Flavie BADREAU
Sous la direction de Slim TOUHAMI

Les objets connectés :

Etat des lieux des risques juridiques et techniques

IoTrust

Un projet soutenu et financé par
la fondation MAIF, la société Digitemis et l'école ESIEA.

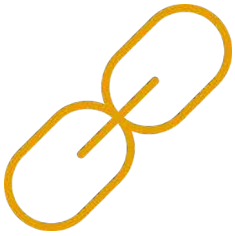
IoTrust

Attributions

Flavie BADREAU

Juriste au sein de la société Digitemis, Flavie BADREAU conseille et accompagne ses clients dans leur mise en conformité avec le règlement européen sur la protection des données personnelles (RGPD).
Avec cet ouvrage, Flavie aborde de manière pédagogique la sécurité technique et juridique des objets connectés.

Le projet IoTrust



IoTrust est un projet dont l'ambition est de favoriser et promouvoir un internet des objets sécurisé et éthique. Cet ouvrage est la première production du projet et vise à sensibiliser consommateurs et industriels à la protection de la vie privée des utilisateurs.

La fondation MAIF

La fondation d'utilité publique MAIF finance la recherche dans le domaine de la prévention des risques qui affectent les personnes, les biens et la vie quotidienne. A l'image de sa participation au projet IoTrust, la fondation soutient des projets innovants dans le but de réduire les risques.

fondation-maif.fr

La société DIGITEMIS

DIGITEMIS accompagne ses clients dans la protection des données personnelles et dans la mise en place de politiques de cybersécurité. Elle propose également des prestations d'audit et de sensibilisation à la sécurisation des données.

digitemis.com

L'école ESIEA

L'École supérieure d'informatique, électronique, automatique (ESIEA) est une école formant des ingénieurs dans le domaine des sciences et technologies du numérique. L'ESIEA apporte son expertise dans le mise en place de solutions techniques innovantes pour la sécurisation des objets connectés.

esiea.fr

20 milliards d'objets connectés

Plus de 20 milliards d'objets connectés sont prévus en 2020 selon le cabinet américain Gartner. Depuis la démocratisation des ordiphones, les concepteurs développent l'idée d'un accès Internet illimité et universel. L'objet connecté est ainsi équipé de capteurs qui recueillent diverses données. Celles-ci sont envoyées sur un support, ordiphone ou tablette le plus souvent, qui grâce à une application spécifique va traiter ces dernières et proposer différents services à l'utilisateur. Les concepteurs interviennent dans des domaines aussi divers et variés que la domotique, la santé, les loisirs ou encore le secteur industriel.

Pour autant, l'explosion de ce nouveau marché connecté prévue par les spécialistes n'a pas encore eu lieu. Plusieurs freins expliquent ce faible engouement. En premier lieu, le prix des objets connectés est bien plus élevé que leur équivalent classique. Les consommateurs les moins technophiles ne perçoivent pas l'utilité de ces nouveaux appareils. En cause, un manque d'informations et un aspect « gadget » qui justifient le désintérêt d'une grande partie d'entre eux. La complexité et les contraintes techniques (chargement, problèmes de connexion…) contraignent l'utilisation de l'objet. Enfin, la crainte de se faire voler ses données clôt l'explication.

Néanmoins, les différents professionnels du secteur peuvent se rassurer. La révolution des objets connectés aura bien lieu, seulement elle ne se fera pas en quelques années. Dans les années 90, l'idée d'un téléphone mobile paraissait curieuse et totalement inutile. Aujourd'hui, les ordiphones sont largement répandus. Ainsi, l'enjeu pour les concepteurs est de se mettre en phase avec les vrais besoins des consommateurs, en proposant en première approche des objets connectés simples et facilement accessibles au plus grand nombre. Les concepteurs devront enfin rassurer les utilisateurs en mettant en place des pratiques assurant la sécurité de leurs données.

Cet état des lieux a donc pour but d'indiquer pour chaque domaine phare du marché des objets connectés les principaux risques existants. Ces risques touchent principalement les biens et les personnes. Cependant, l'environnement peut également être concerné. Les mesures juridiques et techniques essentielles seront présentées, afin que les consommateurs soient informés et soient vigileants dans leurs choix et usages de objets connectés.

Les protocoles de communication

Un protocole de communication permet de faire transiter les données d'un appareil à un autre. Sans lui, impossible pour un objet connecté de communiquer à un ordinateur les données obtenues. Devant les dizaines de protocoles existants, le choix peut s'avérer délicat. Les concepteurs d'objets connectés doivent donc se poser les bonnes questions afin de trouver le protocole qui sera le mieux adapté à leur projet.

On distingue les réseaux à longue portée des réseaux à courte portée. Les premiers permettent une communication longue distance, impossible avec les seconds.

Les réseaux longue portée

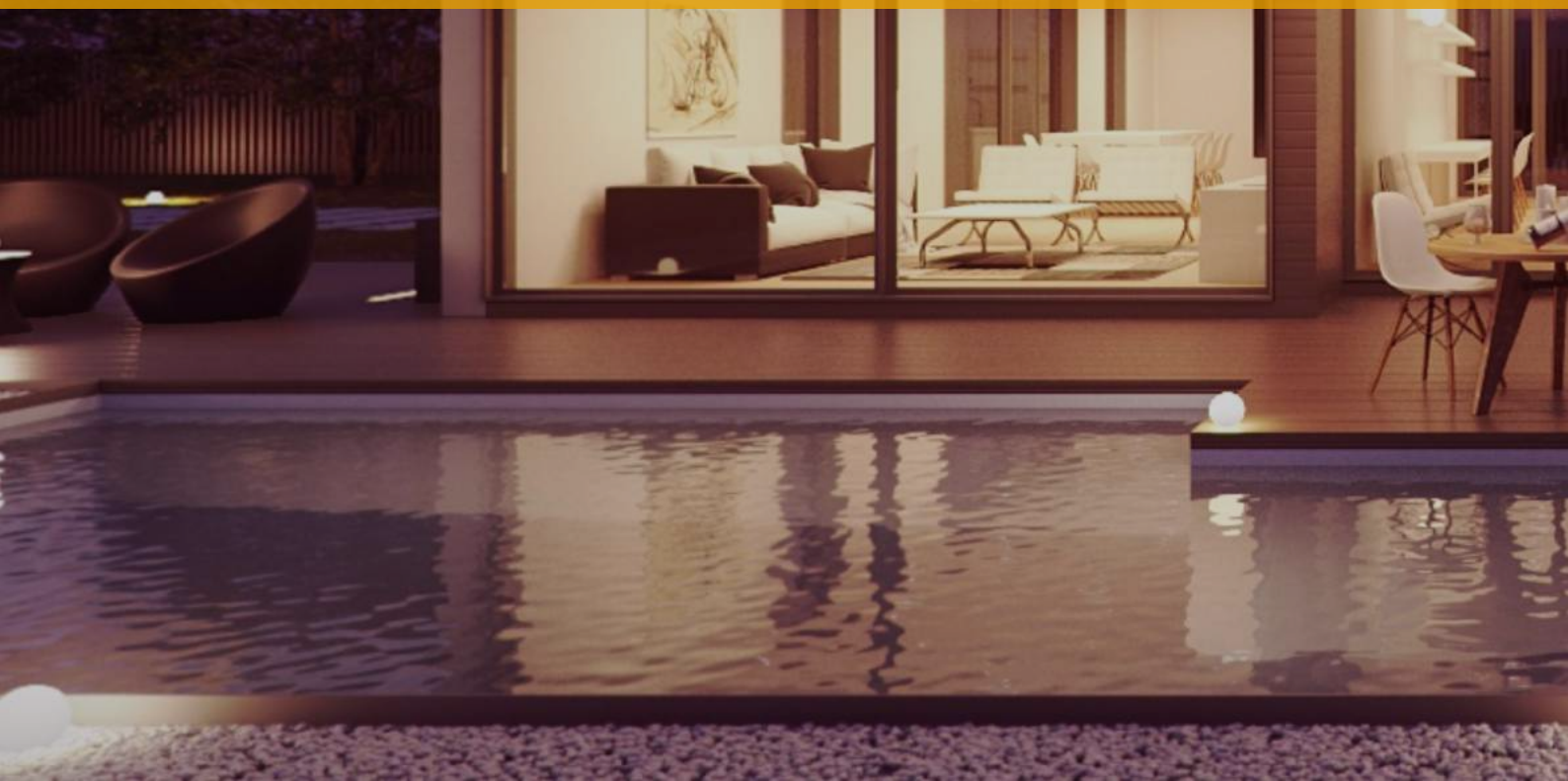
	Réseaux cellulaires	Sigfox	LoRa
Quantité de données	Importante	Faible 10/100 bits/s	Faible 0,3/50 kbits/s
Consommation	Grande	Faible	Faible
Prix	€€€	€	€
Présence nationale	Très bonne	Bonne	En cours
Présence mondiale	Bonne	En cours 19 pays	En cours

Les réseaux courte portée

	Wifi	Bluetooth 5.0	Zwave
Quantité de données	600 mbits/s	4 mbits/s	40kbits/s
Consommation	Très importante	Faible	Très forte
Prix	€€	€€	€
Présence nationale	Réseau universel	Nouvelle version	Présent
Présence mondiale	Réseau universel	Nouvelle version	Présent

La sécurité connectée

La sécurité de l'habitat est l'une des principales attentes des utilisateurs d'objets connectés. De la prévention des accidents domestiques à l'alerte en cas d'intrusion, un large panel d'objets connectés existe et propose des solutions de plus en plus pointues. Les premiers à être apparus sont les alarmes et caméras connectées qui préviennent en cas d'intrusion. Nombre de détecteurs (fumée, inondation) sont présents sur le marché afin de prévenir des risques domestiques.



Les principaux risques

Une défaillance technique de l'objet peut entraîner une multitude de risques. Cette défaillance peut être due à un virus, à un piratage ou aux conditions météorologiques. Un défaut de sécurité de l'objet peut permettre à une personne mal intentionnée de se connecter au réseau domestique et d'espionner les informations qui y transitent. Elle pourra savoir à quel moment la maison est vide et s'y introduire en ayant au préalable désactivé tous les objets prévenant le propriétaire.

En outre, lorsque l'appareil est en extérieur il est sujet aux variations climatiques et météorologiques (orage, vents violents, fortes pluies...). Ces évènements peuvent provoquer une coupure de courant ou un court-circuit bloquant l'utilisation de l'objet, l'utilisateur pouvant se retrouver bloqué à son domicile ou ne pas être informé de la survenance d'un danger critique.

La sécurité technique

Le choix d'appareils domotiques équipés de batteries et pouvant fonctionner sans secteur est primordial. L'hébergement des données dans le nuage peut poser des problèmes pour la vie privée des personnes en cas de divulgation des données. Cependant, utilisé de manière sécurisé et en complément d'un hébergement local ce mode de stockage peut permettre la récupération de données essentielles.

Là encore les mesures de sécurité les plus élémentaires (chiffrement des données, utilisation d'un mot de passe fort, chiffrement des transferts) doivent être prévues par le constructeur pour garantir la protection des données personnelles des utilisateurs.

La sécurité juridique

Le traitement des données collectées par les objets de domotique permet de déterminer la composition du foyer familial et les habitudes de vie de ses habitants. Les données collectées sont particulièrement intimes, d'autant plus que certains de ces objets collectent des données biométriques.

Il est nécessaire pour le concepteur de s'assurer du respect des dispositions relatives à la protection des données personnelles notamment en réalisant une étude d'impact sur la vie privée et en intégrant la sécurité dès la conception de son produit.

Pour aller plus loin

La caméra de surveillance, d'intérieur ou d'extérieur, fait partie des produits phares de la catégorie des objets domotique connectés. Associée à des alarmes et à des détecteurs de présence et de fumée, elle permet la surveillance de son domicile à distance.

L'énergie connectée

Le prix élevé des objets connectés peut empêcher les consommateurs de passer à l'achat. Or, ce coût est rentabilisé lorsque l'appareil permet de réaliser des économies d'énergie. Grâce à eux, l'utilisateur peut réduire ses factures d'électricité, de gaz et d'eau en contrôlant à distance la température des pièces de sa maison ou en surveillant le temps passé sous la douche. Désormais, connecter sa maison participe à la protection de l'environnement.

Les principaux risques

Ces produits sont très prisés par les pirates informatiques en raison de leur nombre et parce qu'ils constituent une porte ouverte sur le réseau d'un foyer. Avec cet accès, les intrus peuvent modifier la température d'un extrême à un autre ou effrayer les habitants en éteignant et rallumant la lumière successivement. La personne s'étant infiltrée dans le réseau peut potentiellement avoir accès à toutes les données qui y circulent. Elle peut alors utiliser les données collectées pour préparer un cambriolage, ou revendre les données récupérées à des professionnels à des fins de prospections commerciales.

Les défauts de fonctionnement ou de sécurité peuvent avoir des conséquences dramatiques sur le plan sanitaire notamment en présence de personnes vulnérables (radiateur qui ne chauffe plus la chambre d'un bébé...).

La sécurité technique

Le concepteur devra mettre en place différents outils techniques pour limiter les risques de défaillance ou d'intrusion. Des mesures simples comme le chiffrement des données, l'authentification par un pseudonyme et un mot de passe et la mise à jour régulière des logiciels sont essentielles. L'action mécanique doit rester possible afin de ne pas créer de situations à risques en cas de coupure de courant ou d'intrusion sur le réseau.

La sécurité juridique

Les objets connectés de cette catégorie peuvent recueillir quelques données personnelles comme la composition du foyer familial, l'âge des habitants et l'adresse de la maison. Le concepteur doit minimiser le traitement de données personnelles au strict nécessaire. A titre d'exemple, la collecte des noms et prénoms des habitants est inutile, le concepteur doit permettre l'utilisation d'un pseudonyme. En revanche, l'âge peut être nécessaire afin de régler la température en fonction qu'il s'agisse d'une chambre d'enfant ou d'adulte.

Pour aller plus loin

En novembre 2016, des universitaires ont souhaité prouver le manque de sécurité des ampoules connectées (1). Grâce à une fausse mise à jour envoyée sur un ordiphone connecté à une ampoule, les chercheurs ont réussi à en prendre le contrôle. Ainsi ils pouvaient faire varier la lumière, en changer la couleur et surtout contrôler tous les objets présents sur le même réseau.

L'électroménager connecté

L’internet des objets est un nouveau secteur de croissance pour les constructeurs d’électroménager. Réfrigérateurs, cafetières, ou encore aspirateurs peuvent désormais se connecter à l’ordiphone. L’aspect gadget freine encore beaucoup de potentiels acheteurs. Néanmoins, ces produits du quotidien 2.0 présentent des avantages certains dès lors que les concepteurs prennent toutes les mesures de sécurité nécessaires.

Les principaux risques

L'électroménager connecté est faiblement sécurisé ce qui facilite les intrusions par des pirates informatiques. Ainsi, un individu malveillant peut accéder au réseau domestique en prenant le contrôle de l'un des appareils du foyer (2). Il peut alors, à l'insu des habitants, observer leurs habitudes de vie. Des spécialistes de la sécurité informatique ont décelé une première intrusion en 2014 où des réfrigérateurs ont été le point de départ à un envoi massif de courriels indésirables.

La sécurité technique

Sur le plan technique le concepteur devra en plus des mesures classiques de chiffrement et d'authentification par mot de passe, installer un contrôle parental afin que les enfants ne puissent passer des commandes seuls. La mise à jour régulière des logiciels et des pare-feu est essentielle afin d'assurer l'efficacité des produits.

Le concepteur doit permettre l'interopérabilité entre les différents objets pour que l'utilisateur puisse associer tous ses appareils électroménagers. Un problème de connectivité ne doit pas empêcher le fonctionnement de l'objet. Le consommateur doit être en mesure d'utiliser normalement l'appareil sans que celui-ci soit connecté au réseau.

La sécurité juridique

Les données personnelles recueillies par cette catégorie d'objets sont l'adresse IP, le courriel, le numéro de téléphone et l'adresse postale. Les noms et prénoms ne sont pas nécessaires au bon fonctionnement de l'appareil. Le concepteur doit indiquer au consommateur que l'utilisation d'un pseudonyme est possible.

En outre, la transmission de ces données à des partenaires commerciaux doit être strictement encadrée. Elle doit être encadrée par une clause contractuelle et un recueil exprès du consentement de la personne concernée. Il doit également être possible pour l'utilisateur de demander la suppression de toutes les données recueillies par l'objet.

Pour aller plus loin

La première cyberattaque via des objets connectés de 2014 a été suivi par de nombreuses autres. Cet exemple prouve l'importance de prévoir la sécurité dès la conception du produit. Les industriels doivent prendre conscience que leur produit peut être la cible d'une intrusion et ainsi prendre les mesures nécessaires afin d'empêcher qu'il ne devienne une arme capable d'infiltrer d'autres réseaux.

La santé connectée

Et si demain le corps humain était un objet connecté ? La question est bien en mesure d'être posée devant la multiplication des données issues de la quantification personnelle. Cette pratique consiste à mesurer différentes actions relatives à son corps comme la fréquence cardiaque ou le nombre de pas effectués en une journée. Les principaux domaines concernés sont ceux de la nutrition, de la forme physique et du sommeil avec des objets tels que des glucomètres, tensiomètres, balances...

Les principaux risques

Le plus grand risque concerne la sécurité physique des personnes. En effet, la prise de contrôle de l'objet connecté par une personne malveillante lui offre un pouvoir d'action direct sur l'état de santé du propriétaire. Un individu a ainsi réussi à prendre le contrôle du pacemaker d'une personne souffrant de problèmes cardiaques (3). Le risque existe également en cas de défaillances techniques impliquant des données erronées dues à un capteur non suffisamment performant.

Le second risque peut concerner l'accès à ces informations par les assurances, mutuelles ou banques. Ces dernières pourraient exercer une surveillance excessive sur les données, afin de moduler leurs offres et tarifs en fonction de l'évolution des résultats.

La sécurité technique

Les concepteurs doivent être particulièrement vigilants sur la protection des données gérées par les objets connectés de santé. En plus des mesures habituelles, chiffrement des données, authentification forte avec mot de passe, le fabricant devra sécuriser le transfert et le stockage des données. Un outil de réglage doit pouvoir permettre à la personne concernée de modifier son consentement à la transmission des données.

Les industriels doivent assurer la fiabilité et la précision des données recueillies et annoncer la marge d'erreur possible. Pour son bon fonctionnement l'appareil doit prendre en compte les aspects extérieurs tels que le climat, l'altitude...

La sécurité juridique

Les données collectées par les objets connectés du commerce ne sont pas qualifiées de données de santé au sens de la loi. En effet, seuls les objets professionnels et reconnus comme étant des dispositifs médicaux, collectent des données de santé. Les autres données sont qualifiées de données de bien-être et échappent ainsi au régime juridique strict des données sensibles. Pour ces dernières, le principe est que leur collecte est interdite sauf si le consentement explicite de la personne a été recueilli.

Pour les données de bien-être, si le régime est moins rigoureux, leur proximité avec les données de santé oblige le concepteur à assurer une protection similaire à celle des données de santé.

Pour aller plus loin

Les accessoires portables visaient initialement à mesurer ses performances physiques et à suivre son état de santé. Désormais le bien-être mental intéresse les concepteurs. Des bracelets ou colliers connectés déterminent l'état de stress du porteur en analysant la respiration ou le rythme cardiaque. Des conseils sont ensuite prodigués via l'application.

Le sport connecté

Avec la santé, le domaine du sport s'inscrit dans la démarche de quantification personnelle. L'activité sportive est mesurée afin d'aider l'utilisateur à améliorer ses performances et lui donner une source de motivation. Les montres et bracelets sont les produits les plus connus et consommés. Ils permettent de mesurer la fréquence cardiaque, le nombre de pas ou encore les calories brûlées. Les concepteurs se tournent désormais vers l'équipement classique du sportif : tapis de gym, corde à sauter, raquettes...

Les principaux risques

Le sport connecté engendre des risques d'atteinte à la vie privée. La plupart des objets, notamment les montres et bracelets, proposent une géolocalisation qui permet de tracer le parcours suivi par leurs utilisateurs. Ces derniers sont ensuite incités à partager leurs performances sur les réseaux sociaux afin d'obtenir encouragements et félicitations. Or, ce partage d'informations laisse la possibilité à des individus malveillants de savoir précisément quelles sont les habitudes de déplacement du sportif. Les marques spécialisées peuvent également accéder aux données et exercer alors une opération de marketing ciblé pouvant être abusive.

De même qu'avec les données de santé, les assurances et mutuelles peuvent analyser les performances de la personne afin d'adapter leurs contrats. Un grand groupe d'assurance s'est associé à une célèbre entreprise d'objets connectés et a offert des bracelets connectés aux souscripteurs de l'une de ses complémentaires santé (4).

La sécurité technique

Le concepteur doit avant tout limiter les risques liés à l'exposition des ondes électromagnétiques. L'une des solutions possibles peut être l'utilisation hors ligne de l'appareil. L'analyse des données recueillies se fera lors de la réactivation de la connexion.

De même les capteurs doivent permettre un relevé précis des données afin que l'utilisateur puisse se fier aux résultats. Le constructeur doit évaluer la marge d'erreur possible et en informer l'utilisateur.

La sécurité juridique

Ces objets et leurs applications peuvent collecter des données personnelles comme l'adresse IP, le numéro de téléphone et la date de naissance. Surtout ils ont la capacité de recueillir des données très proches des données sensibles, notamment les informations relatives à la santé de l'individu. Ainsi le concepteur doit obligatoirement obtenir le consentement de l'utilisateur. Il ne doit demander que les données strictement nécessaires à l'application.

Pour aller plus loin

Les concepteurs ne visent plus seulement les particuliers mais également les sportifs de haut niveau. Le concepteur a tout intérêt à mettre au point un système sécurisé à même de convaincre les professionnels.

L'enfance connectée

Les utilisateurs convaincus de l'utilité des objets connectés s'intéressent aussi à ceux destinés à leurs enfants. Une multitude d'appareils leur sont aujourd'hui dédiés. Initialement, ces objets répondaient à un besoin de surveillance avec des écoutes bébé ou des balises GPS. Le panel s'est élargi avec des objets connectés liés à la puériculture (biberon, landau) et à la santé (balance, thermomètre). Les fabricants de jeux ajoutent aussi de la connectivité à leurs produits.

Les principaux risques

Avec un public ciblé aussi délicat que les jeunes enfants, cette catégorie d'objets connectés présente des risques certains. Au-delà des problèmes sanitaires liés à l'exposition des enfants aux ondes électromagnétiques, des risques d'atteinte à la sécurité physique de l'enfant ou de surveillance d'une famille sont avérés .

Un autre risque concerne la géolocalisation permanente des enfants. Les parents les équipent de vêtements ou bracelets connectés qui leur permettent de savoir précisément et à tout moment, où sont leurs enfants. Ici la sécurité physique est directement menacée puisqu'en cas de piratage l'auteur de l'acte pourra suivre et observer l'enfant.

La sécurité technique

Le concepteur doit assurer la vie privée de l'enfant et sa sécurité physique. Les mesures de base telles que le chiffrement des données et l'authentification de l'utilisateur doivent être appliquées. Le jouet doit pouvoir être utilisé même sans connectivité et la géolocalisation doit pouvoir être coupée à partir d'un ordiphone.

Le concepteur doit veiller à utiliser une connectivité qui transmet le moins d'ondes possibles. Notamment, pour les objets utilisés lors du sommeil de l'enfant, la transmission et l'analyse des données ne doit se faire qu'au réveil et sur un ordiphone éloigné de l'enfant.

La sécurité juridique

Les données recueillies peuvent être de différents types. Elles peuvent concerner la santé de l'enfant, sa géolocalisation mais également toutes les informations qu'il a pu transmettre notamment en parlant à son jouet connecté. Le concepteur devra veiller à bien informer les parents sur tous les risques existants afin que ces derniers réalisent l'achat en toute connaissance de cause. Parmi les aspects à évoquer se trouvent les partenariats commerciaux réalisés (publicité via l'objet, analyse comportementale, échange de données...).

Pour aller plus loin

Un récent cas de faille de sécurité a été rendu public (5). Des pirates informatiques ont réussi à communiquer avec un enfant via sa poupée connectée. La connexion se faisait par bluetooth, or celle-ci n'était pas sécurisée constituant une véritable porte ouverte aux indivus malveillants.

Les drones connectés

Initialement réservés aux militaires pour un rôle de surveillance, les drones sont devenus très attractifs pour le grand public. Cet appareil de loisir se pilote à distance via une télécommande ou des applications reliées à un ordiphone ou à une tablette. Les drones étant de plus en plus sophistiqués, les amateurs ont la possibilité d'observer, filmer et transporter ce qu'ils désirent.

Les principaux risques

La plupart des drones sont discrets et peuvent accéder à n'importe quel endroit même ceux normalement inaccessibles. Les plaintes des particuliers se sentant observés sont de plus en plus nombreuses. (6) Plusieurs heurts, parfois évités de justesse, ont été recensés depuis leur apparition (7).

Les activités illégales telles que le trafic de drogues, d'armes ou les activités de recel sont facilités par l'utilisation de ces appareils. Pis encore, des pirates informatiques ont mis au point un drone qui a la capacité de pirater n'importe quel système de sécurité même ceux se trouvant dans des structures isolées (8).

La sécurité technique

Sur le plan technique, le concepteur se doit de mettre en place tout ce qui est nécessaire à la protection des données personnelles et ce dès la conception de son produit (notion de privacy by design). Des systèmes permettant d'informer les individus lorsqu'un drone les survole devront être pensés (signalement sonore...).

Un contrôle technique annuel devrait être programmé afin d'anticiper toute faille. Le concepteur devra intégrer les mesures de sécurité classiques comme le chiffrement des données, l'authentification afin de permettre l'identification et la certification de l'utilisateur.

La sécurité juridique

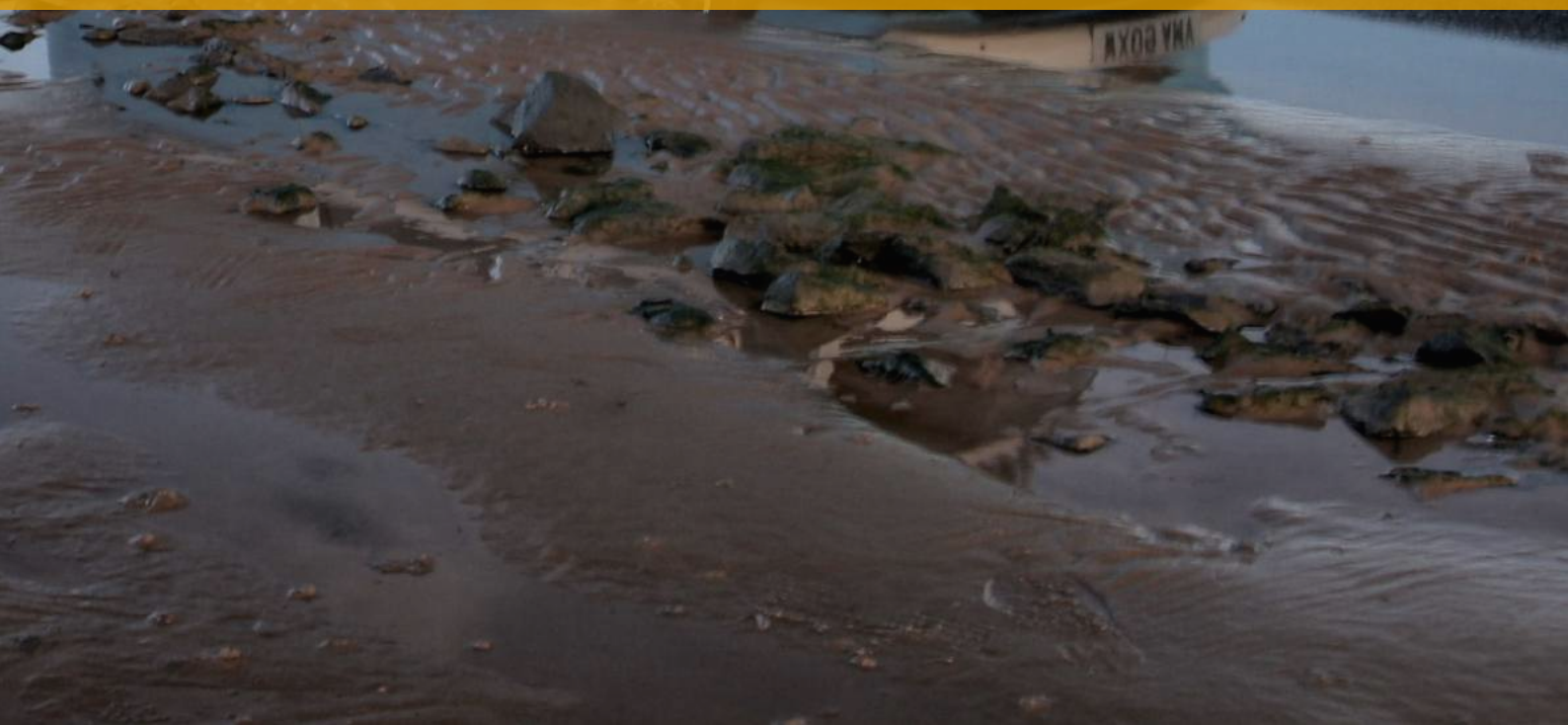
Face à ces complications, le Ministère de l'écologie, du développement durable et de l'énergie français a publié des règles afin d'assurer la sécurité des personnes tout en garantissant l'exploitation civile des aéronefs. Ces règles imposent l'interdiction de survoler des personnes, le respect des hauteurs maximales de vol, l'interdiction de perdre son drone de vue, d'utiliser son drone au-dessus de l'espace public en agglomération, d'utiliser son drone à côté des aérodromes, de survoler des sites sensibles ou protégés et enfin de ne pas diffuser ses prises de vues sans l'accord des personnes concernées. A noter que l'utilisation non conforme d'un drone est passible d'un an d'emprisonnement et de 75 000€ d'amende.

Pour aller plus loin

Le plus connu des réseaux sociaux a créé son propre drone (9). Cet appareil aux dimensions énormes (l'envergure d'un Boeing 737) a pour but de mettre en œuvre un gigantesque réseau de connectivité.

La voiture connectée

Véhicules électriques, autonomes ou connectés, le marché de l'automobile n'échappe pas aux évolutions techniques et s'inscrit totalement dans la révolution de l'internet des objets. Une étude du cabinet IDATE affirme que d'ici 2020 plus de 420 millions de voitures connectées à Internet seront en service (10). Les concepteurs annoncent une diminution des accidents de la route grâce à ces voitures intelligentes qui assureront la sécurité des passagers. Néanmoins, les industriels devront penser aux nouvelles problématiques pesant sur ces véhicules du futur.



Les principaux risques

Le véhicule connecté recueille quantité d'informations sur son propriétaire. En effet, sa conduite est minutieusement détaillée et tous ses déplacements sont recueillis. Les constructeurs proposent également des services optionnels qui sont en théorie gratuits. Cependant, ces divers services tels que le trafic en temps réel ou la recherche de stations essence, sont délivrés contre de nouvelles données (itinéraires suivis, entretien du véhicule). Le constructeur automobile a alors accès à des informations complémentaires qu'il peut décider de vendre à des partenaires commerciaux.

Enfin, comme tout appareil de l'Internet des objets, la voiture connectée risque le piratage informatique. La sécurité physique des personnes est directement menacée.

La sécurité technique

Pour rassurer les utilisateurs, les véhicules connectés doivent prouver que la sécurité physique de l'objet est aussi sûre que celle des véhicules classiques. Pour éviter les intrusions, l'architecture du système informatique doit être sécurisée notamment à l'aide de pare-feu, de mises à jour régulières des logiciels et de chiffrement des données.

Le système d'authentification doit être particulièrement performant afin d'éviter les vols de véhicules et de données. En cas de problèmes, une mise en relation automatique doit être faite entre le véhicule et un conseiller.

La sécurité juridique

Le traitement des données collectées par les objets de domotique permet de déterminer la composition du foyer familial et les habitudes de vie de ses habitants. Les données collectées sont particulièrement intimes, d'autant plus que certains de ces objets collectent des données biométriques.

Il est nécessaire pour le concepteur de s'assurer du respect des dispositions relatives à la protection des données personnelles notamment en réalisant une étude d'impact sur la vie privée et en intégrant la sécurité dès la conception de son produit.

Pour aller plus loin

En cas d'accident de la route, la loi française fait peser une présomption de responsabilité sur le conducteur. La question se pose de savoir qui du constructeur ou du propriétaire sera responsable dans le cas d'une voiture autonome. Certains constructeurs ont d'ores et déjà admis leur responsabilité en cas d'accident durant le mode autnoomie (11). De quoi rassurer les utilisateurs en attendant la fixation d'un nouveau cadre règlementaire.

La ville connectée

La ville intelligente lie technologies numériques et réseaux d'informations afin de favoriser une meilleure gestion urbaine. La ville du futur propose un meilleur cadre de vie pour ses habitants grâce à des actions dans divers domaines tels que la gestion des déchets et l'énergie. L'autre défi important concerne le développement de la mobilité intelligente afin de rendre les transports plus sûrs, économes et écologiques.

Les principaux risques

Vivre dans une ville connectée n'est pas sans risque pour la vie privée de ses habitants. En effet, retracer le parcours d'une personne peut se révéler très facile grâce aux transports connectés et à la présence de caméras de surveillance sur le bord des routes. Toutes les données recueillies ont vocation à être analysées afin d'améliorer les services proposés. Les entreprises ont un intérêt certain à récupérer ces données qui leur permettent de procéder à des actions de marketing ciblé.

Enfin, la ville connectée pourrait rapidement devenir un lieu de non droit si elle est piratée. Les auteurs auraient la main sur tous les services, des transports aux réseaux d'énergie et pourraient alors bloquer la ville.

La sécurité technique

Pour réduire les menaces de défaillance technique ou de piratage des objets, les concepteurs devront vérifier l'identification et la bonne connexion de chaque appareil intégré au réseau de la ville. Pour parvenir à une gestion de risques efficace, une équipe technique devra être chargée de réaliser des contrôles et des plans de restauration réguliers.

Un classement des risques doit être défini afin de réfléchir dès la conception du produit aux solutions possibles. La pérennité du réseau passera par une interopérabilité totale entre les différents objets.

La sécurité juridique

La ville connectée se doit d'assurer l'information et la sensibilisation du citoyen sur ses droits concernant ses données. Le principe de pertinence, qui implique qu'une donnée soit recueillie pour une finalité définie, ne doit pas souffrir de la réorientation. Cette notion consiste à réutiliser les données pour d'autres fonctions que celles prévues initialement.

La ville connectée peut être bénéfique aux habitants si elle se base sur l'intérêt commun. La rédaction d'une charte sera utile afin de préciser que seul l'intérêt commun est visé et prime sur les intérêts individuels et commerciaux.

Pour aller plus loin

Sans réelles protections pour la vie privée de ses habitants, la ville de Singapour se base sur l'utilisation des données à grande échelle afin de réguler le trafic routier, l'acheminement de l'eau, la distribution d'énergie, le tri des ordures...(12)

IoTrust

Notes

(1) Elsa Trujillo, « Pourquoi les ampoules connectées sont une cible de choix pour les pirates » [en ligne], in lefigaro.fr, paru le 04 novembre 2016, consulté le 28 novembre 2016, disponible sur :
http://www.lefigaro.fr/secteur/high-tech/2016/11/04/32001-20161104ARTFIG00007-pourquoi-les-ampoules-connectees-sont-une-cible-de-choix-pour-les-pirates.php

(2) Philippe de Poulpiquet, « Piratage massif de sites Internet : quand les objets connectés attaquent » [en ligne] in leparisien.fr, paru le 23 octobre 2016, consulté le 13 décembre 2016, disponible sur :
http://o.nouvelobs.com/high-tech/hacker-ouvert/20140118.OBS2913/decouverte-d-une-premiere-cyberattaque-contre-des-objets-connectes.html

(3) Baudoin Eschapasse, "Les pacemakers dans le collimateur des pirates informatiques" [en ligne] in lepoint.fr, paru le le 02 février 2016, consulté le 14 décembre 2016, disponible sur :
http://www.lepoint.fr/high-tech-internet/le-jour-ou-les-hackers-frapperont-au-coeur-02-02-2016-2014746_47.php

(4) Elsa Bembaron, « Axa s'associe à Withings dans la santé connectée », [en ligne], in lefigaro.fr, paru le 2 juin 2014, disponible sur :
http://www.lefigaro.fr/secteur/high-tech/2014/06/02/32001-20140602ARTFIG00239-axa-s-associe-a-withings-dans-la-sante-connectee.php

(5) UFC que choisir, « Jouets connectés : Alerte sur la sécurité et les données personnelles », [en ligne], in quechoisir.org, paru le 6 décembre 2016, consulté le 7 décembre 2016, disponible sur :
https://www.quechoisir.org/action-ufc-que-choisir-jouets-connectes-alerte-sur-la-securite-et-les-donnees-personnelles-n23355/

(6) Renaud, « Drones : le nombre de plaintes explose en Angleterre », [en ligne], in objetconnecte.net, paru le 17 décembre 2015, consulté le 1er décembre 2016, disponible sur : http://www.objetconnecte.net/angleterre-les-drones-inquietent-la-population/

(7) Anne-Katell Mousset, « Quand un drone entre en collision avec un avion, ça fait des dégats », [en ligne], in usinenouvelle.com, paru le 9 janvier 2017, consulté 9 janvier 2017, disponible sur :
http://www.usinenouvelle.com/article/photo-quand-un-drone-entre-en-collision-avec-un-avion-ca-fait-des-degats.N485314

(8) Barthélémy Touraine, « Un drone qui pirate les objets connectés depuis le ciel » [en ligne], in stuffi.fr, paru le 11 août 2015, consulté le 12 décembre 2016, disponible sur:
http://www.stuffi.fr/un-drone-qui-pirate-les-objets-connectes-depuis-le-ciel/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Stuffi+%28Stuffi+-+L%27actualit%C3%A9+des+objets+connect%C3%A9s%29

(9) Gaëtan R, « Aquila : le drone de Facebook fait l'objet d'une enquête aux USA », [en ligne], in objetconnecte.com, paru le 27 novembre 2016, consulté le 28 novembre 2016, disponible sur :
http://www.objetconnecte.com/aquila-facebook-defaillance-221116/

(10) Christophe Lagane, « La voiture connectée conduira les bénéfices des opérateurs » [en ligne], in silicon.fr, paru le 1er décembre 2015, consulté le 15 décembre 2016, disponible sur :
http://www.silicon.fr/voiture-connectee-conduira-benefices-operateurs-132862.html

(11) Mathieu M, « Voiture autonome : Volvo se portera responsable en cas d'accident », [en ligne], in generation-nt.com, paru me 8 octobre 2015, consulté le 14 décembre 2016, disponible sur :
http://www.generation-nt.com/voiture-autonome-volvo-se-portera-responsable-cas-accident-actualite-1920218.html

(12) Maud Duforest, « Singapour, une ville (Etat) intelligente et surtout durable, [en ligne], in weave.eu, paru le 6 octobre 2016, consuté le 13 décembre 2017, disponible sur :
http://ristretto.weave.eu/2016/10/06/singapour-ville-etat-intelligente-surtout-durable/

IoTrust

Bibliographie

Ouvrages :

-Hersent O. 2014, «L'internet des objets : les principaux protocoles M2M et leur volution vers IP». Dunod. 384 pages.

-Dosquet E., Acas R., Dosquet F. et al, 2016, «Objets connectés : la nouvelle révolution numérique». Eni Editions. 190pages.

Articles de périodiques :

-Marino Laure, «To be or not to be connected: ces objets connectés qui nous espionnent», in *Recueil Dalloz*, 2014, p.29.

-Rozenfeld Sylvie, «Thomas Roche : la santé une donnée très connectée», in *Expertises,* mars 2015, p.91-95.

-Louvet Benoît, «Données de santé, réflexions à propos du quantified Self», in *Expertises*, avril 2015.

-Debiès Elise, «L'ouverture et la réutilisation des données de santé: panorama et enjeux», in *Revue de droit sanitaire et social*, août 2016, p.697.

-Dary Mathieu et Benaissa Leïla, «Privacy by Design: un pricipe de protection éduisant mais complexe à mettre en oeuvre», in *Dalloz IP/IT*, septembre 2016, p.46

-Geffray Edouard, «Quelle protection des données personnelles dans l'univers de la robotique ?», in *Dalloz IP/IT*, septembre 2016, p.295

-Martial-Braz Nathalie, «Objets connectés et responsabilité», in *Dalloz IP/IT*, septembre 2016, p.399

-Daoud E. et Plénacoste F., «Cybersécurité et objets connectés», in *Dalloz IP/IT*, septembre 2016, p.409

Sites internet :

-Ali Benfattoum «Les LPWAN,ces nnouveaux réseaux de l'internet des objets», in *frugalprototype.com*, paru le 26 décembre 2015, consulté le 12 décembre 2016, disponible sur :
http://www.frugalprototype.com/les-lpwan-ces-nouveaux-reseaux-de-linternet-des-objets/

-Claude Soula, «Les objets connectés n'intéressent personne» [en ligne], in *tempsreel.nouvelobs.com*, paru le 10 décembre 2016, consulté le 21 février 2017, disponible sur :
http://tempsreel.nouvelobs.com/economie/20161209.OBS2448/les-objets-connectes-n-interessent-personne.html

Textes institutionnels - Rapports :

-CNIL, "Avis sur l'Internet des objets" [en ligne], in *cnil.fr*, 2 octobre 2014, consulté le 22 novembre 2016, disponible sur : http://www.cnil.fr/linstitution/actualite/article/article/communique-g29-avis-sur-linternet-des-objets/

-Conseil National de l'Ordre des Médecins, «Santé connecté : de la e-santé à la santé connecté, le livre blanc du Conseil National de l'Ordre des Médecins» [en ligne], in *conseil-national.medecin.fr,* paru le 15 janvier 2015, consulté le 23 novembre 2016, disponible sur : http://www.conseil-national.medecin.fr/sites/default/files/medecins-sante-connectee.pdf

-Institut Montaigne, «Big Data et objets connectés: Faire de la France un champion de la révolution numérique», avril 2015.

-Haute autorité de santé, « Réféntiel de bonnes pratiques sur les applications et les objets onnectés en santé», [en ligne], in *has-sante.fr*, paru le 7 novembe 2016, consulté le 18 novembre 2016, disponible sur:
http://www.has-sante.fr/portail/jcms/c_2681915/fr/referentiel-de-bonnes-pratiques-sur-les-applications-et-les-objets-connectes-en-sante-mobile-health-ou-mhealth

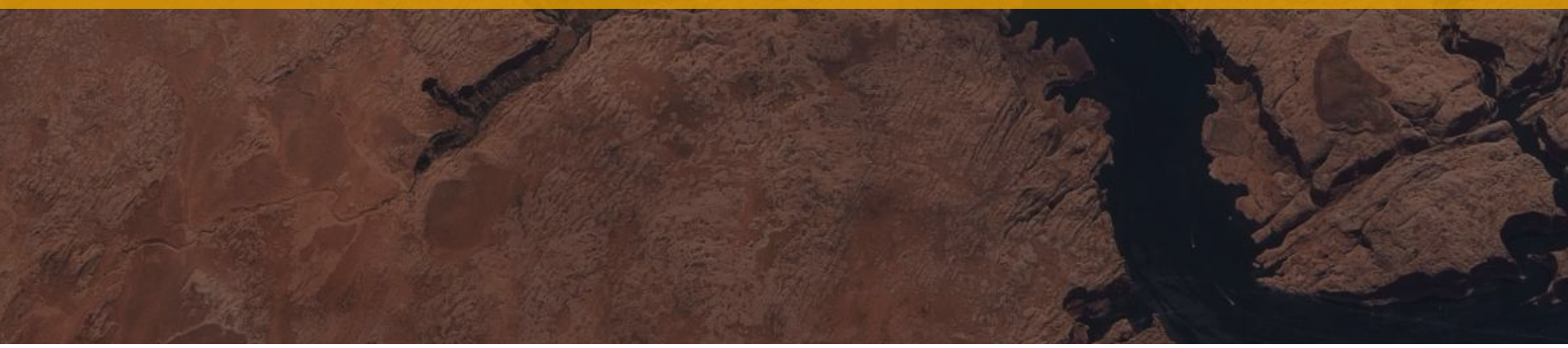
Les objets connectés :

Etat des lieux des risques juridiques et techniques

Par Flavie BADREAU

Avec la démocratisation des téléphones intelligents et la large disponibilité d'Internet, l'univers des objets connectés est en fulgurante expansion. Dans un marché dynamique et en constante mutation, l'urgence était pour les acteurs du secteur de concevoir et de vendre leur produit. La priorité n'était pas portée sur la sécurité informatique et/ou sur la protection de la vie privée des utilisateurs. La prise de conscience de l'importance de ces enjeux est venue avec la survenance d'évènements de piratage à grande échelle des objets connectés. A ces risques, s'ajoute la nouvelle réglementation européenne sur la protection des données personnelles qui renforce les obligations des acteurs économiques du marché de l'internet des objets.

L'ambition de cet ouvrage est d'apporter une vision globale du secteur des objets connectés et d'alerter les différents acteurs sur les risques techniques et juridiques liés au défaut de sécurisation. Dans une approche pédagogique, les risques et les premières solutions sont présentés par famille d'objet.



IoTrust

Un projet soutenu et financé par
la fondation MAIF, la société Digitemis et l'école ESIEA.