oeil.htm.

qui concerne les produits et services permettant indirectement le meilleur respect des règles (dans le cadre d'assurance conducteur avec le « *pay how you drive* »), mais aussi la question des voitures autonomes, la CNIL ayant par exemple annoncé le lancement de travaux visant à réaliser un pack de conformité « véhicule connecté »[24] afin de privilégier une « *démarche positive de « privacy by design »* » (sur cette notion de *privacy by design* voir nos développements ci-dessous (partie 3)).

De façon générale, le groupe de travail a considéré qu'au-delà de l'étude de tel ou tel objet connecté, l'important était plutôt de se focaliser sur le type de données produites ou manipulées par ces objets (quelles sont les données enregistrées, où sont-elles transmises, comment sont-elles traitées, qui en est propriétaire, qui est le porteur, sont-elles enrichies et comment ?, etc.).

2. Données « collectées », données « connectées », données « personnelles » ?

Les objets connectés sont susceptibles de collecter, d'analyser et de transmettre un grand nombre de données. Le groupe de travail a choisi d'analyser le type de données susceptible de faire l'objet de tels traitements, et d'en souligner les conséquences.

Quelles sont ces « data » ? A qui appartiennent-elles ?

2.1 – Quelle qualification juridique pour ces données ?

Rappelons certains éléments ou distinctions fondamentales qui expliquent l'application de corps de règles spécifiques :

- Une donnée se définit comme « *la représentation conventionnelle d'une information donc d'un (élément de connaissance) sous une forme convenant à son traitement par ordinateur* » pour être conservée, traitée ou communiquée[25].

- « *Toute information se rapportant à une personne physique […] (ci-après dénommée «personne concernée») ; […] qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* »[26], est une donnée à caractère personnel au sens du règlement européen 2016/679 dit « Règlement général sur la protection des données » (ou RGPD[27]) du 27 avril 2016, qui remplacera, au 25 mai 2018, la loi du 6 janvier 1978 ;

[24] Voir à sujet https://www.cnil.fr/fr/en-route-vers-un-pack-de-conformite-consacre-aux-vehicules-connectes.
[25] Cf. les définitions de « donnée » et d'« information » – dictionnaire Larousse.
[26] Article 4 1° du RGPD.
[27] RGPD : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de

- Comme nous le verrons, il existe des catégories particulières de données[28] , Par exemple celles relatives à la santé d'une personne. Ces données sont particulièrement protégées par le législateur aussi bien français que communautaire ;

- Par ailleurs, quand ces données concernent les clients d'un établissement de crédit ou d'un assureur[29], elles sont soumises à l'obligation légale de secret professionnel imposée à ces acteurs économiques. Outre cette obligation de secret (issue des articles 226-13 du Code pénal[30] et L. 511-33 I du Code monétaire et financier[31]), les établissements de crédit sont également tenus au respect des dispositions de l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution (ACPR). Il prévoit dans son article 89 c), spécifique au contrôle des systèmes d'information, que « *l'intégrité et la confidentialité des informations sont en toutes circonstances préservées* » ; Enfin, les traitements automatisés produisant des conséquences juridiques ou des effets significatifs sur les personnes concernées[32], du fait de leur nature, sont soumis à des obligations renforcées en matière de protection des données. C'est par exemple le cas des traitements de *scoring* (segmentation de population sur la base de critères) opérés par les établissements de crédit dans la mesure où ils sont susceptibles d'exclure les personnes du bénéfice d'un contrat.

- Certaines données ne présentent pas de caractère personnel : celles relatives aux mesures climatiques ou atmosphériques, à l'état d'un matériel appartenant à l'entreprise, les données financières concernant la vie d'une entreprise, etc. La règlementation en matière de protection des données ne leur est pas applicable. Elle ne s'applique pas non plus aux données statistiques, ni aux données à caractère personnel anonymisées de façon irrémédiable, c'est-à-dire sans espoir de réidentification.
  Il serait pourtant faux de croire que le traitement de ces données non personnelles ou qui ne sont plus personnelles est parfaitement libre et peut être opéré par l'entreprise sans aucune contrainte. Outre ce que la donnée peut révéler sur une personne (ce qui est le fondement de la protection par la loi du 6 janvier 1978 et du RGPD), elle représente d'une part une connaissance et d'autre part une **valeur**, liée à cette connaissance. D'autres textes sont alors susceptibles de s'appliquer, s'attachant dans le premier cas à la protection de la confidentialité de cette connaissance (cf.

---

ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) dit Règlement général sur la protection des données.

[28] Cf : article 9 du RGPD

[29] Hypothèse des lunettes connectées d'un chargé de clientèle lui affichant l'historique d'un client se trouvant en face de lui.

[30] « *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende.* »

[31] « *Tout membre d'un conseil d'administration et, selon le cas, d'un conseil de surveillance et toute personne qui à un titre quelconque participe à la direction ou à la gestion d'un établissement de crédit, d'une société de financement ou d'un organisme mentionné aux 5 et 8 de l'article L. 511-6 ou qui est employée par l'un de ceux-ci est tenu au secret professionnel* ».

[32] Article 22 du RGPD.

directive sur le secret des affaires[33]) et dans le second cas à la protection de cette valorisation (*via* le droit dit *sui generis* des producteurs de bases de données[34]).

2.2 – A qui appartiennent ces données ?

La connaissance est valorisable par essence. La question se pose dès lors de savoir si la propriété d'un objet connecté entraîne *de facto* celle des données produites par cet objet. Les données, produites par les objets connectés appartenant à une entreprise, appartiennent-elles donc à cette entreprise ? Font-elles partie de son patrimoine informationnel ?

Tout dépend des données considérées, qui peuvent être divisées en trois catégories :

- Si les données collectées par l'entreprise ne concernent, par exemple, que des données statistiques, liées aux grandeurs physiques des événements naturels, à la mobilité urbaine ou encore au suivi des marchandises produites (météorologie, déplacement de foule, gestion des stocks, etc.), les données sont gouvernées par l'existence des textes susmentionnés protégeant le producteur de la base de données ou le détenteur de l'information secrète. Très souvent en pratique, ces données appartiennent donc à leur producteur et/ou à leur détenteur.

- Si ce sont des « données à caractère personnel » (cf. la définition précisée au 2.1 ci-dessus), elles font partie en France des **droits de la personnalité** (droit à l'image, droit à la protection de la vie privée, protection des données à caractère personnel, droit moral de l'auteur, etc.). Elles sont à ce titre en principe inaliénables et incessibles (elles ne peuvent être ni vendues, ni cédées). Le législateur, concernant ces données, a prévu un principe fort d'autodétermination informationnelle[35] : étant donné que ces données font partie de ma personnalité, elles me caractérisent, je peux les contrôler et décider de l'usage qui en sera fait, mais elles ne « m'appartiennent » pas au sens juridique du terme, tout comme l'on peut être titulaire de son nom sans pourtant pouvoir en disposer pleinement, c'est-à-dire le vendre ou le louer par exemple.

[33] Directive n°2016/943 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites.

[34] Le législateur a entendu protéger le contenu de la base de données au titre d'un droit spécifique lorsque la constitution, la vérification ou la présentation d'une base de données atteste d'un investissement financier, matériel ou humain substantiel (articles L. 341-1 et suivants du Code de propriété intellectuelle). Ces textes confèrent au « producteur de la base de données » un monopole d'exploitation, autrement dit le pouvoir d'interdire ou d'autoriser à tous tiers le fait d'extraire ou de réutiliser indûment tout ou partie de sa base de données :

- soit les données les plus importantes de la base (article L. 342-1 du Code de propriété intellectuelle) ;
- soit les données qui le sont moins, si l'extraction ou la réutilisation est répétée, systématique, et que cette extraction ou réutilisation excède manifestement les conditions d'utilisation normale de la base de données (article L. 342-2 du Code de propriété intellectuelle).

[35] Article 1 de la loi Informatique et Libertés modifié par la loi n°2016-1321 du 7 octobre 2016.

Dès lors, il n'y a pas de « propriétaire » de données à caractère personnel, ni du côté de ceux qui ont mis en œuvre les moyens techniques permettant de les générer, ni du côté des personnes ayant été la source de cette collecte. Dans un cas, on parlera simplement de « responsable de traitement » et, dans l'autre, de « personne concernée » ou encore de « titulaire de ces données ». Si le responsable de traitement peut par exemple céder les données qu'il a collectées, ce n'est que sous réserve du respect strict du cadre légal en matière de protection des données, et notamment du respect des droits de la personne concernée qui peut s'opposer, pour des motifs légitimes, à cette collecte ou à cette exploitation, voire sans avoir à en justifier dans le cas d'une utilisation à des fins de prospection commerciale (art. 38 de la loi du 8 janvier 1978 et article 21 du RGPD). D'ailleurs, la Chambre commerciale de la Cour de cassation a récemment reconnu qu'un fichier de données à caractère personnel établi sans déclaration préalable à la Commission Nationale Informatique et Libertés (CNIL)[36] est *de facto* illicite. Considéré comme « hors du commerce » par les magistrats, il ne peut donc être vendu[37].

- Enfin, on constate de plus en plus que, du fait de la multiplication des capteurs et des objets connectés, des informations auparavant purement statistiques ou complètement indépendantes de tout comportement humain et non identifiantes s'avèrent de plus en plus individualisées, ce qui permet *in fine*, en les croisant avec d'autres d'identifier une personne physique : ces informations deviennent de ce fait des données à caractère personnel. Un parallèle peut être tracé avec d'autres données collectées et analysées par nombre d'objets connectés, les « données de bien-être », qui se rapprochent de plus en plus des « données de santé » (voir ci-dessous un exemple des effets de la corrélation sur le type de données).

2.3 - Les « données de santé » vs les « données de bien-être » : le rôle de la finalité du traitement

Pour l'heure, il n'existe pas encore de définition légale opposable relative aux données de santé. Cependant, le RGPD, qui sera applicable le 25 mai 2018, donne une définition des « données concernant la santé » qu'il convient de prendre en compte dès à présent. Ainsi les « données concernant la santé » sont définies à l'article 4 15) comme des « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».

Le principe posé est celui d'une vision relativement stricte de la notion de « données de santé » qui laisse de la marge aux « données de bien-être ». Ces deux types de données sont tous deux des données à caractère personnel[38], mais les « données

[36] Obligation imposée par l'article 22 I de la loi Informatique et Libertés.

[37] Décision du 25 juin 2013 de la Chambre commerciale de la Cour de cassation, disponible ici : https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000027632440.

[38] Cf. Considérant 35 du RGPD, chaque considérant d'un texte européen ayant une valeur forte pour guider l'interprétation dudit texte : « *Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de*

de bien-être » sont soumises à un régime bien moins rigide que les données de santé *stricto sensu,* qui sont des données sensibles dont le traitement est interdit, sauf exceptions prévues par la loi (assurer le suivi médical de la personne par exemple).

En pratique, et selon leurs concepteurs, des capteurs connectés peuvent ainsi collecter des constantes afférentes au fonctionnement biologique d'une personne (pouls, température, etc.) sans que celles-ci ne révèlent forcément l'état de santé d'une personne. Si l'on dresse un parallèle avec la sécurité routière, la situation est comparable à celle de l'avertisseur de la présence d'un radar, dont la détention est interdite en France, alors que l'assistant d'aide à la conduite, évoquant la catégorie plus large de « zone de danger », étant quant à lui encore légal (ce qu'a remis en question un projet de décret d'avril 2017, qui n'est pas encore entré en vigueur au 25 septembre 2017[39]).

Pourtant, tout comme l'« avertisseur de danger » peut révéler dans certaines circonstances la présence quasi-certaine de radars[40], certaines situations tendent à transformer d'objectives « données de bien-être » en bien plus précises « données de santé ». Ainsi, un bracelet captant le pouls et révélant des mesures apparemment incohérentes (deux pouls avec des rythmes distincts) peut indiquer à sa porteuse l'existence d'une grossesse[41], donnée de santé s'il en est.

La frontière entre données à caractère personnel d'un côté et données qui ne le sont pas de l'autre tend à se réduire en fonction de l'usage qui sera fait des données et du type de traitement qui leurs sera appliqué. Il importe de bien définir la « finalité des traitements », c'est-à-dire l'objectif de la collecte et de l'utilisation des données, qui conditionne le cadre juridique applicable (champ de l'information dû à la personne concernée, périmètre des droits qui lui sont accordés, etc.) et structure l'analyse[42] : c'est en fonction du type de données collectées d'une part, et de la finalité de la collecte que les risques liés à ce traitement pourront être analysés et que les mesures de sécurité appropriées pourront être mises en œuvre. A ce titre, l'essor de technologies telles que le Big Data ou, pour ce qui nous occupe, les objets connectés, est de nature à augmenter les risques potentiels en fonction de leurs conditions de mise en œuvre.

---

bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro. »

[39] http://ec.europa.eu/growth/tools-databases/tris/fr/search/?trisaction=search.detail&year=2017&num=160.

[40] Exemple d'une « zone de danger » annoncée sur une autoroute parfaitement droite en pleine journée et sans un véhicule en vue : l'automobiliste attentif y décèlera une probabilité importante que le danger soit en réalité spécifiquement un radar.

[41] http://www.rtl.be/info/magazine/hi-tech/une-femme-decouvre-qu-elle-est-enceinte-grace-a-son-bracelet-connecte--793506.aspx.

[42] Ce qui explique l'application de sanctions lourdes en cas de détournement de cette finalité, prévues dans la loi de 1978, mais également dans le RGPD en vigueur en mai 2018.

Le fait pour certains personnels de disposer d'un « indicateur de verticalité » illustre bien cette notion centrale de finalité. En effet, qu'une société de conseil impose à tous ses salariés le port d'un « indicateur de verticalité » dans ses locaux n'aurait pas grand sens et de ce fait ne permettrait pas d'étayer une finalité licite et objective pour cette mise en œuvre : veut-on lutter contre les siestes sauvages ? A l'inverse, le port de ce type de dispositif implanté dans un objet connecté, à l'instar d'une montre, peut parfaitement se concevoir au regard du principe de finalité pour certains salariés. Par exemple, pour un salarié restant seul afin d'éviter qu'il ne soit victime d'un malaise (agent EDF en intervention, conseiller de clientèle seul dans son agence, etc.), dès lors que ce moyen apparaîtrait comme la meilleure solution à tous égards (conformément au principe de proportionnalité cher à la réglementation sur la protection des données).

Une dernière notion semble fondamentale à mentionner : celle de consentement des personnes concernées au traitement de leurs données. Il est défini dans le RGPD comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* » [43]. Ce consentement est requis dans un certain nombre de cas (notamment le cas des traitements ayant des conséquences significatives pour la personne concernée). Mais, et ceci rejoint directement le fait que ces données soient « hors commerce », le consentement ne peut tout permettre et ne peut tout autoriser, à la différence d'autres systèmes juridiques. La loi protège la personne concernée en considérant dans certains cas que son contentement ne peut, en tout état de cause, être valable. C'est notamment l'interprétation de la CNIL et du groupe dit « de l'article 29 » ou G29[44] concernant le consentement donné par un salarié à son employeur sur un traitement de données : il est considéré comme non valide par hypothèse, car n'étant pas « libre » de toute pression hiérarchique.

2.4 - L'impératif réglementaire de protection des données à caractère personnel

Rappelons que l'article 32 du RGPD, reprenant en cela le contenu de l'article 24 de la loi du 6 janvier 1978, impose au responsable de traitement, sous peine de sanctions notamment pénales, une obligation de sécurité et de confidentialité des données. Ce dernier doit prendre « *toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

Si les sanctions pénales ont été très rares depuis 1978 (sur cette question, les lecteurs intéressés pourront se référer aux précédents travaux du Forum des Compétences[45]), les manquements à cet article ont donné lieu, avec une fréquence

[43] Article 4 11° du RGPD.
[44] Groupe de travail de l'article 29 réunissant les différents régulateurs des pays de l'Union européenne. Appelé ainsi en raison du numéro de l'article de la directive 1995/46 l'instituant, il deviendra le 25 mai 2018 le Comité européen de la protection des données (CEPD) et verra ses pouvoirs fortement accrus.
[45] Cf. notamment « Obligations en matière de Sécurité de l'Information », première version, fiche A « Obligation de sécurité issue de la loi « Informatique et Libertés ».

toujours plus importante, à des amendes administratives et surtout à la publicité des sanctions.

Depuis la loi du 7 octobre 2016 (« loi pour une République numérique »), la sanction financière maximale a été multipliée par 10 : elle est maintenant de 3 millions d'euros. La CNIL a par ailleurs, depuis cette même loi, la possibilité de sanctionner le responsable de traitement en lui imposant d'informer individuellement, et à ses propres frais, l'ensemble des personnes dont les données été concernées par ce traitement. Le RGPD accroit aussi les sanctions en cas de manquement aux règles qu'il établies. Le 25 mai 2018, elles atteindront 20 millions € ou 4% du chiffre d'affaires mondial du groupe auquel le responsable de traitement appartient.

Enfin, la loi du 18 novembre 2016 (« loi de la modernisation de la justice du XXIe siècle ») prévoit dorénavant « l'action de groupe en matière de protection des données à caractère personnel » [46] (succédané français des « class action » américaines). En vertu de ce texte, les associations de défense des consommateurs représentatives au niveau national et agréées, les associations ayant pour objet la protection de la vie privée ou des données personnelles ou encore les organisations syndicales de salariés représentatives pourront exercer cette action « *lorsque plusieurs personnes physiques placées dans une situation similaire subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions de la présente loi par un responsable de traitement de données à caractère personnel ou un sous-traitant* ». Cette action ne peut cependant tendre qu'à la demande de la cessation du manquement (par exemple par l'arrêt du traitement) et non à la réparation du dommage subi.

Ainsi, à titre d'exemple, une organisation syndicale représentative, agissant au niveau national et pas forcément directement dans l'entreprise, pourrait arguer d'une mise en place illicite d'objets connectés dans l'entreprise et agir dans le cadre d'une action de groupe afin d'obtenir la cessation du manquement[47].

2.5 – Les objets connecté, objets d'une réglementation particulière ?

La question a pu être posée de l'existence d'une réglementation propre aux objets connectés.

Ce choix n'est pas celui qu'a fait le législateur, tant européen que français. Son objectif a plutôt été de se concentrer sur les moyens et finalités de la collecte, ainsi que sur le type d'informations collectées. Ainsi, il attache des règles spécifiques à certaines techniques de traitement plus intrusives (profilage des données[48]) ou

[46] Cf. article 91 et suivant de la loi.

[47] Le RGPD prévoit également la possibilité pour les associations valablement constituées, actives dans le domaine de la protection des données, d'introduire une réclamation devant l'autorité de contrôle compétente lorsqu'elles estiment que les droits des personnes concernées sur leurs données ont été violés (article 80 du RGPD).

[48] Article 4 4) du RGPD : le "profilage" consiste en « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ».

encore à la collecte de certaines catégories de données (données de santé, données sensibles, numéro d'inscription au registre ou n° INSEE en France, etc.).

Il est donc fondamental, si ce type de données est traité par les objets connectés que l'entreprise propose ou fournit à ses salariés, de prendre en compte ces règlementations particulières.

2.6 - La question de la géolocalisation

La géolocalisation n'est pas une problématique apparue avec les objets connectés. Elle existait déjà notamment *via* la question des dispositifs de géolocalisation installées sur les véhicules mis à disposition du personnel. La CNIL, saisie de longue date de cette question [49], a rappelé les principes permettant l'acceptation de l'utilisation de tels dispositifs à l'occasion d'une délibération récente[50].

La géolocalisation du salarié est possible à condition que :

- les finalités soient limitées (par exemple le suivi du temps de travail « à la condition qu'il ne puisse être effectué par d'autres moyens ») ;
- les droits des employés soient préservés (possibilité pour le salarié de désactiver la fonction de géolocalisation « *en particulier à l'issue de leur temps de travail ou pendant leur temps de pause* », information du salarié sur l'existence du dispositif, accès aux données enregistrées par l'outil) ;
- les destinataires soient limités aux personnels strictement habilités ;
- des mesures de sécurité soient prises ;
- la durée de conservation des données collectées soit limitée (en principe 2 mois, et 5 ans lorsqu'elles sont utilisées pour le suivi du temps de travail).

Si la délibération est récente, les principes étaient déjà connus. Ainsi, Orange a été condamné par la Cour d'appel de Paris le 29 septembre 2016 pour avoir placé depuis 2012, sur 20 000 de ses véhicules, un appareil permettant de les transformer en voitures connectées en les reliant *via* un réseau téléphonique 2G à un logiciel de gestion de flotte « *permettant de supprimer les tâches manuelles et erreurs, de suivre l'évolution du kilométrage parcouru de manière actualisée, les informations pouvant être consultées à la fois par le gestionnaire de flotte et le conducteur* ». Or cet appareil pouvait également géolocaliser en temps réel les véhicules. La Cour a affirmé que ce dispositif « portait atteinte aux droits des salariés », du fait de la nature des données collectées, de leur durée de conservation et de l'impossibilité pour les salariés de désactiver le boîtier[51].

Ces principes devront naturellement être transposés à une époque où, de plus en plus, ce n'est plus le véhicule qui est géolocalisable, mais potentiellement le salarié

[49] Ainsi, le nombre de déclarations de dispositifs de géolocalisation de véhicules de salariés de 3 400 en 2009 a-t-il quasiment doublé en 5 ans, pour aboutir à 6100 en 2014.
[50] Délibération n°2015-165 du 4 juin 2015 « *portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés* ».
[51] Cour d'appel de Paris du 29 septembre 2016, n°15/17026.

lui-même via son badge RFID[52] ou plus récemment sa montre ou ses lunettes connectées. A ce titre, l'utilisation des porte-badges RFID anonymisés du personnel de Sanofi Val de Bièvre est parlante : elle permet la visualisation des flux d'employés et donc l'optimisation de la configuration des locaux[53].

L'utilisation par les employeurs de technologies plus intrusives, telles que la géolocalisation des salariés, nécessite de réfléchir en amont **aux finalités du traitement, aux types de données collectées ou encore à la façon dont ces données seront manipulées. Cette démarche renvoie au principe de « *privacy by design* » (ou vie privée dès la conception[54]), qui se traduit par la prise en compte de la protection des données dès la conception des outils ou encore dans les méthodologies projets incluant le traitement de données.**

3. Une approche éclairée nécessaire… des processus internes à modifier aux analyses de risque à renforcer

Déjà, en 2003, le commissaire de la CNIL Philippe Lemoine avait identifié quatre « pièges » pouvant conduire à minorer le risque de l'internet des objets sur la protection des données à caractère personnel et la vie privée[55]. Ces « pièges », encore d'actualité, étaient les suivants :

– *L'insignifiance des données,* soit le fait de ne pas identifier l'importance que peuvent revêtir les données collectées. Sur ce point, elle n'est parfois qu'apparente, et c'est à la personne concernée comme au responsable de traitement de ne pas tomber dans cette illusion (cf. paragraphes précédents) ;

– *La priorité donnée aux objets*. Il convient de ne pas se focaliser que sur les objets, donc la technologie, et ne pas oublier les données et les traitements permis par ces objets, et surtout les personnes qui en sont équipées et dont les données sont traitées ;

– *Le risque de « non vigilance » individuelle,* soit le fait de banaliser l'objet doublé de l'intérêt technologique ou pratique, qui entraîne l'oubli des risques de la part de l'utilisateur comme des fournisseurs ;

– *La logique de mondialisation* qui, jusqu'alors, conduisait à ne pas prendre en compte les impératifs considérés comme purement locaux des réglementations sur la protection des données.

En effet, les entreprises qui souhaitaient, dans le cadre de l'équipement de leurs personnels par de tels objets, imposer au fabricant ou au distributeur une mise à niveau de leur sécurisation, se heurtaient la plupart du temps à des fins de non-recevoir plus ou moins voilées.

Sur ce dernier aspect au moins, la situation évolue. Pour les fabricants qui continuent

[52] RFID pour *Radio Frequency Identification* ou radio-identification.
[53] http://www.lefigaro.fr/societes/2016/04/14/20005-20160414ARTFIG00204-sanofi-equipe-les-porte-badges-de-certains-employes-de-puces-electroniques.php.
[54] Article 25 du RGPD.
[55] Communication de Philippe Lemoine relative à la radio identification, séance de la CNIL du 30 octobre 2003.

à ne pas prendre en compte la sécurité comme prérequis au développement des objets connectés qu'ils produisent, une nouvelle réalité normative s'impose : entreprises clientes et entreprises prestataires devront à court terme respecter les obligations du Règlement sur la protection des données (RGPD) applicable au 25 mai 2018, qui rebat les cartes de façon très importante sur ce sujet.

Sans détailler l'ensemble des règles introduites ou réaffirmées par ce volumineux Règlement, il suffira d'en signaler six éléments fondamentaux :

- **Il s'applique spécifiquement aux sous-traitants, considérés en tant que tels et qui doivent se plier aux mêmes règles strictes que le client**, notamment concernant la sécurisation des traitements de données dans lesquels ils interviennent, et donc des objets connectés ;
- **Le Règlement prévoit de s'appliquer, dans un certain nombre de cas, aux acteurs économiques étrangers,** même s'ils n'ont pas d'établissement au sein d'un pays de l'Union Européenne, ce qui permet d'agir sur des prestataires américains ;
- **Le Règlement met en avant le principe de protection des données dès la conception (ou « *Privacy by design* ») qui oblige à prendre en compte la question de la protection des données à caractère personnel dès le début du cycle de développement des produits ou services.** De façon complémentaire, les notions de « protection des données par défaut » et de « minimisation des données collectées »[56] conduisent à ne s'obliger à traiter que les données strictement nécessaires. Ce qui là aussi aura des impacts forts pour les fabricants, distributeurs et fournisseurs d'objets connectés ;
- **Le texte impose aux entreprises ayant recours à des prestataires de faire « *uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées* de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée** » (article 28 alinéa 1) ;
- **Le règlement oblige le responsable de traitement à mener des études d'impact sur la vie privée (EIVP ou « *Privacy Impact Assessment* »)[57] à titre préalable lorsque le traitement est susceptible de comporter un risque élevé pour les droits et libertés des personnes[58].** Compte tenu de l'importance du sujet pour les établissements de la Place, le Forum des

[56] Cf. article 25 du RGPD « *Protection des données dès la conception et protection des données par défaut* » ainsi qu'article 5 du RGPD : « *Article 5*
Principes relatifs au traitement des données à caractère personnel
Les données à caractère personnel doivent être : (…) c) adéquates, pertinentes ***et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)*** *»* ;

[57] Cf. article 35 du RGPD « Analyse d'impact relative à la protection des données ».

[58] Le Groupe de l'article 29 conseillait déjà aux entreprises de mener une telle étude lors de la mise en place de dispositifs RFID, cf. Avis 9/2011 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID. Ces analyses conduisent ainsi à évaluer la vraisemblance de ces risques et à documenter les mesures prises pour y faire face. Pour élaborer ces PIA, la lecture de la Norme AFNOR NF EN 16571 est recommandée (mais elle est spécifique aux dispositifs RFID), de même que la méthode PIA de la CNIL de juin 2015 (https://www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil) dont la méthode et les outils qu'elle met à disposition sont plus transversaux. Le groupe de l'article 29 a également publié des lignes directrices relatives à l'élaboration des études d'impact sur la vie privée le 4 avril 2017.

Compétences a créé un groupe de travail sur cette problématique auquel participe la CNIL[59] ;

- **Les manquements aux règles sont sanctionnés par une amende pouvant aller jusqu'à 4 % du chiffre d'affaires annuel mondial du Groupe auquel appartient l'entité en faute.**

Ces différents éléments sont parfaitement résumés dans le considérant l'article 78 du RGPD que nous reproduisons ici : « *Afin d'être en mesure de démontrer qu'il respecte le présent règlement, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut. Ces mesures pourraient consister, entre autres, à réduire à un minimum le traitement des données à caractère personnel, à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, à permettre à la personne concernée de contrôler le traitement des données, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer. Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions,* ***il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données*** ».

Plus spécifiquement, le Groupe de travail réunissant les différents régulateurs des pays de l'Union européenne (G29 précité note 44), a rendu un avis le 16 septembre 2014 qu'il convient de considérer avec attention concernant les développements récents de l'Internet des objets - *quantified self*, ou « technologies prêtes à porter » (montres, bracelets, lunettes, etc.) et domotique[60].

Les recommandations de cet avis, que nous reproduisons en annexe pour information, se concentrent sur les questions juridiques liées aux objets connectés. Mais ces recommandations doivent selon nous être couplées avec les politiques techniques et organisationnelles à mettre en place afin de pallier les risques de sécurité identifiés dans la partie suivante, afin de permettre une mise en œuvre efficace et coordonnée au sein de l'entreprise.

En effet, parmi les points soulevés dans l'avis, notons en particulier **le manque d'information et de maîtrise par l'utilisateur des objets connectés, la création par le fabricant de modèles considérés comme intrusifs, ou encore les risques liés à la sécurité**.

[59] https://www.forum-des-competences.org/nos-groupes-de-travail/reglement-europeen-sur-la-protection-des-donnees-personnelles-(rgpd).html.
[60] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

4. Objets connectés et sécurité de l'information : un couple mal assorti dès l'origine ?

Pendant longtemps, l'insécurité des objets connectés n'était pas un sujet pour beaucoup d'acteurs du domaine. Il s'agissait pourtant d'une réalité, comme l'ont montré maints exemples récents, que nous rappelions en introduction de ce document et que nous allons détailler ci-après. Pour autant, loin d'être une fatalité, l'insécurité des objets connectés peut être largement réduite en suivant les guides de bonnes pratiques édités par divers organismes ces dernières années.

4.1 - L'insécurité des objets connectés – une fable ?

D'aucuns ont pu soutenir que l'insécurité des objets connectés était largement exagérée et n'avait pas d'impact pratique. Mais au contraire, l'insécurité des objets connectés est sous-estimée et le constat de son impact ne fera que s'affermir au fur et à mesure que les objets connectés se répandront.

Ainsi, l'enquête « *Internet of things research study : 2015 report* » de Hewlett Packard Enterprise[61] menée sur une dizaine d'objets connectés populaires y a décelé un grand nombre de vulnérabilités :

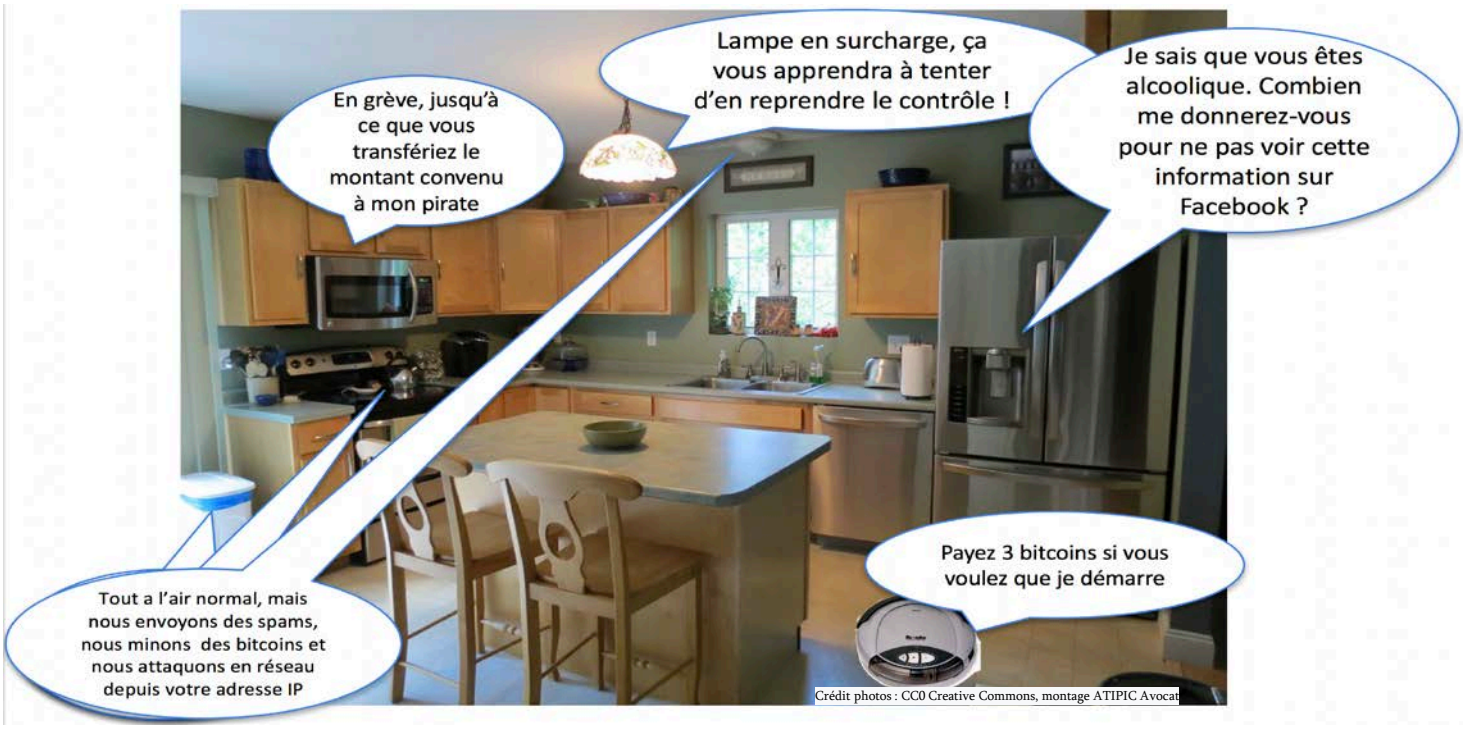
- 90 % des objets connectés récupèrent des informations personnelles sur leur utilisateur, que ce soit *via* l'appareil, le cloud ou l'application mobile utilisés ;
- 80 % des objets connectés sont concernés par des problèmes de confidentialité, et les problèmes sont de plus en plus nombreux avec le cloud et l'application mobile. Dans la plupart des cas les informations ne sont pas chiffrées lors de la transmission d'informations, que celle-ci soit en direction d'un réseau local ou en direction d'internet ;
- 60 % des objets connectés sont concernés par des failles concernant leur interface Web, donnant accès, *via* l'interface Web, aux appareils ainsi qu'aux données.

De façon plus pratique, et si l'on synthétise les principales études en matière de sécurité des objets connectés, les **principaux risques** que l'on retrouve sont les suivants :

- vol (notamment à des fins de divulgation), écoute ou interception de données « à forte valeur » telles que des données de géolocalisation, de bien-être – cf. 2.3 ci-dessus – voire de santé (données sensibles), des données bancaires, mais également des données permettant de savoir qu'un appartement est vide donc prêt à être cambriolé, etc. ;
- falsification des données échangées ;
- mise hors service et/ou dysfonctionnement, notamment à des fins de chantage ou d'extorsion (blocage du système de climatisation en plein été, d'un appareil ménager ou du système de démarrage de la voiture, etc.).

[61] https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

- prise de contrôle à d'autres fins que le fonctionnement originel et classique de l'objet connecté, notamment minage de bitcoin et piratage pour mise en réseau parmi d'autres objets connectés permettant une attaque par déni de service distribuée (l'objet connecté est alors piraté pour servir de vecteur d'attaque à d'autres systèmes d'information).



Ainsi, depuis plusieurs années, les **conséquences de ces vulnérabilités** ne sont plus virtuelles et ont pris corps dans le monde réel. Nous avons repris ci-après quelques exemples non-exhaustifs :

- augmentation importante – et difficilement indemnisée – des vols de voiture sans effraction [63]. Il semblerait ainsi selon le classement 2015/2016 de l'association 40 millions d'automobilistes, que « *sur 300 modèles de véhicules volés en France, 70% le sont par piratage du système de sécurité informatique* » ;
- prise de contrôle de centaines de milliers de webcams ou encore d'enregistreurs numériques fin 2016 pour commettre les plus grandes attaques par déni de service distribuée connues [64]. Dans le même ordre d'idée, prise de contrôle d'objets connectés ménagers (réfrigérateur, etc.) pour envoyer des spams, des malwares, etc.) ;
- prise de contrôle de voitures à distance (des freins, du volant, etc.) pendant que celles-ci étaient en mouvement[65] ;

[62] http://www.undernews.fr/reseau-securite/fic-2016-lanssi-sinquiete-du-danger-des-objets-connectes.html
[63] http://www.challenges.fr/automobile/actu-auto/volkswagen-particulierement-touche-par-le-piratage-des-telecommandes_415097
[64] http://www.objetconnecte.com/ovh-camera-connectees-ddos-260916/. Classement réalisé selon la bande passante mobilisée.
[65] http://www.numerama.com/tech/195828-hackers-chinois-prennent-controle-de-voitures-tesla-a-distance.html

- piratage d'un robot-chirurgien par internet *via* la modification des instructions données au bras robotisé de la machine[66]. Il est intéressant de noter que, pour les chercheurs ayant construit le robot, le temps de latence introduit par le chiffrement qui pourrait être mis en place serait de nature à compliquer l'intervention, voire son issue ;
- piratage de bracelets connectés liés à l'acquisition de produits financiers (des chiffres démontrant la bonne santé permettaient de bénéficier de taux plus intéressants) en Russie.

Les raisons de cette situation sont à rechercher :

- **dans le mode de développement de plus en plus agile et itératif ;**
- **dans la multiplication des éléments techniques hétérogènes ;**
- **dans le périmètre de moins en moins déterminé des SI, qui s'interconnectent toujours plus largement.**

Les entreprises sont bien sûr concernées par ces risques liés à la sécurité des objets connectés que leurs salariés utilisent, que cette utilisation soit imposée par l'employeur ou soit de leur propre fait.

Mais outre les risques de piratage, les objets connectés, et notamment certains objets connectés miniaturisés de type « informatique vestimentaire », peuvent aussi être des vecteurs de **fuite d'informations confidentielles**. Les exemples de fraudes commises par le grand public et leur généralisation ne font que renforcer la nécessité de prendre en compte ce risque.

Ainsi, les montres et lunettes connectées sont régulièrement utilisées par des étudiants[67], voire même des joueurs professionnels[68] pour tricher en transmettant frauduleusement des informations.

4.2 - L'insécurité des objets connectés – une fatalité ?

La sécurisation des objets connectés doit prendre en compte trois réalités : la mise en œuvre souvent défaillante des protocoles de sécurité les plus basiques, les difficultés réelles de sécurisation des objets connectés du fait de leur nature et de l'hétérogénéité des acteurs du domaine, et la sensibilisation de leurs utilisateurs à la sécurité.

4.2.1 La mise en œuvre défaillante des protocoles de sécurité

[66] https://www.industrie-techno.com/des-chercheurs-parviennent-a-pirater-un-robot-chirurgien.38074.

[67] Des exemples ont été répertoriés pour des étudiants néerlandais ou encore thaïlandais - http://www.lemonde.fr/campus/article/2016/05/10/une-fraude-digne-de-mission-impossible-au-concours-de-medecine-thailandais_4916842_4401467.html, étant entendu que l'Education nationale a publié des listes actualisées de montres interdites pendant les concours.

[68] Cf. l'équipe de Baseball professionnelle des Boston Red Sox ayant utilisé l'informatique vestimentaire (une montre connectée) pour transmettre des informations au préjudice des New York Yankees - https://www.usatoday.com/story/tech/columnist/baig/2017/09/06/how-you-can-use-apple-watch-cheat-not-you-would/639446001/.

Si le risque de piratage est inhérent à la mise en réseau des dispositifs et à l'attrait qu'ils représentent pour les pirates (source d'information, vecteur d'attaque, etc.), **le danger pourrait être limité si les sociétés qui conçoivent les objets connectés observaient les principes d'hygiène de sécurité informatique de base**.

A titre d'exemple, en 2016, l'une des sociétés qui fabriquent des montres connectées, Garmin, ne chiffrait pas en HTTPS les informations de l'application de fitness présente sur sa montre lors de leur envoi sur l'internet : HTTPS n'était utilisé que lorsque le client créait son compte et s'y connectait[69], ce qui laissait les données échangées vulnérables à toute prise de connaissance, voire altération par un tiers plus ou moins bien intentionné.

Un autre exemple d'intégration non maîtrisée de la sécurité peut être trouvé dans la mise en œuvre du protocole Bluetooth Low Energy (BLE). Rappelons qu'une grande part des fonctionnalités de communication mises en œuvre au sein des objets connectés repose sur ce protocole, qui comporte certaines lacunes en termes de sécurité : le périphérique envoie de manière régulière des trames à tous les périphériques de sa zone (broadcast) permettant de s'identifier auprès des autres périphériques Bluetooth. Certes, le mécanisme « BLE Privacy » change de manière aléatoire l'identifiant du périphérique Bluetooth (adresse MAC[70]) envoyé aux autres périphériques, de manière à empêcher l'identification du périphérique par un tiers non concerné par l'échange de données. Malheureusement cette fonction est mal implémentée : parfois l'adresse MAC reste fixe, parfois toutes les adresses MAC utilisées commencent de la même manière, ce qui rend facile l'identification d'un appareil en particulier. Ainsi, en 2016, l'Apple Watch était la seule montre connectée du marché à avoir correctement mis en place le protocole BLE[71].

4.2.2 Les difficultés réelles de sécurisation du fait de leur nature

Les lacunes des objets connectés en matière de sécurité ne sont pas exclusivement imputables à une mauvaise sensibilisation de leurs concepteurs à ces questions. En effet, **à la difficulté « classique » de sécuriser un système d'information connecté se rajoutent des difficultés propres à la majorité des objets connectés** : souvent, leur espace mémoire est limité, leur connexion au réseau n'a qu'une bande passante faible, leur puissance de traitement est restreinte ou encore leurs réserves énergétiques doivent être gérées avec parcimonie, limitant les traitements consommateurs de ressources (antivirus, chiffrement).

La mise en œuvre de solutions de sécurité avérées, tels que par exemple le chiffrement, est également accusé de faire baisser drastiquement les débits de connexion et à ce titre, parfois « *négligée au profit d'une bonne disponibilité du*

[69] « *Every step you fake - A Comparative Analysis of Fitness Tracker Privacy and Security* », rapport de l'association canadienne Open effect, v. 1.5 du 18 avril 2016, projet financé par le « Privacy Commissioner of Canada », p.35.
[70] MAC pour Media Access Control ou sous-couche de contrôle d'accès au support. C'est la moitié basse de la couche de liaison de données du modèle OSI, selon les standards de réseaux informatiques IEEE 802.
[71] « *Every step you fake - A Comparative Analysis of Fitness Tracker Privacy and Security* », rapport de l'association canadienne Open effect, v. 1.5 du 18 avril 2016, projet financé par le « Privacy Commissioner of Canada », p.73.

service »[72], le fabricant laissant la responsabilité au client *« qui est mieux à même de juger s'il a besoin de chiffrer ses messages et de quelle manière* »[73].

Dès lors, à des vulnérabilités « classiques » (mots de passe par défaut, sécurité mal implémentée notamment dans la communication, etc.) s'ajoutent des vulnérabilités plus spécifiques aux objets considérés : matériel peu résistant du point de vue sécuritaire, peu de mémoire et de puissance de traitement disponibles, mises à jour problématiques du fait de l'intégration poussée des matériels, augmentation de la surface d'attaque (il faut considérer non seulement l'objet lui-même au plan matériel et logiciel, mais aussi le réseau jusqu'au point de connexion à l'internet, le service intégré/cloud et l'utilisateur final), etc.
Enfin, il ne faut pas oublier qu'une grande partie des objets connectés commercialisés à l'heure actuelle ne bénéficient que difficilement de solutions permettant leur mise à jour facilitée (c'est-à-dire que les utilisateurs penseront à effectuer).

L'approche de l'ENISA est intéressante à ce titre, car elle opère une distinction entre deux familles d'appareils [74] : d'une part, les appareils à faible capacité ou « ***Constrained devices*** », petits appareils très limités en termes de puissance, de mémoire et de processeur, comme par exemple des ampoules connectés, détecteurs de fumée, alarmes connectées, caméras IP, serrures connectées, etc. ; et d'autre part, les appareils à forte capacité ou « ***High-capacity devices*** », qui nécessitent pour fonctionner une alimentation secteur et sont potentiellement capables d'intégrer des fonctionnalités avancées de sécurité, comme par exemple une télévision connectée, des routeurs, stockages réseau, etc.. **Les vulnérabilités spécifiques aux objets connectés n'ont donc pas toujours la même portée pratique et l'appréciation de leur impact doit être nuancée selon les objets.**

4.2.3 L'hétérogénéité des acteurs du domaine

Un troisième facteur entre en ligne de compte pour expliquer les lacunes en matière de sécurité : la **diversité des acteurs du secteur**. En effet, les objets connectés sont au cœur d'un écosystème où chacun a sa part en matière de sécurité : fabricants du hardware, développeurs software, concepteurs/i-intégrateurs de la solution, opérateurs de télécom (avec utilisations de protocoles généralistes ou dédiés), prestataires divers (cloud, etc.). Pour ne rien simplifier, certains acteurs peuvent cumuler plusieurs rôles.

Ainsi, si le constructeur d'un objet connecté met en avant des questions de sécurité, des entreprises participant à son écosystème peuvent y être moins enclines que lui. Si l'on prend par exemple la fonctionnalité « Apple Homekit »[75], plusieurs années se sont écoulées entre son annonce par Apple et la commercialisation de produits compatibles par des sociétés tierces, en raison du retard pris dans l'implémentation par ces sociétés du strict cadre sécuritaire imposé par Apple.

---

[72] Renaud Lifchitz, chercheur en sécurité de la société Digital Security, à propos du réseau Sigfox.
[73] Raoul Mallart, vice-président innovation chez Sigfox, en réponse à Renaud Lifchitz.
[74] Guide de l'ENISA « *Security and Resilience of Smart Home Environments* », décembre 2015.
[75] Cette fonctionnalité permet d'utiliser un appareil iOS, AppleTV & Siri pour contrôler les accessoires compatibles dont l'utilisateur dispose à son domicile : luminaires, capteurs, alarmes, etc.

La multiplicité des intervenants soulève également la question de la pérennité de certains d'entre eux, alors que le support et la mise à jour de certains objets connectés (ou de fonctionnalités de connexion dans des objets plus classiques) semble nécessaire.

4.2.4 La nécessaire sensibilisation des utilisateurs aux problématiques de sécurité

Si l'éducation à l'hygiène de la sécurité informatique progresse pour les utilisateurs d'ordinateurs fixes ou portables, voire de téléphones, qui ont pris conscience des risques et sont souvent demandeurs de solutions pratiques à ces risques, la problématique se complexifie à mesure que les objets connectés deviennent des objets du quotidien. Former les utilisateurs à mettre à jour le système d'exploitation et les anti-malware de leurs ordinateurs n'est pas toujours facile, mais les former à mettre à jour leurs lunettes, leurs voitures ou à s'intéresser à la sécurité de leur montre est une étape *a priori* encore plus difficile.

Ainsi, un avis du groupe de l'article 29[76] met ainsi en avant le manque d'information et de maîtrise par l'utilisateur des objets connectés. Cela se vérifie en pratique : prenons l'exemple de l'appairage d'une Apple Watch avec un iPhone réalisé sans précaution particulière, « *out of the box* ». L'appairage entraîne la transmission automatique des authentifications aux réseaux wifi auquel le téléphone s'est déjà connecté et notamment la duplication sur la montre des messages électroniques présents sur le téléphone. Cet appairage est réalisé par une application qui, à l'origine et pendant de nombreux mois, était présente d'office et ne pouvait être désinstallée simplement du téléphone. Concernant les salariés disposant d'une telle montre, les entreprises mettant à disposition des iPhones ou permettant la connexion des iPhones personnels (BYOD[77]) devaient donc mettre à jour leur analyse de risque et déployer les solutions nécessaires (désinstallation, etc.) pour continuer à opérer un confinement extrêmement strict des flux de l'entreprise… A défaut, l'Apple Watch personnelle pouvait en effet se trouver connectée à un téléphone professionnel sans que le cas ne soit prévu par la politique BYOD (on parlerait alors de *shadow* BYOD).

De facto, à côté de la responsabilité des fournisseurs, les entreprises utilisatrices des objets connectés sont donc forcées d'être responsables de leur sécurité. Sans pouvoir se reposer sur leurs fournisseurs, c'est aussi à elles qu'il appartient de mener les analyses de risques nécessaires et de :

- préconiser les mesures techniques ou organisationnelles liées à l'usage qui en sera fait, de nature à limiter les risques identifiés (ou, à défaut, décider d'abandonner la solution) ;
- et/ou se fournir auprès de prestataires proposant des solutions de sécurisation adéquates.

[76] Avis 8/2014 du 16 septembre 2014 sur les récentes évolutions relatives à l'internet des objets. V. la définition du Groupe de l'article 29 à la note 43.
[77] Bring Your Own Device / Apportez votre équipement personnel de communication (AVEC). Désigne la pratique qui consiste à utiliser ses équipements personnels dans un contexte professionnel et le plus souvent en les connectant à tout ou partie du système d'information de l'employeur.

4.3 - Sécuriser les objets connectés : démarche de normalisation et bonnes pratiques

Afin de combattre l'insécurité des objets connectés, certaines pratiques sont imposées, notamment par le législateur européen, tandis que d'autres relèvent de recommandations et de guides de bonnes pratiques.

Le **RGPD** déjà mentionné (cf. note 27) a ainsi participé à cette prise de conscience en imposant une obligation de sécurité particulièrement contraignante au responsable du traitement de données à caractère personnel[78] applicable dès le 25 mai 2018 (étant entendu que nombre de régulateurs européens appliquent dès à présent ses principes à défaut de pouvoir sanctionner leur non observation).

En ce qui concerne les bonnes pratiques, plusieurs organismes ont émis des recommandations de bonnes pratiques : l'ANSSI[79], l'ENISA[80], Harvard Business Review[81], le CIGREF[82], INHESJ[83], le GSMA[84], l'ARCEP[85], etc. Leurs recommandations diffèrent mais on y retrouve un courant d'idées similaires.

De façon synthétique, les différents organismes mettent en avant les préconisations suivantes :

- **La réalisation d'analyses de risque poussées** en ce qui concerne les scénarios et les conséquences. Les objets connectés recueillant par nature un grand nombre de données personnelles, les études d'impact sur la vie privée (EIVP ou « *Privacy Impact Assessment* »)[86] seront à coup sûr un passage obligé pour les entreprises utilisatrices, comme le préconise d'ailleurs le Groupe de l'article 29.
- **Une appropriation de la sécurité par les acteurs du marché des objets connectés,** qu'ils conçoivent les outils, qu'ils les acquièrent pour un usage interne, qu'ils les recommandent à des clients ou des tiers ou qu'ils se préparent à en accueillir dans des usages internes[87]. Les différents organismes précités conseillent d'intégrer l'objectif de sécurité dès le début du projet et pendant toute sa durée, même si ce n'est pas une sécurité maximale, par exemple en repensant l'organisation de l'entreprise de telle sorte que les différents départements collaborent mieux entre eux.
- **Une responsabilisation de tous les acteurs concernés** : l'ENISA recommande par exemple que tous supportent les coûts liés à la sécurité et contribuent à la prise de conscience du grand public de son importance, alors

[78] RGPD, art. 32 et s.
[79] « Cybersécurité des objets connectés – risques, bonnes pratiques et opportunités », ANSSI - Vincent Strubel – 17 juin 2015
[80] Cf. infra (note 74).
[81] « Comment les objets intelligents connectés transforment les entreprises », Revue Harvard Business Review France, Avril-Mai 2016
[82] « Objets connectés, Un 360 pour bien les comprendre », CIGREF, Décembre 2016
[83] « Sécurité des objets connectés », Travaux de la 24e promotion des auditeurs de l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ), Décembre 2014
[84] https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[85] « Préparer la révolution de l'Internet des Objets », ARCEP, novembre 2016
[86] Cf. article 35 du RGPD « Analyse d'impact relative à la protection des données ».
[87] Cf. approche CARA de Wavestone : Concevoir / Acquérir / Recommander / Acccueillir aillant de fortes incidences notamment sur le contrôle que l'entreprise peut exercer en pratique sur la sécurisation de ces objets.

que d'autres organismes insistent sur la nécessité d'une analyse systématique des risques adaptée au produit ainsi que sur les conséquences potentielles d'une faille de sécurité. A cet égard, le CIGREF tend cependant à relativiser l'effort nécessaire aux entreprises : il conclut ses préconisations en matière de sécurité en soulignant les nombreuses similitudes des problématiques de sécurité en matière d'objets connectés avec celles des projets informatiques plus classiques, **la spécificité de l'IoT résidant davantage dans les problématiques techniques, la diversité des acteurs et la nature particulière des risques.** Le Groupe de l'article 29 met le focus quant à lui sur l'utilisateur final (le salarié dans nos hypothèses) : il doit pouvoir consentir de manière éclairée à l'utilisation de leurs données, pouvoir paramétrer l'objet et exercer ses droits d'accès et d'opposition[88].

- Si l'on s'intéresse à la conception, le principe de **Privacy by design (**cf. partie 3) doit nécessairement mener non seulement à la sécurisation physique des objets, mais également à celle des protocoles de communication comme des applications et des systèmes embarqués ;
- **La prise de conscience de l'importance du sourcing et donc des processus « achat ».** En effet, si les analyses de risque sont déjà effectuées au sein des établissements financiers par exemple, il n'est pas certain que les directions achat des entreprises des autres acteurs aient intégré la problématique « protection des données » comme étant un critère *sine qua non* de l'acquisition de matériels[89], qu'ils soient destinés à l'interne ou à l'externe, comme le prévoit explicitement l'article 28 du RGPD.
- **La recherche de labels et de certifications** peut s'avérer intéressante, dans la mesure où de tels labels et certifications constitueront à l'avenir un avantage concurrentiel pour les fabricants d'objets connectés, qui se démarqueront ainsi des autres solutions, et où le RGPD prévoit l'attribution de labels en matière de protection des données à caractère personnel. Attention toutefois à l'effet de mode, car il faut nécessairement étudier le périmètre du label : quelles données, quels traitements, quelles mesures de sécurité prend-t-il en compte ?
- **La nomination d'un Data Protection Officer** (**DPO)** pour nombre de fabricants d'objets connectés permettra une meilleure imprégnation de la culture de la sécurité dans l'entreprise : avec le RGPD, le DPO devient de toute façon obligatoire (un des critères étant que les activités du responsable de traitement consistent en un suivi régulier et systématique des personnes concernées).
- **Enfin, une nouvelle approche à développer en mode agile** en y incluant les exigences de sécurité et de *Privacy by design*.

Plus largement, la sensibilisation de toute la chaîne des acteurs de l'entreprise, depuis les directions opérationnelles jusqu'au RSSI, semble une évidence pour sécuriser l'entreprise au plan technique, au plan organisationnel, mais également sur le plan de la conformité à ces nouvelles règles. L'amélioration de la sécurité des objets connectés ne peut se passer des échanges en interne entre les différentes équipes chargées de la conception et de la fabrication du produit (l'étude des

[88] Avis 8/2014 du 16 septembre 2014 sur les récentes évolutions relatives à l'internet des objets

[89] Les travaux au sein du Groupe ont permis de montrer qu'*a priori*, les processus achat intégraient déjà largement la problématique « protection des données » dans les prestations de services (clauses type dans les contrats).

process de fabrication est alors décisive), des échanges avec les sous-traitants, ainsi que du retour d'expérience des utilisateurs du produit.

En ce qui concerne l'approche BtoB, un consortium de fournisseurs pour l'IIoT[90] (Industrial Internet of the Things) a récemment convenu d'un cadre de sécurité visant à trouver un équilibre entre la sécurité et la fiabilité requises pour les opérations industrielles. Afin de répondre aux enjeux du secteur, le consortium met en avant cinq caractéristiques : la sûreté, la fiabilité, la résilience, la sécurité et la vie privée. La notion de sécurité a elle-même été subdivisée en cinq parties : communication, configuration, gestion, sécurité des terminaux et surveillance[91].

Afin de prendre la sécurité des objets connectés à bras le corps, d'autres entités ont par exemple créé un CERT dédié à la veille, à l'évaluation et à la réponse à incidents sur les systèmes d'informations et les nouvelles technologies en matière d'objets connectés[92].

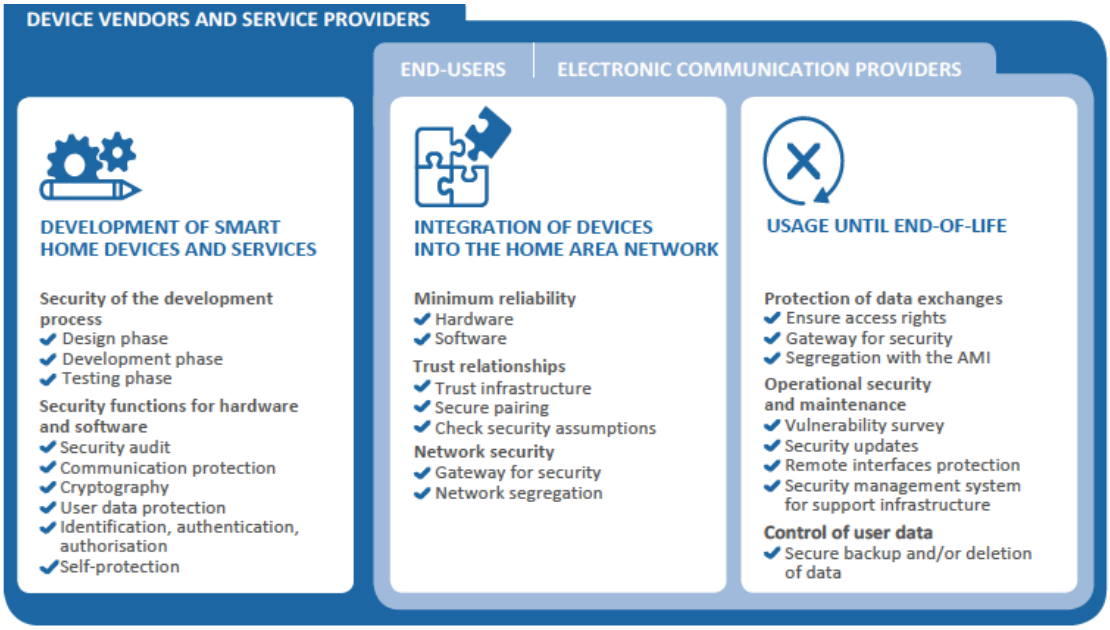
Au plan pratique, l'ENISA a également élaboré 3 guides de bonnes pratiques :

- Le premier guide est à destination des fournisseurs de services et de produits connectés : il s'agit du « Guide de développement pour les appareils connectés » ;
- Les deux autres guides sont à destination des utilisateurs finaux :
    - Guide d'intégration d'un appareil dans la « maison connectée » ;
    - Guide de gestion de l'appareil jusqu'à sa fin de vie.

Chacun de ces guides comporte un ensemble de points d'attention détaillés en termes de sécurité. Une annexe du document sous forme de fiche récapitulative permet rapidement d'identifier 39 menaces classées par grandes catégories.

Pour chacune de ces catégories sont précisés les bonnes pratiques associées ainsi les actions à mener en pratique[93], comme résumé dans la figure suivante issue du document de l'ENISA[94] :

[90] Il s'agit de l'Industrial Internet Consortium, créé en 2014. Il est composé de membres particulièrement prestigieux tels que AT&T, Cisco Systems, General Electric, Intel ou encore RSA Security.
[91] http://www.objetconnecte.com/iiot-securite-normes-2109/.
[92] https://www.digitalsecurity.fr/fr/articles-et-donnees-cert/presentation-du-cert-ubik.
[93] Cf. note 74.
[94] « Good practices within the Smart Home lifecycle and their applicability to stakeholder », © European Union Agency for Network and Information Security (ENISA), 2015.



En conclusion, si certains craignent l'apparition d'une économie à deux vitesses, partagée entre un marché des objets connectés sécurisés et le reste du marché, il convient selon nous de faire preuve d'optimisme. En effet, le processus de sécurisation des objets connectés est bien pris en compte par l'essentiel des acteurs, les autres acteurs étant amené à disparaître s'ils ne respectent pas les exigences légales issues des différents textes (RGPD, NIS). De plus, les problèmes de sécurité détectés ne sont aucunement insurmontables. Nous sommes aujourd'hui dans une période d'adaptation, de transition pour les constructeurs d'objets connectés et les entreprises les utilisant, où la mise en place des différents process et mesures de sécurité est parfois difficile.

Quoiqu'il en soit, les pouvoirs publics ont pris en compte ces problématiques si l'on en juge notamment par le rapport parlementaire sur les objets connectés rendu le 10 janvier 2017, l'avis du G29 du 02 octobre 2014 et les travaux de la CNIL sur la voiture connectée du 23 mars 2016.

Allant encore plus loin, aux USA, un projet de loi visant à imposer des standards de sécurité à tout dispositif connecté utilisé par le gouvernement américain va prochainement être examiné par le Sénat des Etats-Unis. Le « IoT Cybersecurity Improvement Act »[95] vise ainsi à utiliser le poids des achats du gouvernement américain pour relever le niveau de sécurité des objets connectés. En particulier, le texte va obliger les fournisseurs à s'assurer que leurs terminaux peuvent bien être « patchés » à distance, qu'ils ne renferment pas de mots de passe codés en dur (autrement dit non modifiables) et qu'ils ne possèdent pas de vulnérabilités connues au moment où ils sont vendus. Les agences gouvernementales se verraient également imposer un audit des objets connectés en usage dans leur périmètre respectif.

[95] Internet of Things Cybersecurity Improvement Act of 2017 (bill).

5. Objets connectés, responsabilité, preuve, assurance : des conséquences à intégrer dès l'origine du projet

Si les problématiques liées à la protection des données à caractère personnel sont usuellement les premières auxquelles pense le juriste s'intéressant aux objets connectés, elles sont cependant loin d'être exclusives.

D'autres thématiques telles que la responsabilité, la preuve, l'assurance ou encore la santé méritent d'être examinées.

5.1 - Objets connectés du quotidien utilisés en entreprise et droit de la sécurité des systèmes d'information

Le cadre juridique relatif à la sécurité des systèmes d'information impacte la thématique des objets connectés de plusieurs manières, qui peuvent se résumer *via* les questions suivantes :

- L'entreprise peut-elle mettre en place un système de brouillage des signaux, afin par exemple de lutter contre une éventuelle fuite d'informations confidentielles ?
- Le piratage des objets connectés est-il punissable ? Dans quelle mesure ?
- Quelles conséquences vont entraîner l'application de la loi de programmation militaire (LPM) et de la directive Network and Information Security (NIS) ?

5.1.1 La question du brouillage volontaire du signal des objets connectés

L'entreprise qui voudrait brouiller les signaux des objets connectés de ses salariés, afin par exemple de lutter contre une éventuelle fuite d'informations confidentielles, devrait y réfléchir à deux fois.

En effet, sont interdits :

- « *l'importation, la publicité, la cession à titre gratuit ou onéreux, la mise en circulation, l'installation, la détention et l'utilisation* ***de tout dispositif destiné à rendre inopérants*** *des appareils de communications électroniques de tous types, tant pour l'émission que pour la réception* » (article L33-3-1 du Code des postes et communications électroniques).
- le fait de « perturber » les émissions d'un service autorisé, comme un réseau de téléphone mobile ou de connexions spécifiques aux objets connectés tel que le réseau « Sigfox » par exemple (art. L. 39-1 du même code).

Ces actes sont passibles d'une peine de six mois d'emprisonnement et de 30 000 euros d'amende, voire de 150 000 euros pour une entreprise (même article L39-1).

Le fait de rendre inopérant ou de perturber les émissions doit être réalisé de façon **volontaire** pour donner lieu à sanction.

5.1.2 Le piratage des objets connectés est-il punissable par le droit français ?

De par leur nature, et au vu des éléments dégagés dans les définitions abordées au chapitre 1 auquel nous renvoyons, les objets connectés nous semblent parfaitement répondre à la définition de « système de traitement automatisé de données » (STAD) introduite par la loi relative à la fraude informatique du 5 janvier 1988 dite « loi Godfrain »[96].

Ils peuvent également être qualifiés de « système d'information » au sens de l'article 2 a) de la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information, dite « directive cybercrime »[97].

Dès lors, les articles 323-1 et suivants du Code pénal ont vocation à réprimer les atteintes portées aux objets connectés. Ces dispositions répriment l'accès ou le maintien frauduleux, l'altération du fonctionnement, l'introduction de données frauduleuses ou encore la détention ou la commercialisation « d'exploits » permettant les attaques. A cet égard, il est indifférent que les objets connectés en cause appartiennent à l'entreprise ou à ses salariés. Il convient de noter que les sanctions de ces infractions, notamment financières, ont été doublées par la loi relative au renseignement du 24 juillet 2015.

Les articles précités sanctionnaient davantage l'atteinte au support matériel (l'objet connecté) qu'aux données collectées et conservées par lui.

Le législateur a ajouté un article 323-3 au Code Pénal, par la loi du 15 novembre 2014 « *afin de punir non plus seulement l'intrusion dans un système automatisé de données mais également le vol de ces données, véritable lacune de notre droit que des acteurs privés peu scrupuleux ne manquaient pas d'exploiter dans le cadre d'opérations d'espionnage économique* »[98]. Cet article réprime ainsi spécifiquement la détention, la reproduction ou encore la transmission frauduleuse de données issues d'un système d'information[99]. En pratique, cela signifie que l'interception frauduleuse du flux de données provenant d'un objet connecté est punissable.

---

[96] D'après les travaux parlementaires du Sénat sur le sujet, repris et cités dans plusieurs décisions de justice récentes notamment par la Cour de cassation le 19 mars 2014, le « système de traitement automatisé de données » visé par la loi se définit comme « *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs déterminés* ».

[97] « *Un dispositif isolé ou un ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci* ».

[98] Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014 réalisé par M. Jean-Jacques Urvoas, 18 décembre 2014.

[99] « *Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.*
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. »

Il convient de souligner selon la jurisprudence constante de la Cour de cassation[100] que le défaut de sécurisation du système d'information n'écarte pas l'infraction. Sa constitution dépend :

- De l'intention pour le maître du système d'information d'en restreindre l'accès ;
- De la conscience, pour l'utilisateur y accédant, de l'existence du caractère restreint de cet accès (autrement dit, l'utilisateur sait-il qu'au moment où il se connecte, il n'est pas autorisé à le faire ?).

Néanmoins le niveau de sécurisation du système d'information est un critère fondamental pour déterminer le montant de la réparation financière. En effet, la Chambre criminelle, modifiant récemment sa jurisprudence établie, a décidé qu'une sécurité insuffisante du système d'information de l'entreprise réduit son droit à réparation du préjudice en cas de piratage. Cette diminution est déterminée par les magistrats en fonction du niveau de sa faute (à quelle point la sécurisation est-elle insuffisante ?) et donc de sa participation au préjudice[101].

En pratique, utiliser, fournir ou distribuer des objets connectés insuffisamment sécurisés pourra donc réduire d'autant le droit à réparation auquel pourrait prétendre l'entreprise en cas de piratage de ceux-ci…

5.1.3 Quelles conséquences de l'application de la loi de programmation militaire (LPM) ou de la directive Network Information Security (NIS) ?

L'absence de réglementation spécifique visant les objets connectés n'est pas synonyme de « vide juridique ».

Les textes tels que la LPM du 18 décembre 2013 ou encore la directive du 6 juillet 2016 « *concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union* » dite « NIS » bientôt transposée, sont susceptibles de s'appliquer aux systèmes d'information des entreprises concernées dans le cadre des obligations qu'ils prévoient, que ces systèmes d'information soient composés en tout ou partie d'objets connectés ou non. Sur cette question, les lecteurs intéressés pourront se référer aux précédents travaux du Forum des Compétences[102].

Les contraintes opérationnelles imposées par ces textes, notamment en termes de choix d'opérateurs ou de clauses contractuelles à prévoir, ne sont donc en rien spécifiques aux objets connectés. En revanche, elles ajoutent une couche de complexité à la problématique de la conformité, compte tenu de la faible maturité et des pratiques de la majorité des fabricants et fournisseurs d'objets connectés à l'heure actuelle.

[100] Voir notamment Cass.crim, 15 janvier 2014 et Cass. Crim. 9 mars 2016.
[101] Cass.crim, 19 mars 2014.
[102] Cf. notamment la FAQ « Notification des incidents » ou encore « Obligations en matière de Sécurité de l'Information », fiche « Cloud Computing ».

5.2 - Vers une nouvelle vision du droit de la preuve

L'usage des objets connectés ne cesse de se répandre, à titre personnel comme professionnel. Par conséquent, *quid* de l'acceptation par les tribunaux des traces informatiques et autres données créées, collectées ou agrégées par ces objets ? Quelle valeur juridique leurs accorder ?

Concernant la recevabilité à titre de preuve des informations issues des objets connectés, en supposant que la collecte soit licite et loyale[103], les règles sont simples. Dans un contentieux :

- Entre entreprises, les règles du droit commercial ont vocation à s'appliquer. Or ces règles prévoient que « la preuve est libre entre commerçants ». Autrement dit, tous les moyens de preuve sont recevables. Les traces informatiques et données issues des objets connectés pourraient donc être valablement utilisées devant les tribunaux.
- Entre particuliers, les règles du droit civil, récemment modifiées par l'ordonnance du 10 février 2016, s'appliquent. Les principes en la matière, repris notamment à l'article 1358 du Code civil[104], sont restés similaires au droit antérieur. Pour synthétiser, la preuve est libre, hors cadre contractuel. Là aussi, les traces informatiques et données issues des objets connectés pourraient donc être valablement produites devant les tribunaux. A noter que la jurisprudence admet déjà, notamment en droit de la famille, d'autres modes de preuves dématérialisés (SMS, pages des réseaux sociaux[105] , etc.).
- Entre un employeur et son salarié, la preuve est là aussi libre hors problématiques contractuelles, et pour autant que les formalités nécessaires à son recueil aient été observées. Ce type de preuve est souvent utilisé pour fonder une sanction et rentre donc dans la qualification de « contrôle de l'activité du salarié ». Par conséquent, avant toute utilisation, les moyens de collecte de cette preuve (à l'instar des objets connectés utilisés pour contrôler l'activité du salarié) devront être présentés au comité d'entreprise[106], faire l'objet d'une déclaration à la CNIL (jusqu'au 25 mai 2018) et a priori d'une Etude d'Impact sur la Vie Privée passé cette date. Le salarié devra bien entendu être informé préalablement de leur existence. Les informations des objets connectés personnel des salariés ne peuvent être utilisées à titre probatoire par l'employeur. Par exception, ces données peuvent servir de preuve dans deux hypothèses :
    - la connexion de ceux-ci au système d'information de l'entreprise (ce qui a pour effet de transformer les données produites par ces objets connectés en données professionnelles),
    - peut-être si le salarié lui-même publiait ces données (ex. données sur son sommeil montrant que le salarié dort toute la journée pendant son travail).

[103] Et donc conforme aux principes précédemment énoncés au chapitre 2.
[104] « *Hors les cas où la loi en dispose autrement, la preuve peut être apportée par tout moyen.* »
[105] Civ. 1re, 30 avril 2014, n° 13-16.649.
[106] Art. L. 2323-47 al. 3 du Code du Travail : « *Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés*. »

Si la question de la recevabilité de la preuve ne fait pas vraiment débat, il en va autrement de la question de sa force probante, qui dépendra de l'appréciation des tribunaux. Pour l'évaluer, ils se fonderont sur leur perception de la réalité technique, ou en tout cas sur celle que les experts techniques saisis du sujet leur retransmettront. A titre d'exemple, au Canada, une femme qui demandait à être indemnisée pour préjudice corporel après un accident de voiture a utilisé les données de son bracelet connecté Fitbit pour prouver que l'accident avait provoqué une perte d'autonomie[107]. Aux Etats-Unis, une femme qui avait porté plainte pour viol a été contredite par les données de son bracelet électronique, également un Fitbit : elle avait affirmé que son agresseur l'avait surprise dans son sommeil, alors que les données de son objet connecté ont indiqué qu'elle n'avait pas dormi et qu'elle avait marché toute la nuit[108]. Mais en France, dans des cas similaires, il faudrait que la fiabilité des données soit, sinon établie, du moins, peu questionnable.

Deux questions se posent donc avec acuité : d'une part, la question de la sécurité et de l'intégrité des données collectées ou produites par les objets connectés ; et d'autre part, celle de la fiabilité qu'un tiers (un service de police, un magistrat, etc.) peut en attendre.

De la même façon que pour la prise en compte de nouveaux moyens de preuve (SMS, réseaux sociaux, etc.), le droit et les magistrats sauront s'adapter. Mais le vrai bouleversement n'est pas là. Il est plutôt à rechercher du côté de la transformation progressive d'une preuve déterministe (cela existe ou non) à une preuve probabiliste (cela existe probablement). A terme, on n'utilisera plus seulement un enregistrement donné, mais une moyenne des enregistrements de tous les utilisateurs, pour comparer un comportement, une performance à des résultats considérés comme « objectifs », par le biais d'analyses et de comparaisons statistiques.

5.3 - Droit social et objets connectés dans l'entreprise

La présence d'objets connectés dans l'entreprise nécessite de s'intéresser à deux séries de questions en droit social. La première a trait aux objets connectés que les salariés possèdent à titre personnel et qu'ils voudraient utiliser au temps et au lieu du travail ; la seconde, aux objets connectés que l'entreprise voudrait imposer à ses salariés.

En premier lieu, un salarié qui possède un objet connecté peut vouloir l'apporter sur son lieu de travail. Mais les réactions de ses collègues peuvent faire montre d'une certaine réticence. Si l'on prend l'exemple du port de lunettes connectés lors des moments de pause, par exemple au restaurant d'entreprise, on ne peut exclure une réaction de rejet de la part d'autres salariés, à la mesure de ce qui a pu se passer hors du cadre de l'entreprise. A titre d'exemple, un malvoyant porteur d'une prothèse s'est fait physiquement agresser par les employés d'un McDonald's à Paris en juillet

[107] http://www.clubic.com/mag/sport/actualite-739717-canada-donnees-recoltees-bracelet-connecte-utilisees-proces.html

[108] http://rue89.nouvelobs.com/2015/07/01/quand-les-objets-connectes-temoignent-a-proces-contre-260040

2012, car ils avaient cru qu'il s'agissait de Google Glass[109] et qu'il était en train de les filmer sans leur consentement.

Un salarié qui apporterait un objet connecté dans son entreprise risque donc de subir une certaine pression sociale de la part de ses collègues. Pour peu qu'il refuse de renoncer à son objet connecté, cela pourrait donner lieu à un trouble caractérisé au sein de l'entreprise. Que l'employeur se pose la question *a priori* ou qu'il soit confronté à une situation concrète de litige entre ses salariés, la question de l'interdiction des objets connectés sur le lieu de travail – ou en tout cas à l'occasion de certaines heures de pause – peut donc être posée. Elle devra être étudiée également au regard de la mise en œuvre effective du « droit à la déconnexion » dans les entreprises, afin que l'exercice de celui-ci n'aboutisse pas à des « effets de bord » non souhaités ou non anticipés (déconnexion ou désactivation d'objets connectés professionnels à certaines heures ou pendant certaines plages alors même qu'ils pourraient être utilisées à des fins privées).

La jurisprudence relative à l'habillement des salariés est une analogie qu'il convient de garder en tête lorsque l'on s'intéresse à cette question. En effet, la situation d'un salarié qui tient à porter des lunettes connectées au travail malgré l'interdiction émanant de son employeur pourrait être comparée à celle d'un employé qui s'obstine à porter un bermuda alors que son entreprise lui impose le port du pantalon. La problématique est commune : quel équilibre trouver entre les prérogatives disciplinaires de l'employeur et les libertés individuelles du salarié ? La Cour de Cassation, confrontée au problème du bermuda, a énoncé que « *la liberté de se vêtir à sa guise au temps et au lieu de travail n'entre pas dans la catégorie des libertés fondamentales* »[110]. Cette affirmation ne donne cependant pas toute latitude à l'employeur de décider de ce que peuvent porter ou non ses salariés : conformément à l'article L. 120-2 du Code du Travail, les contraintes imposées par l'employeur doivent être « *justifiées par la nature de la tâche à accomplir [et] proportionnées au but recherché* ».

Reste à savoir si le souci d'une bonne entente entre les salariés constitue une justification suffisante, question à laquelle les juges auront sans doute à se prononcer dans les années qui viennent.

En second lieu, une entreprise peut souhaiter imposer à ses salariés d'utiliser des objets connectés qu'elle mettrait à leur disposition. Par analogie, l'équipe de football nationale allemande a ainsi imposé à ses joueurs le port des capteurs connectés notamment sur leurs chaussures lors de l'entraînement. Celles-ci fournissaient des informations sur les distances parcourues, les accélérations et décélérations, les rythmes cardiaques. Ces données, couplées à l'usage de caméras, a permis par exemple d'analyser les conséquences de la fatigue sur le comportement d'un joueur (et d'anticiper ses futures blessures ou ses mouvements d'humeur), ou encore d'adapter la tactique en fonction de la forme physique de l'équipe[111].

[109] http://www.journaldugeek.com/2012/07/17/mc-donalds-agresse-handicape-porte-lunettes-digitales/
[110] Cass. Soc., 28 mai 2003, pourvoi n°02-40.273.
[111] http://www.lexpress.fr/actualite/sport/football/coupe-du-monde-comment-le-big-data-coache-l-equipe-d-allemagne_1553634.html

L'employeur peut-il imposer à son salarié de porter un objet connecté de la même façon qu'il peut imposer un uniforme ou des chaussures de sécurité ? Là encore c'est l'article L. 120-2 du Code du Travail tel qu'interprété par la Cour de Cassation qui s'applique. Or une jurisprudence constante conditionne la possibilité d'imposer aux salariés le port d'une tenue de travail soit à des impératifs d'hygiène et de sécurité (ex. blouse, casque…), soit à l'intérêt de l'entreprise[112]. Il est permis d'imaginer que l'utilisation d'un objet connecté appartient à l'une ou l'autre de ces catégories. Par exemple, si un bracelet connecté permet de prévenir en temps réel un malaise ou un accident du travail, ce pourrait être un impératif de sécurité pour le salarié d'en porter un. Quant à l'intérêt de l'entreprise, il pourrait éventuellement être invoqué en ce que l'usage d'objets connectés améliorerait à la fois les performances et l'image de l'entreprise.

Avant d'imposer l'usage d'objets connectés, l'entreprise doit cependant réfléchir à un point : sa responsabilité pourrait-elle être engagée s'il s'avérait ultérieurement que ces objets ont des conséquences négatives sur la santé des salariés ? Autrement dit, est-elle astreinte à un principe de précaution, concernant par exemple les ondes se rapprochant de l'être humain dans le cadre de l'informatique vestimentaire ? Il s'agit là de l'application particulière de problématiques plus générales.

5.4 - Droit de la santé et objets connectés dans l'entreprise

Aujourd'hui, aucune étude ne semble démontrer avec certitude que les objets connectés représenteraient un danger pour la santé de leurs utilisateurs. Pour autant, ce n'est pas un risque à exclure. L'impact des ondes émises par le téléphone portable fait débat depuis de nombreuses années. Si l'usage du seul téléphone n'a pas de conséquences suffisamment nettes sur la santé pour être incontestables, on ne peut en déduire qu'il en ira de même des lunettes ou des bracelets. En effet, ces derniers sont portés en permanence et au plus proche du corps et seront présents, dans un futur proche, aussi bien dans la sphère professionnelle que privée. Par ailleurs l'utilisation d'un objet connecté est souvent combinés avec d'autres. A cela s'ajoutent les problématiques liées au rayonnement dits « non-ionisants » (ondes radios notamment).

L'entreprise pourrait-elle être tenue pour responsable s'il s'avérait un jour que les objets connectés présentent un danger ? Deux cas de figure sont envisageables : soit l'entreprise fabrique et vend des objets connectés, soit elle demande à ses salariés d'en utiliser dans le cadre de leur travail.

L'entreprise qui fabrique et vend des objets connectés, en l'absence d'interdiction, exerce sa liberté d'entreprendre qui a valeur constitutionnelle[113]. Il existe certes, un principe de précaution, qui s'applique principalement au droit de l'environnement et qui a parfois été étendu au domaine de la santé[114] ; mais il est difficile de demander

[112] Ex. Port d'un uniforme pour une hôtesse d'aéroport, CA Paris 13 mars 1984

[113] Art. 4 de la Déclaration des droits de l'homme et du citoyen de 1789 : « *La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi.* »

[114] Cf. arrêt rendu par la CJCE le 5 mai 1998 dans l'affaire dite « de la vache folle » : *« lorsque des incertitudes subsistent quant à l'existence ou à la portée de risques pour la santé des personnes, les institutions peuvent*

à une entreprise, dont l'activité repose sur un produit, de cesser cette activité au nom de ce principe. L'entreprise qui fabrique et vend des objets connectés paraît donc à l'abri d'une mise en cause s'il s'avérait un jour que les radiofréquences ou toute autre caractéristique essentielle d'un objet connecté étaient dangereuses pour la santé. La question de la commercialisation d'objets connectés dotés d'une intelligence artificielle, qui nous emmènerait dans d'autres débats, ne sera pas ici abordée.

Le cas d'une entreprise qui impose à ses salariés l'utilisation d'objets connectés est en revanche plus clair *a priori*. Depuis un arrêt du 25 novembre 2015, l'employeur est tenu d'une obligation de moyens renforcée en matière de sécurité et de santé physique et mentale des travailleurs[115]. Par « obligation de moyens renforcée », il faut entendre que l'employeur est en principe tenu d'une obligation de résultat en la matière, mais qu'il peut s'exonérer de sa responsabilité en prouvant qu'il n'a pas manqué aux diligences prévues par le Code du Travail[116]. Or, une entreprise qui distribuerait des objets connectés à ses salariés en leur demandant de s'en équiper et de les utiliser régulièrement sans s'être préoccupée de leur possible dangerosité pourrait être critiquée. En effet, au regard du principe général de prévention mentionné à l'article L. 4121-2 du Code du Travail, l'entreprise doit éviter les risques. Par conséquent, la mise à disposition d'objets connectés auprès des salariés nécessite que la question de la dangerosité pour la santé des salariés ait été préalablement posée, voire résolue par l'utilisation d'objets connectés dont l'absence de conséquence pour la santé semble établie.

5.5 - Droit de la consommation et responsabilité du fait des objets connectés

Les articles 1245 et suivants du Code civil rendent responsable d'un produit défectueux le producteur de ce produit quand ce dernier cause un dommage soit à une personne, soit à un bien autre que le produit défectueux lui-même quand le dommage est supérieur à 500 euros.

Il n'y a à cet égard pas de spécificité des objets connectés : si la batterie d'une montre connectée explose, le fabricant de la montre sera responsable au même titre que s'il s'était agi de la batterie d'un ordinateur portable.

Que se passe-t-il si un objet connecté n'est pas clairement défectueux, mais qu'il ne répond pas aux attentes de son utilisateur ? L'exemple n'est plus celui d'une batterie qui explose, mais plutôt celui d'une entreprise qui a distribué des lunettes connectées à ses conseillers de vente afin qu'ils puissent reconnaître les clients et qui découvre que les lunettes ne sont pas fiables. On pourrait aussi citer une collecte de données erronées ou, dans le cas d'une intelligence artificielle, une prise de décision non conforme à ce que l'intelligence artificielle aurait dû décider.

Un consommateur serait sans doute protégé par les articles L. 217-4 et suivants du Code de la Consommation, qui impose au vendeur de livrer un bien conforme au

prendre des mesures de protection sans avoir à attendre que la réalité et la gravité de ces risques soient pleinement démontrées. »

[115] Cass. Soc. 25 novembre 2015, n°14-24.444. Auparavant, c'était une obligation de résultat.

[116] Cf. art. L. 4121-1 et L4121-2 du Code du Travail.

contrat, étant entendu que la conformité au contrat comprend « *les qualités qu'un acheteur peut légitimement attendre eu égard aux déclarations publiques faites par le vendeur… notamment dans la publicité ou l'étiquetage* ». Ainsi, si un fabricant de lunettes connectées axait sa publicité sur la reconnaissance faciale mais que cette dernière n'était pas au point, le bien ne serait sans doute pas conforme au contrat au sens du Code de la Consommation.

En revanche, si c'est une entreprise qui achète les lunettes connectées, le Code de la Consommation ne s'applique pas à elle. Ne reste ainsi que l'article 1603 du Code civil, mais qui est plus vague et n'inclut pas la publicité dans le contrat comme tend à le faire l'article L. 217-5 précité. Le vendeur n'aurait alors plus qu'à introduire dans le contrat une clause exonératoire de responsabilité en cas d'imperfection des fonctionnalités de son objet pour échapper à toute poursuite. Une telle clause n'est illicite que si elle *« contredit la portée de l'obligation essentielle souscrite par le débiteur* »[117] ; or il est fort discutable que la perfection de la reconnaissance faciale constitue une obligation objectivement essentielle, peu important que l'entreprise ait acheté les lunettes connectées dans ce but. Là encore, tout repose sur le contrat et la façon dont il est rédigé.

5.6 - Assurance et objets connectés

L'arrivée d'objets tels que les serrures connectées sur le marché soulève des problématiques liées à l'assurance. Sur le fond, rien ne devrait changer : un vol reste un vol, que la serrure soit connectée ou non. Mais une serrure physique forcée garde des traces beaucoup plus visibles qu'une serrure connectée piratée. Par conséquent, l'effraction d'une serrure connectée sera beaucoup plus difficile à **prouver (**analyse des failles de sécurité d'une serrure connectée, analyse des logs dont la conservation est souvent réduite à sa plus simple expression avec les objets connectés faut de mémoire suffisante, etc.) alors même que ses défauts sont connus ou démontrés par la suite[118]. En fonction de la rédaction des clauses d'assurance, du risque réellement couvert et des exceptions prévues, cette problématique de preuve et plus globalement de couverture pourra être plus ou moins bien prise en compte par le contrat d'assurance souscrit. D'autant que le sujet est lié aux assurances pour « risque cyber » dont on sait le potentiel, mais dont on attend encore la diffusion d'offres spécifiques et généralisées à tous. Les magistrats ont d'ailleurs réagi à cette problématique de preuve particulière. Ainsi, le TGI de Paris[119] a-t-il décidé le 5 janvier 2017, à propos d'une clause d'un contrat d'assurance concernant l''effraction d'une voiture, que la définition très stricte prévue au contrat de « l'effraction »[120] prévoyait en réalité un mode de preuve **« *qui ne correspond plus à la réalité des techniques modernes mises en œuvre pour le vol des véhicules* »**. Pour le Tribunal, la clause du contrat de garantie[121] doit donc être réputée abusive et non

[117] Cass. Com. 29 juin 2010, n°09-11.841, *Faurecia*

[118] http://www.lefigaro.fr/conjoncture/2016/08/11/20002-20160811ARTFIG00196-les-cles-de-voitures-de-100-millions-de-vehicules-facilement-falsifiables.php

[119] , N° RG : 15/06093

[120] L'effraction y était définie comme le « *forcement de la direction, détérioration des contacts électriques permettant la mise en route ou de tout système de protection antivol en phase de fonctionnement* », sans prendre en compte le cas de l'usage d'une fausse clé électronique.

[121] « *Toutefois, si votre véhicule était retrouvé sans effraction de nature à permettre sa mise en route et sa circulation (forcement de direction, détérioration des contacts électriques ou de tout autre système antivol en phase de fonctionnement), la garantie Vol ne serait acquise* ».

écrite au sens de la réglementation sur les clauses abusives (« *car elle a pour objet ou effet de limiter indûment les moyens de preuve à disposition du consommateur* »). L'évolution permanente de la menace conduit ainsi naturellement les magistrats à en tirer toutes les conséquences dans le cadre des contentieux qui leur sont soumis.

Une autre question liée est de savoir si la garantie des produits défectueux, à défaut d'assurance, peut s'appliquer à ces hypothèses de piratage facilité par des failles de sécurité. L'article 1245-3 du Code civil définit un produit défectueux comme « *[n'offrant] pas la sécurité à laquelle on peut légitimement s'attendre.* » Cette définition a été peu précisée par la jurisprudence ; par ailleurs, le niveau de sécurité auquel l'utilisateur d'une serrure connectée peut légitimement s'attendre reste flou dans la mesure où il n'en comprendra certainement pas les implications techniques. Gageons toutefois au vu de l'évolution de la jurisprudence et de la future application du RGPD (encore lui !) que le manquement à la sécurisation de l'objet devra être réparé d'une manière ou d'une autre par le fabricant ou le distributeur.

Annexe

Annexe 1 – Acronymes

Dans leur ordre d'apparition dans le texte.

Les acronymes soulignés n'apparaissent qu'une seule fois dans le texte.

LPM : Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, dite « loi de programmation militaire.

NIS : Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite directive *Network Information Security* / ou Sécurité des Réseaux et des systèmes d'Information (SRI).

AESA : Agence européenne de la sécurité aérienne.

SCADA : *Supervisory Control And Data Acquisition* ou Système de contrôle et d'acquisition de données : système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques.

IoT : Internet of the Things / Internet des objets (connectés).

G29 : Groupe de travail de l'article 29 réunissant les différents régulateurs des pays de l'Union européenne. Appelé ainsi en raison du numéro de l'article de la directive 1995/46 l'instituant, il deviendra le 25 mai 2018 le Comité européen de la protection des données (CEPD) et verra ses pouvoirs fortement accrus.

ARCEP : Autorité de Régulation des Communications Electroniques et des Postes.

CNIL : Commission Nationale de l'Informatique et des Libertés.

RGPD : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) dit Règlement général sur la protection des données.

ACPR : Autorité de contrôle prudentiel et de résolution.

INSEE : Institut national de la statistique et des études économiques

RFID : *Radio Frequency IDentification*. Système de radio-identification, activé par un transfert d'énergie électromagnétique, se composant de marqueurs et d'un ou plusieurs lecteurs.

CEPD : Comité européen de la protection des données (voir « G29 »).

BYOD : Bring Your Own Device / Apportez votre équipement personnel de communication (AVEC). Désigne la pratique qui consiste à utiliser ses équipements personnels dans un contexte professionnel et le plus souvent en les connectant à tout ou partie du système d'information de l'employeur.

EIVP : étude d'impact sur la vie privée. Une telle étude est requise par l'art. 35 du RGPD avant un traitement de données à caractère personnel quand celui-ci est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques* ».

AFNOR : Association française de normalisation

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

BLE : *Bluetooth Low Energy* ou Bluetooth à basse énergie est une technique de transmission sans fil créée par Nokia en 2006 sous la forme d'un standard ouvert basé sur Bluetooth et permettant une bien moindre dépense d'énergie.

MAC : Media Access Control ou sous-couche de contrôle d'accès au support. C'est la moitié basse de la couche de liaison de données du modèle OSI, selon les standards de réseaux informatiques IEEE 802.

SI : Système d'Information

BtoC : *Business to Consumer* (relations entre professionnels et consommateurs)

BtoB : *Business to Business* (relations entre professionnels)

ENISA : Agence européenne chargée de la sécurité des réseaux et de l'information

CIGREF : Club Informatique des Grandes Entreprises Françaises

INHESJ : Institut national des hautes études de la sécurité et de la justice

GSMA : *Groupe Special Mobile Association,* association qui représente près de 800 opérateurs de téléphonie mobile à travers 220 pays du monde.

SRSHE : *Security and Resilience of Smart Home Environments*

DPO : Data Protection Officer ou délégué à la protection des données

STAD : Système de traitement automatisé de données

TGI : Tribunal de Grande Instance

RSE : Responsabilité Sociétale de l'Entreprise

CERT : *Computer Emergency Response Team* (marque déposée) ou *Computer Security Incident Response Team* (CSIRT), centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous.

ANSES : Agence Nationale Sécurité Sanitaire Alimentaire Nationale

Domotique : ensemble des techniques de l'électronique, de physique du bâtiment, d'automatisme, de l'informatique et des télécommunications utilisées dans les bâtiments et permettant de centraliser le contrôle des différents systèmes et sous-systèmes de la maison et de l'entreprise (chauffage, volets roulants, porte de garage, portail d'entrée, prises électriques, etc.)

Quantified self : ou *personal analytics* ou « mesure de soi » regroupe les outils, les principes et les méthodes permettant à chacun de mesurer ses données personnelles (de bien être ou de santé), de les analyser et de les partager

Annexe 2 – Sélection de définitions concernant les objets connectés / l'Internet des objets

- **Institute of Electrical and Electronics Engineers (IEEE) :** Les objets connectés sont des réseaux d'éléments chacun muni de capteurs qui sont connectés à l'internet.

- **Selon l'Union Internationale des Télécommunications (UIT)[122],** les objets connectés ont les 5 caractéristiques suivantes :

  1° l'interconnectivité : les objets peuvent être connectés entre eux et à l'ensemble de l'infrastructure internet ;

  2° les services propres : les objets fournissent des services de façon intrinsèque ;

  3° l'hétérogénéité : les dispositifs utilisés pour le fonctionnement des objets sont hétérogènes (logiciels, réseaux, caractéristiques physiques) ;

  4° les changements dynamiques: les objets évoluent dans un environnement qui évolue (emplacement, vitesse) et le nombre de dispositifs évolue également, avec l'apparition de nouvelles vagues technologiques ;

  5° la très grande échelle : les dispositifs qui devront être gérés et qui communiqueront entre eux seront sensiblement plus nombreux que ceux connectés à internet aujourd'hui.

- **ARCEP[123] :** ensemble d'objets physiques connectés qui communiquent via de multiples technologies avec diverses plateformes de traitement de données, en lien avec les vagues du cloud et du big data.

- **Institut Gartner[124]** : L'Internet des Objets est le réseau des objets physiques qui embarquent des technologies pour communiquer et interagir avec l'environnement externe selon leurs états internes.

- **Dictionnaires Larousse ou Petit Robert** depuis mai 2015, « *Se dit d'un équipement ayant une connexion à Internet ou relié à un téléphone intelligent dont il utilise les capacités* »
  Les champs ou secteurs d'application.
  - Santé connectée
  - Mode connectée
  - Sport connecté
  - Automobile connectée

[122] UIT, Présentation générale de l'internet des objets, recommandation Y.2060, juin 2012.
[123] Préparer la révolution de l'Internet des Objets, 7 novembre 2016.
[124] Gartner – Glossary - http://www.gartner.com/it-glossary/internet-of-things.

- Sécurité connectée
- 2 roues ou moto connectée
- IOT et seniors
- IOT et bébés / enfants
- IOT et smartphone
- maison connectée, domotique
- Exosquelette et IOT
- IOT et design
- IOT et wearables
- agriculture connectée
- business / marketing des IOT
- réseaux connectés
- etc.

- **Wikipedia** : l'Internet des objets représente l'extension d'Internet à des choses et à des lieux du monde physique. Alors qu'Internet ne se prolonge habituellement pas au-delà du monde électronique, l'Internet des objets connectés représente les échanges d'informations et de données provenant de dispositifs présents dans le monde réel vers le réseau Internet. Considéré comme la troisième évolution de l'Internet, baptisé Web 3.0 (parfois perçu comme la généralisation du Web des objets mais aussi comme celle du Web sémantique) qui fait suite à l'ère du Web social, l'Internet des objets revêt un caractère universel pour désigner des objets connectés aux usages variés, dans le domaine de la e-santé, de la domotique ou du quantified self.

- **INSA Rennes** : Les premiers objets connectés (aussi appelés objets communicants, ou encore internet des objets) sont apparus vers la fin des années 90, donc très récemment, c'est pourquoi il n'existe actuellement aucune **définition « officielle »** d'un objet connecté. Pour réaliser la définition simple nous nous aiderons d'un dictionnaire. Pour cela nous procéderons de la manière suivante : nous définirons un par un chaque mot composant les termes « objet connecté », « objet communicant » et « internet des objets ».
  - Objet : « Chose solide considérée comme un tout, fabriquée par l'homme et destinée à un certain usage » (Dictionnaire Larousse, version dématérialisée, décembre 2013) ;
  - Connecter : « Unir, lier des choses entre elles ; -TECHNIQUE : Établir une liaison électrique, hydraulique, etc… entre divers organes ou machine. Etablir une liaison avec un réseau informatique » (Petit Larousse illustré 2004) ;
  - Communicant : « Se dit d'une chose qui communique avec une autre » (Petit Larousse illustré 2004) ;
  - Communiquer : « Faire passer quelque chose d'un objet à un autre, d'une personne à une autre » (Petit Larousse illustré 2004).

  Si l'on se fie aux quatre définitions ci-dessus, un objet connecté est une chose, fabriquée par l'homme, dont l'usage est d'établir **une liaison afin de pouvoir faire passer des informations diverses et variées à un autre objet ou à toute autre chose connectée**.