DEROULEZ
AVOCAT

LIVRE BLANC

Enjeux juridiques des objets connectés

Photo by NASA on Unsplash

Avant-propos

Pourquoi un livre blanc consacré aux enjeux juridiques des objets connectés ?

Pour évoquer tout d'abord la montée en puissance du marché des objets connectés, la révolution des usages et des pratiques comme les combinaisons technologiques particulièrement innovantes dans ce domaine mêlant l'IA, la blockchain, le Big Data ou encore le recours à la 5G… Il ne s'agit pas ici d'être exhaustif mais de souligner la rapidité et la force de ces évolutions comme leurs probables conséquences.

Pour analyser ensuite les enjeux juridiques liés à l'internet des objets et aux objets connectés, à leur utilisation et aux responsabilités qui en découlent, dans tous les domaines. Analyse qui implique de prendre en compte les projets législatifs et réglementaires en cours dessinant le droit de demain et pour faire preuve de prospective.

Pour apporter également notre regard et notre expertise d'avocats et dégager des solutions globales et pérennes lors de la conception, de la commercialisation et de l'utilisation d'objets connectés, dans un cadre complexe et évolutif. Ce livre blanc s'inscrit dans le prolongement de nos échanges avec nos clients et prend en compte leurs questions comme leurs défis.

Bonne lecture !

Jérôme Deroulez
Avocat aux Barreaux de Paris et de Bruxelles

Table des matières

« When a thing connects to the internet, three things happen: it becomes smart, it becomes hackable and it's no longer something you own. »[1]

Les objets connectés font partie intégrante du quotidien de chacun et leur utilisation par le grand public croît chaque année, ces nouveaux usages étant considérés comme l'annonce d'une troisième révolution de l'Internet.

Les possibilités offertes par ces objets connectés dans tous les domaines (smart-grids, santé, logistique, ville intelligente etc.), les nouveaux usages qu'ils génèrent comme les challenges juridiques qu'ils suscitent ouvrent des champs de réflexion particulièrement larges.

Par ailleurs, partagés entre désir d'innovation et exigences de sécurité, les utilisateurs et les consommateurs s'interrogent légitimement sur l'intégrité, la qualité et la sécurité de ces objets connectés. La DGCCRF[2] comme la CNIL en France sont également très sensibles à ces aspects et cette dernière a déjà eu l'occasion de se prononcer concernant des jouets connectés pour enfant qui procédaient à l'enregistrement de conversations[3]. Cette autorité s'efforce aussi par des fiches pratiques[4] et par des infographies didactiques de sensibiliser les utilisateurs des dangers des objets connectés[5].

La prise de conscience des pouvoirs publics et des autorités de régulation des enjeux liés à l'explosion des usages d'objets connectés est internationale[6] et témoigne de l'actualité du sujet comme des défis à relever. Défis qui sont pluriels : sécurité des produits, protection des consommateurs, lutte contre le risque cyber, responsabilité des objets connectés etc… Défis qui peuvent aussi être analysés différemment selon le contexte propre à chaque type d'objet connecté (véhicule autonome, wearables, drones militaires etc.).

Ces questions nombreuses et pluridisciplinaires sont d'abord juridiques, pour déterminer ce qui peut être considéré comme un objet connecté, avant de tenter de tracer les contours du ou des régimes juridiques applicables aux objets connectés. L'impact des législations et des réglementations existantes ou en cours à l'échelle nationale, européenne ou internationale devra aussi être pris en compte.

La notion d'objet connecté est récente. Le premier objet connecté remonterait à 2003, avec la lampe DAL de Violet, connectée en WI-FI : « *elle pouvait s'allumer de différentes couleurs en fonction de différents événements, liés à la météo, la bourse, la pollution, les alertes Google ou encore des "envois de messages de couleurs" par sms ou email*. »[7]

Par la suite, le marché des objets connectés n'a cessé d'évoluer avec l'utilisation de nouvelles technologies comme l'intelligence artificielle ou la Blockchain qui permettent des interconnexions et des modes de communication autonome des objets sans intermédiation humaine.

Par conséquent, la notion d'objet connecté est intrinsèquement liée à celle d'internet des objets.

A ce titre, l'UIT (Union Internationale des Télécommunications) définit l'IoT comme *« une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution »*[8]. Outre Atlantique, l'Administration nationale des télécommunications et de l'information définit encore l'IoT comme *« un ensemble de dispositifs et de capteurs externes qui génèrent des données, lesquelles, grâce à une connexion internet, peuvent être analysées pour fournir des informations exploitables »*[9] et considère qu'il existe trois types de technologies IoT :

- commerciale ou industrielle
- personnelle ou mobile
- domestique

Enfin lors de l'adoption du rapport Delvaux, le Parlement européen a proposé de définir l'IoT comme *« un réseau distribué reliant des objets physiques capables de détecter ou d'agir sur leur environnement et capables de communiquer entre eux, avec d'autres machines ou ordinateurs. Les données que ces dispositifs rapportent peuvent être collectées et analysées afin de révéler des informations et de suggérer des actions qui permettront de réduire les coûts, d'accroître l'efficacité ou d'améliorer les produits et services. »*[10]

Ce que soulignent ces définitions sont leur caractère international par nature, leur forte génération et consommation de données et la nécessité d'infrastructures innovantes et robustes.

Quelles applications pour l'IoT

Dans son étude sur la cartographie des clusters d'IoT en Europe du 19 juin 2019[11], la Commission européenne a signalé la très grande diversité et variété des objets connectés.

- Smart Home : *« Une maison intelligente est une résidence qui utilise des appareils connectés à Internet pour permettre la surveillance et la gestion à distance d'appareils et de systèmes, tels que l'éclairage et le chauffage ».*
- Smart Building and Architecture : *« Les bâtiments intelligents répondent à notre utilisation des ressources et l'optimisent, en réduisant la consommation. Les bâtiments intelligents visent à minimiser l'impact sur l'environnement.*
- Smart Mobility : désigne des initiatives ayant pour objectif d'améliorer la mobilité au sein des villes afin qu'elle n'ait pas d'impact négatif sur la vie des citoyens comme sur son développement économique. Cette amélioration de la mobilité ne se limite pas à la circulation mais concerne tous les moyens de transport, la marche, le vélo, les transports publics et privés, avec un objectif commun : la réduction des coûts, de la pollution et de la durée des déplacements.
- Smart Health : « *les soins de santé intelligents se définissent par la technologie qui permet d'obtenir de meilleurs outils de diagnostic, de meilleurs traitements pour les patients et des appareils qui améliorent la qualité de vie de chacun* ». Le concept clé de la santé intelligente comprend les services de santé en ligne et de santé mobile, la gestion des dossiers électroniques, les services à domicile intelligents et les dispositifs médicaux connectés.
- Smart Farming and Food : l'agriculture et l'alimentation intelligentes représentent l'application des technologies de l'information et de la communication à la production et au suivi de l'agriculture et de l'alimentation. L'agriculture intelligente pour le climat vise à renforcer la capacité des systèmes agricoles à soutenir la sécurité alimentaire, en intégrant la nécessité d'adaptation et le potentiel d'atténuation dans les stratégies de développement agricole durable.
- Smart Industry : *« Les industries intelligentes ont un degré élevé de flexibilité dans la production, en termes de besoins de produits (spécifications, qualité, conception), de volume, de calendrier, d'efficacité des ressources et de coût, pouvant s'adapter précisément aux besoins des clients et utiliser toute la chaîne d'approvisionnement pour la création de valeur. Elle est rendue possible grâce à une approche réseau-centrée, utilisant la valeur de l'information, pilotée par les TIC et les dernières techniques de fabrication éprouvées disponibles.* »
- Smart Energy : « *Les systèmes énergétiques intelligents se concentrent sur l'inclusion d'un plus grand nombre de secteurs (électricité, chauffage, refroidissement, industrie, bâtiments et trans-*

ports) et permettent d'identifier des solutions pour la transformation en futures solutions d'énergie renouvelable et durable ».

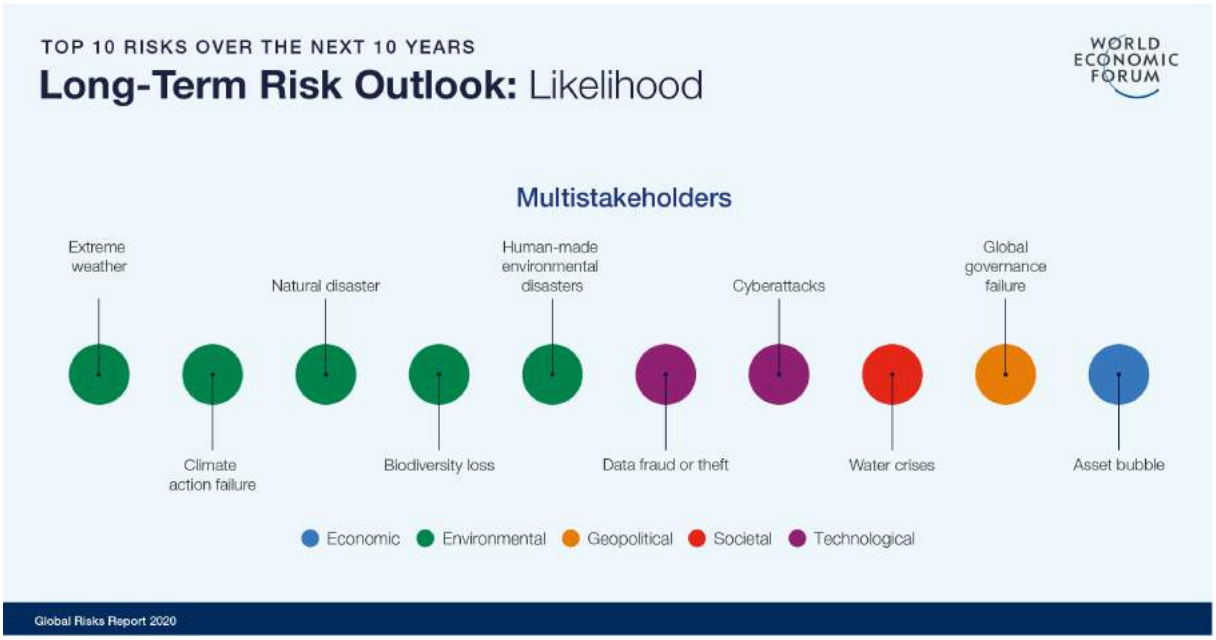
Photo by meric tuna on Unsplash

L'assistant vocal, objet connecté par excellence

Les assistants vocaux apparaissent aussi comme un symbole des objets connectés, outils incontournables dont le marché devrait peser 40 milliards de dollars en 2022[12] et s'adressant aussi bien aux particuliers qu'aux professionnels. L'assistant vocal, capable d'interaction vocale, peut lire de la musique, faire des listes de tâches, régler des alarmes, lire des podcasts et des livres audio, donner la météo, le trafic et d'autres informations en temps réel. Ces assistants vont occuper une place de plus en plus importante dans la vie des consommateurs en devenant des *personal shopper*[13] ou encore en assistant médicalement leurs utilisateurs[14] ou en interagissant avec d'autres objets connectés. Leurs usages potentiels dans la vie des affaires sont également très nombreux.

Big Data et IoT

Comme l'indique à juste titre l'ICO britannique dans son rapport de 2017 sur le « Big data »[15], le développement de l'IoT est lié à l'explosion de masses de données et à l'émergence du Big Data. Alors que les capteurs de données se multiplient, la possibi-



lité de structurer, de lire, d'agréger et d'utiliser ces mêmes données s'ouvre de façon quasi exponentielle. L'essor du Big Data et l'utilisation de ces données pose là encore de très nombreuses questions, qu'il s'agisse de la protection des données personnelles des utilisateurs ou des consommateurs, du niveau de sécurité des outils utilisés ou encore du droit applicable aux bases de données constituées.

Les enjeux actuels de l'IoT

L'explosion des cyberattaques à l'encontre des objets connectés - en hausse de 300% au premier semestre 2019[16] - fait de la sécurité de l'IoT une préoccupation majeure tant pour les fabricants, pour les individus mais également pour les entreprises qui ont recours à des objets connectés. Le tableau du World Economic Forum ci-dessus témoigne de la montée en puissance de ces risques et pose la question des garde-fous à prendre en compte.

Si la préoccupation éthique joue un rôle considérable dans la régulation des produits connectés, rien n'impose aux acteurs de l'IoT et plus largement de la technologie, de prendre de tels engagements. Pour autant, la mise en place d'un encadrement juridique semble nécessaire et les bonnes pratiques d'aujourd'hui et autres lignes directrices constituent les obligations légales de demain.

Les fiches pratiques suivantes ont pour objet d'accompagner les acteurs de l'IoT, dès le début de la conception des objets connectés, dans leur mise en conformité juridique et à jusqu'à leur commercialisation. Toutes les parties prenantes au marché des objets connectés doivent en outre avoir conscience de l'importance d'un cadre juridique propice à un développement économique pérenne.

Se posent aussi des questions en termes de sécurité technique, avec notamment l'utilisation d'objets connectés pour des attaques DDoS. Quelles technologies utiliser et quel

niveau de sécurité ? Quel protocole de communication ? Quelle certification possible des produits ?

La question de la sécurité juridique de l'IoT est aussi particulièrement délicate, dans un contexte législatif et règlementaire mouvant, tout particulièrement au sein de l'Union européenne qui se veut tête de pont des régulateurs et a déjà commencée à prendre en compte certaines problématiques, notamment en matière de protection des données :

- Comment mettre en œuvre le principe de minimisation concernant un objet connecté ?
- Quelles relations établir avec les sous-traitants ?
- Quelle marge de manœuvre lorsqu'un sous-traitant ou partenaire est le seul acteur à proposer une solution donnée ?
- Quelles obligations à la charge des partenaires commerciaux technologiques ?
- Quels types de traitements de données personnelles ?
- Quel encadrement juridique des transferts internationaux ?
- Quels outils de mise en conformité mettre en place lorsqu'il existe un risque élevé pour les droits et libertés des personnes physiques ?
- Quelles procédures d'alertes en cas de faille ?

Ces problématiques sont éminents diverses et à la mesure du foisonnement des objets connectés. Autant de questions à prendre en compte et que vous retrouverez dans les prochaines fiches.

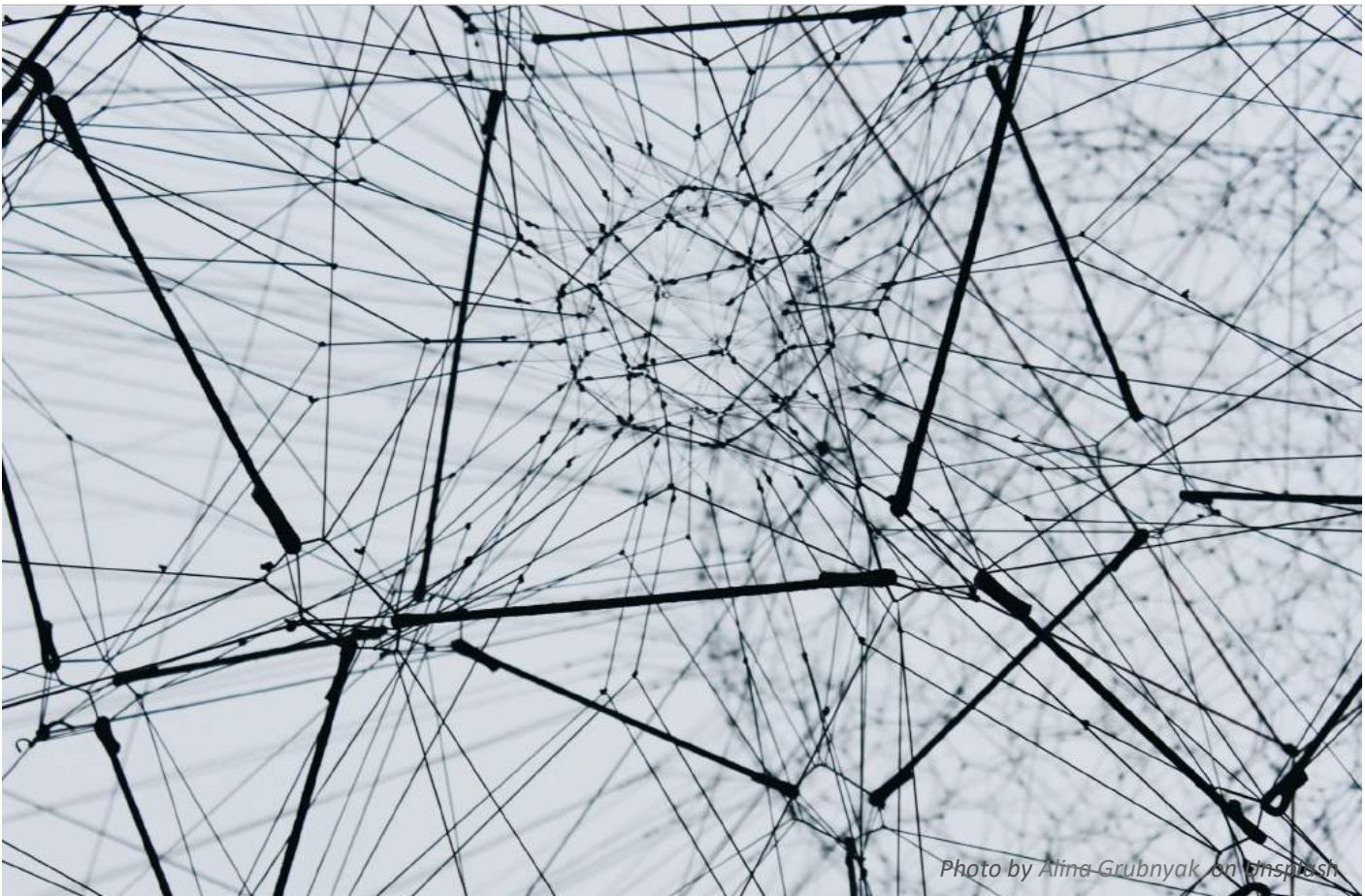


Photo by Alina Grubnyak on Unsplash

Ressources :

[1] https://www.theatlantic.com/technology/archive/2014/09/when-everything-works-like-your-cell-phone/379820/

[2] https://www.economie.gouv.fr/dgccrf/objets-connectes-sante-et-bien-etre-sont-ils-fiables

[3] https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000036142140&fastReqId=606052286&fastPos=2

[4] https://www.cnil.fr/fr/jouets-connectes-quels-conseils-pour-les-securiser

[5] https://www.cnil.fr/fr/infographie-il-etait-une-fois-lours-connecte-mal-securise

[6] https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf ; https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_FR.html ; https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

[7] https://www.objetconnecte.net/histoire-definitions-objet-connecte/

[8] https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-F&type=items

[9] https://www.itic.org/dotAsset/6e35740e-70d9-481b-a25a-255d576ec98a.pdf

[10] https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

[11] https://ec.europa.eu/digital-single-market/en/news/study-mapping-internet-things-innovation-clusters-europe

[12] https://hbr.org/2019/05/how-voice-assistants-could-change-the-way-we-shop

[13] https://hbr.org/2018/05/marketing-in-the-age-of-alexa

[14] https://www.forbes.com/sites/emmawoollacott/2019/12/09/uk-government-hands-nhs-data-to-amazon-for-free/

[15] https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[16] http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

DEROULEZ
AVOCAT

FICHE PRATIQUE N°1 – Objets connectés : un droit en construction

La « discontinuité des normes »[1] est un facteur de complications mais également d'insécurité juridique pour les acteurs de l'IoT

Les défis juridiques sont à la mesure de la diversité des usages en matière d'objets connectés et cette fiche s'efforcera de recenser les textes ayant vocation à encadrer les objets connectés comme les initiatives législatives et règlementaires en cours.

Un cadre français neutre pour l'IoT

La France dispose d'un cadre règlementaire qui permet d'encadrer en partie l'utilisation des objets connectés. Entre droit de la consommation, droit de la responsabilité (v. fiche pratique n°2), droit pénal et droit à la vie privée par le biais de la Loi Informatique et Libertés et du RGPD, la France n'a pas encore adopté de mesures spécifiques à l'IoT et paraît privilégier ainsi une régulation européenne.

A noter tout de même, le rapport parlementaire du 10 janvier 2017 sur les objets connectés[2] qui suggère d'adapter le code de la consommation pour obliger les fabricants et éditeurs de services à informer clairement les consommateurs sur l'utilisation de leurs données. Nous reviendrons sur le cadre français dans la fiche n°2.

Un intérêt marqué de l'U.E.

Parmi les différents textes européens régulant l'IoT, il faut bien évidemment mentionner le règlement général sur la protection des données mais aussi les textes suivants, adoptés ou en cours d'adoption :

- Regulation on the free flow of non-personal data : applicable depuis le 28 mai 2019, le règlement vise à supprimer les obstacles à la libre circulation des données non personnelles entre les États membres et les systèmes informatiques en Europe. Ce nouvel encadrement fait partie de la stratégie de l'U.E. en matière de gouvernance des données et a pour objet de favoriser la vie privée sur internet et surtout la réutilisation de données non-personnelles pour le développement d'I.A. européennes. Les acteurs de l'IoT de santé et de la mobilité sont particulièrement concernés par ce nouveau règlement.

- Network and Information Security Directive: Elle prévoit des mesures juridiques visant à renforcer le niveau général de cybersécurité dans l'UE via des mesures de coopération et de supervision. La directive devait être transposée au plus tard le 9 mai 2018.

- Intelligent Transport Systems Directive : Ladite directive prévoit l'application du régime des produits défectueux à tout objet connecté relatif au transport (v. fiche n°2). Elle est applicable depuis le 27 février 2012.

- eCall regulation : eCall est un système utilisé dans les véhicules de l'UE qui permet d'appeler automatiquement et gratuitement le 112 en cas d'accident de la route grave. Ce système est obligatoire pour tout achat de véhicule neuf dont la fabrication a été approuvée après le 31 mars 2018.

- Directive on Energy Performance of Buildings : concernant globalement la perfor-

mance énergétique de l'immobilier européen, l'IoT est mis en avant pour atteindre un parc immobilier à haute efficacité énergétique et décarbonisé d'ici 2050, créer un environnement stable pour les décisions d'investissement et permettre aux consommateurs et aux entreprises de faire des choix plus éclairés. La directive devait être transposée au plus tard au 10 mars 2020.

- Cybersecurity Act : Entré en application le 27 juin 2019, ce dispositif vise à définir un cadre européen de certification de cybersécurité, essentiel pour renforcer la sécurité des services en ligne et des appareils de consommation sur le marché unique numérique européen. Il précise la portée de la certification avec plusieurs niveaux d'assurance :
    - Le niveau élémentaire qui cible typiquement des objets grand public, non critiques (exemple : IoT)
    - Le niveau substantiel qui cible le risque médian (exemple : Cloud)
    - Le niveau élevé qui cible les solutions pour lesquelles il existe un risque d'attaques menées par des acteurs avec des compétences et ressources significatives (exemple : véhicules ou dispositifs médicaux connectés).
- Le code des communications électroniques européens : Ce code obligera là encore les acteurs Over the top (OTT) à se conformer à des obligations de sécurité des réseaux ou encore d'interopérabilité. Le code interdit l'écoute, l'enregistrement, le stockage ou tout autre type d'interception ou de surveillance des communications et des données de trafic associées par des personnes autres que les utilisateurs, sans le consentement préalable des utilisateurs concernés. Une obligation qui aura un impact en termes de messageries proposées sur les objets connectés, tant les utilisateurs peuvent redouter de voir leurs conversations analysées pour se voir ensuite diffuser des annonces personnalisées. Nouvelle exigence de recueil du consentement qui vient de nouveau interroger sur la validité du consentement donné par le biais de conditions générales et *a fortiori* sur internet. Par ailleurs, les OTT devront limiter l'utilisation de données de trafic et de localisation, notamment concernant la durée d'un échange téléphonique, message ou courrier mais aussi la localisation de l'expéditeur ou du destinataire. L'avantage d'une telle régulation est de s'assurer que tous les OTT, quel que soit l'objet connecté concerné, devront respecter des règles plus respectueuses de la vie privée des consommateurs. La directive, adoptée le 11 décembre 2018, doit être transposée au plus tard le 21 décembre 2020.
- Directive on Contracts for the supply of digital content and digital services : les consommateurs seront protégés lorsque des contenus ou services numériques sont défectueux, et auront le droit d'obtenir réparation en demandant au professionnel de régler le problème ou si le problème persiste en obtenant une réduction de prix ou en résiliant le contrat. Cela n'existait que pour les biens matériels au niveau européen. La directive inclut désormais par exemple une musique téléchargée non diffusée sur l'appareil ou un logiciel qui cesse de fonctionner. A ce titre, dans de nombreux cas, le consommateur ne paie pas pour accéder au contenu ou aux services numériques, mais

fournit des données personnelles au commerçant. La nouvelle directive sur le contenu et les services numériques donne aux consommateurs le droit à un recours en cas de contenu numérique ou de service numérique défectueux, qu'ils aient payé ou seulement fourni des données personnelles. Tel est le cas en matière d'IoT. Adoptée le 20 mai 2019, cette directive devra être transposée au plus tard le 1er juillet 2021 et sera applicable au 1er janvier 2022.

- EU Basic Regulation for Drones : Le cadre européen créé trois catégories d'opération pour les drones – « *ouverte* » pour les engins à faible risque allant jusqu'à 25 kg, « *spécifique* » pour les drones devront être autorisés à voler ou « *certifiée* » pour la catégorie de drone la plus élevée, telle que l'exploitation de drones de livraison ou de passagers, ou le survol de grandes masses de personnes. Cette règlementation est applicable à compter du 1er juillet 2020.

- Medical Device Regulation : les conseils d'orientation[3] publiés en décembre 2019 et relatifs à ce règlement prévoient que le mode d'emploi doit comporter les informations nécessaires pour que les patients et les consommateurs puissent être informés des dernières version du logiciel, protéger l'appareil pendant toute sa durée de vie, utiliser des mots de passe suffisamment complexes, désactiver les fonctionnalités qui ne sont pas utilisées, sécuriser l'ordinateur ou les tablettes, utiliser des sauvegardes et protéger leurs données de santé. Il faut notamment s'assurer que les appareils connectés, tels que les ordinateurs et les appareils mobiles, sont conformes aux instructions d'utilisation fournies avec le dispositif médical. Ces dispositions assureront une coexistence sûre des dispositifs médicaux dans un environnement IoT. Ce règlement 2017/745 sera applicable le 26 mai 2020.

- Parmi les futurs textes à venir, il faut bien évidemment évoquer le projet de règlement ePrivacy. Avec ce projet les cookies seraient désormais paramétrés dans le logiciel et le navigateur de l'utilisateur, sans qu'il soit nécessaire de recueillir le consentement de l'utilisateur pour chaque page web. Cette mesure permettrait aux utilisateurs d'IoT de mieux s'approprier leur appareil et de susciter leur confiance. Autre objectif du règlement ePrivacy, obliger les fournisseurs de communications électroniques aux mêmes diligences que les fournisseurs de télécommunications traditionnels. Seraient concernés Messenger, Gmail, Skype, WhatsApp, etc. Ce projet est toujours en discussion.

- Il faut citer par ailleurs le rapport Delvaux contenant des recommandations à la Commission et concernant des règles de droit civil sur la robotique : ce rapport préconise d'adopter des normes communes en matière de robotique et notamment en termes de responsabilité. La principale innovation de ce rapport tient au fait qu'il suggère d'attribuer une « *personnalité juridique spécifique* » aux robots avec l'attribution d'une « *personnalité électronique* ». Certains robots se verraient attribuer des devoirs, comme celui de « *réparer tout dommage causé à un tiers* ». Le rapport suggère également la création d'un système d'assurance obligatoire et d'un fonds pour garantir le dédommagement total des victimes en cas d'accidents causés par les voitures autonomes. Le rapport fut adopté le 16 février 2017 par le Parlement européen.

- Enfin la question du lien entre les objets connectés et l'intelligence artificielle est régulièrement évoquée. A ce sujet la commission européenne a publié un livre blanc[4] en février 2020 dans lequel est évoqué une possible certification européenne en matière d'IA. Un rapport sur la faisabilité d'une telle certification est attendu à la fin d'année 2020.

Initiatives américaines

Aux États-Unis le cadre juridique applicable aux objets connectés est déjà structuré par de nombreux textes et recommandations[5].

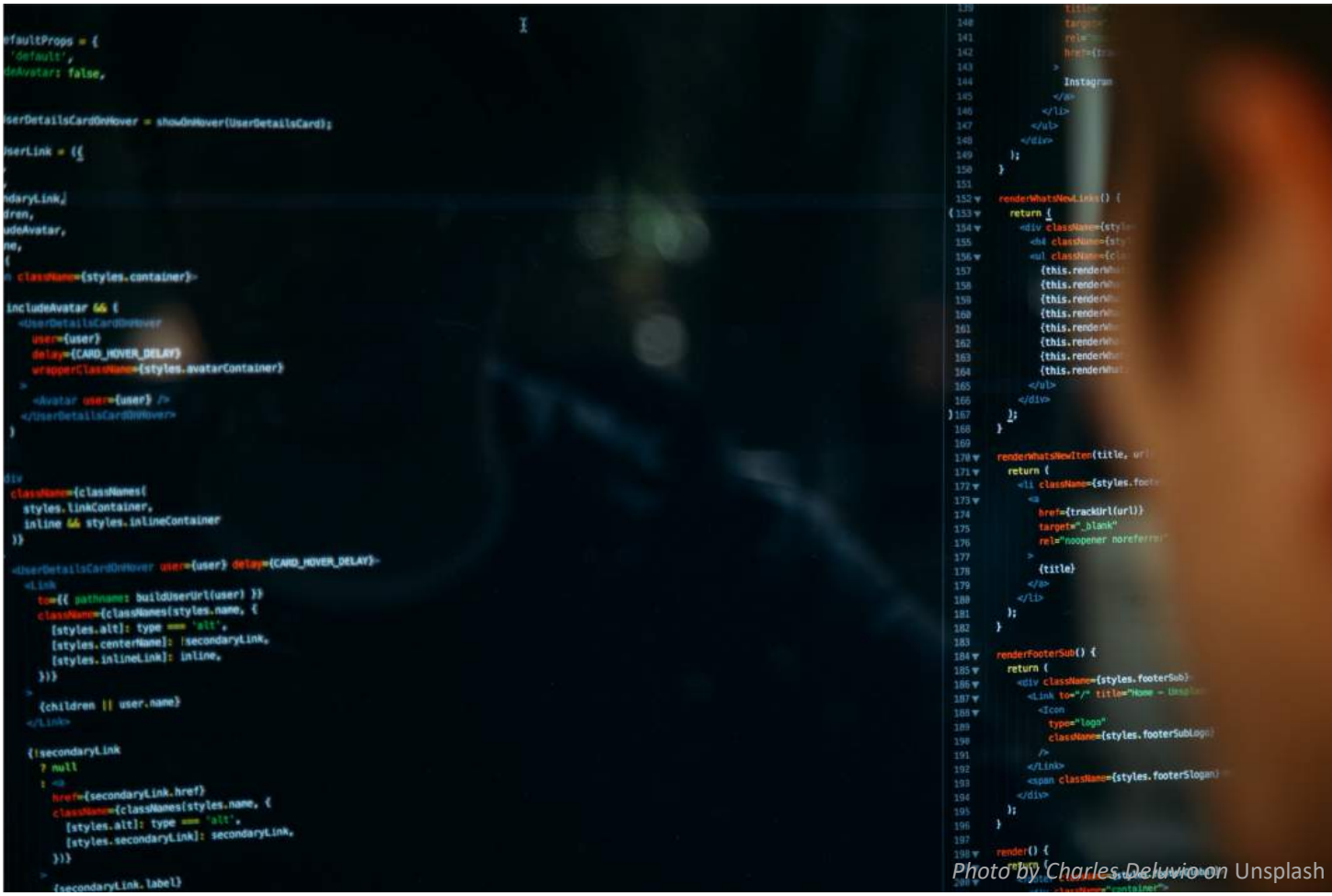
Ainsi, le DIGIT (Developing and Growing the Internet of Things) Act a été adopté par le Sénat américain le 8 janvier 2020 qui établit un groupe de travail chargé de fournir des recommandations au Congrès sur la manière de faciliter la croissance de l'IoT. Ceci notamment en *« identifiant les lois et réglementations fédérales, les pratiques en matière de subventions, les difficultés budgétaires ou juridictionnelles et autres politiques sectorielles qui entravent le développement de l'IoT ».* Parallèlement, le DIGIT Act charge également la Commission fédérale des communications (FCC) d'établir un rapport pour évaluer les besoins nécessaires pour soutenir l'IoT.

Bien qu'il n'existe pas de législation fédérale, la Californie et l'Oregon ont été les premiers États à légiférer sur l'IoT. Depuis le 1er janvier 2020 le SB 327 (loi californienne) est applicable à tout fabricant d'appareil qui se connecte « *directement ou indirectement* » à internet doit l'équiper de dispositifs de sécurité « *raisonnables* », conçus pour empêcher tout accès, modification ou divulgation d'informations non autorisés. S'il est possible d'y accéder en dehors d'un réseau local avec un mot

de passe, il doit soit être fourni avec un mot de passe unique pour chaque dispositif, soit forcer les utilisateurs à définir leur propre mot de passe lors de leur première connexion. Cela signifie qu'il n'y a plus d'informations d'identification génériques par défaut qu'un hacker pourrait utiliser.

Par ailleurs, tel qu'il est rédigé, le SB 327 peut exclure les fabricants de technologie immatérielle - comme les logiciels. A ce titre, des questions se posent à la lumière du droit de la responsabilité américain. Lorsqu'il s'agit de principes stricts de responsabilité du fait des produits, un fabricant de produits peut être tenu pour strictement responsable du défaut d'un produit, comme en France. Mais lorsqu'il s'agit de dispositifs IoT, la ligne de démarcation est floue. Presque toujours, la partie logicielle du dispositif IoT est « *fabriquée* » par une entité distincte de l'entité qui fabrique l'objet physique. Si le dispositif IoT s'avère défectueux, la question se pose de savoir quelle entité peut être tenue pour strictement responsable.

Si le défaut se situe dans l'objet physique du dispositif, l'entité qui a fabriqué le dispositif risque d'être tenue pour strictement responsable. Mais si le défaut se trouve dans le logiciel, la réponse est moins évidente car les tribunaux n'ont pas clairement indiqué si le logiciel est un produit aux sens de la responsabilité du fait des produits[6].



La plupart des observateurs s'attendent à ce que les tribunaux traitent les logiciels dans les dispositifs IoT comme un service plutôt que comme un produit. Le SB 327 abonde en ce sens. Le législateur californien a imposé au fabricant physique d'un dispositif IoT la charge de garantir la sécurité des données stockées dans le dispositif, mais les fabricants de dispositifs physiques peuvent encore soutenir que le logiciel était un simple composant, lorsqu'il s'agit de questions de responsabilité stricte. Il appartiendra à la jurisprudence de trancher cet aspect.

Également applicable au 1er janvier 2020, l'Oregon a adopté une législation similaire, qui tout comme la Californie concerne la sécurité de l'IoT et ne se limite aux objets recueillants des données personnelles. Les mesures de l'Oregon sont toutefois légèrement plus restreintes car ne sont concernés que les objets utilisés principalement à des fins personnelles, familiales ou domestiques lorsque les mesures californiennes s'appliquent également aux objets connectés industriels ou d'une utilisation B2B. Ces deux lois excluent les fournisseurs de magasins d'électronique, *marketplaces* et autres moyens d'achat ou de téléchargement de logiciels.

Au-delà de l'objectif d'une législation propre à l'IoT, les États-Unis semblent s'inspirer progressivement de la règlementation européenne et notamment en matière de données personnelles.

Les États-Unis disposent déjà du Privacy Act de 1974 qui protège déjà les données à caractère personnel, mais uniquement lorsque ces données sont détenues par le secteur public. Cinq principes sont prévus : le principe de transparence, le principe d'accès, le principe de correction, le principe de sécurité des données et le principe de limitation des finalités. Mais ce n'est qu'après le Privacy Act que le secteur privé fut réglementé sur la gestion des données privées. Par exemple, le Health Insurance Portability and Accountability Act qui protège les données de santé, le Gramm-Leach-Bliley Act pour les données financières, ou le Children's Online Privacy Protection Act concernant les données des enfants. Ainsi, tous les États ont voté des lois spécifiques pour la défense de certains aspects de la vie privée.

Le caractère commercial ou non des données personnelles est le critère de différenciation par rapport à la règlementation européenne et limite ainsi la régulation des données outre Atlantique.

Le CCPA (California Consumer Privacy Act), entré en vigueur le 1er janvier 2020, a instauré de nouvelles obligations à la charge de toute entreprise opérant en Californie et générant un chiffre d'affaires de 25 millions de dollars ou qui récolte les données d'au moins 50 000 personnes ou enfin dont le chiffre provient pour moitié de l'exploitation de données utilisateurs.

Plus restreint dans son champ d'application que le RGPD, le CCPA instaure des droits particuliers. Le CCPA permet ainsi aux particuliers de savoir quelles données personnelles sont en possession d'une entreprise, de pouvoir demander la suppression desdites données et d'exiger que ces données ne soient plus vendues à des tiers (mécanisme d'*opt-out*). Il va sans dire que cette législation s'appliquera désormais aux objets connectés. Reste à savoir si les entreprises de la Silicon Valley en profite-

ront pour appliquer d'elles-mêmes les nouvelles mesures à l'ensemble de leurs objets connectés ou uniquement à ceux destinés à la Californie.

Les propositions de législation en matière de protection des données à l'échelle fédérale n'ont toujours pas abouti à l'instar du *« Washington Privacy Act ».* D'autres initiatives avaient également été proposées (*« Democrats' Consumer Online Privacy Rights Act »* et le *« Republicans' United States Consumer Data Privacy Act of 2019 »*) mais sans succès. D'autres propositions de législations sont en cours de discussion, sur des aspects sectoriels. Ces propositions montrent à quel point les Etats-Unis privilégient en pratique une législation point par point, qui n'aurait pas la vocation universelle du RGPD. Voici une liste de plusieurs projets à l'échelon fédéral, datant de moins d'un an et susceptibles de s'appliquer à l'environnement des objets connectés[7] :

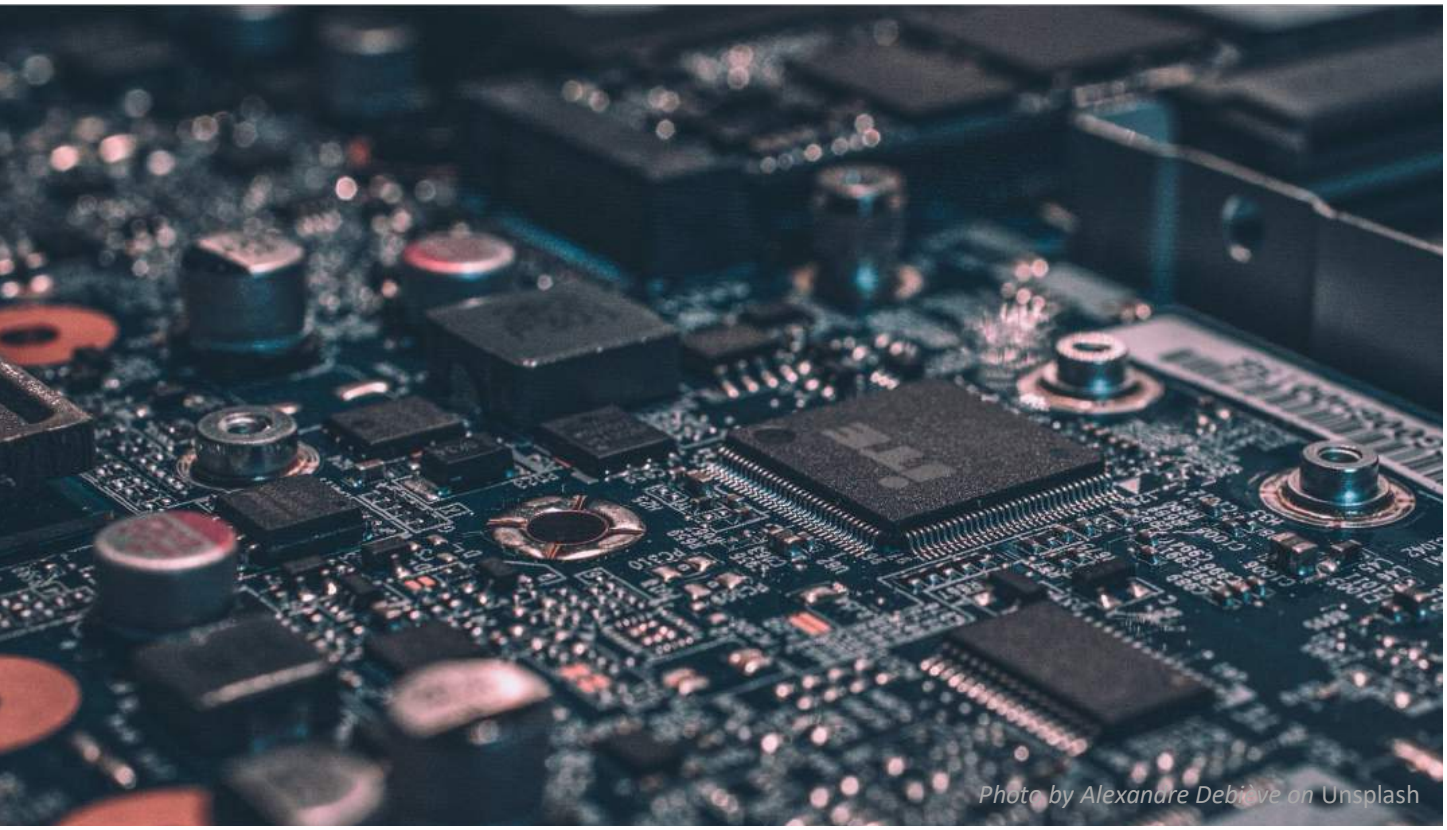
- Filter Bubble Transparency Act : Ce projet de loi oblige les sites web qui utilisent des données personnelles pour filtrer les résultats de recherche ou personnaliser des fils d'information à en informer les utilisateurs. Il exige également qu'ils offrent aux utilisateurs une version non altérée de leurs résultats de recherche ou de leurs fils d'information qui ne sont pas basés sur des données personnelles.

- Social Media Privacy Protection and Consumer Rights Act : Ce projet de loi oblige les responsables de plateformes en ligne à informer les utilisateurs que leurs données sont collectées et traitées par le responsable, ainsi que par des tiers. Il donnerait également aux utilisateurs un droit d'accès à une copie de leurs données et obligerait les opérateurs à informer les utilisateurs en cas de violation des données.

- Do Not Track (DNT) Act : En vertu du projet de loi, les entités visées ne pourraient pas collecter de données auprès des utilisateurs qui envoient des signaux DNT c'est-à-dire qui refusent que leurs données personnelles autres que celles données nécessaires au fonctionnement de leur site web, service ou application soient traitées. Le projet interdirait également d'utiliser ces données à des fins secondaires, telles que la publicité ciblée, ou de partager les données avec des tiers, sauf si l'utilisateur y consent expressément. Il serait également interdit aux entités couvertes de refuser l'accès aux services ou de fournir différents niveaux d'accès ou de service aux utilisateurs qui utilisent le signal DNT.

- DASHBOARD Act : Ce projet de loi impose aux services de médias sociaux comptant plus de 100 millions d'utilisateurs actifs par mois de divulguer non seulement les types de données qu'ils collectent, mais aussi la valeur de ces données. En outre, le projet de loi donnerait aux utilisateurs le droit de demander la suppression de tous les champs ou de certains champs de données que les opérateurs commerciaux ont collectés à leur sujet.

- ACCESS Act : Ce projet de loi oblige les grands fournisseurs de plateformes de communication à « *initier le transfert sécurisé des données de l'utilisateur* », à la demande de ce dernier, accordant essentiellement aux utilisateurs le droit à la portabilité des données.



- BROWSER Act : Ce projet de loi exige que les fournisseurs de services d'accès internet à haut débit et de services de périphérie informent les utilisateurs de leur politique en matière de protection de la vie privée. Il exige également que les entités visées obtiennent l'accord d'un utilisateur pour utiliser ou divulguer des informations sensibles et qu'elles obtiennent l'accord d'un utilisateur pour utiliser ou divulguer des informations non sensibles.

- Protecting Personal Health Data Act : Le but de ce projet de loi est de combler les lacunes de la réglementation de la loi sur la portabilité et la responsabilité en matière d'assurance maladie en réglementant des entités telles que les appareils de suivi de la condition physique portables et les sites de médias sociaux qui recueillent des informations sur la santé.

- Commercial Facial Recognition Privacy Act : ce projet interdit l'utilisation des technologies de reconnaissance faciale en l'absence d'un consentement positif des individus.

- Facial Recognition Technology Warrant Act : le projet de loi obligerait notamment le « *Federal Bureau of Investigation and Immigration and Customs Enforcement* », à obtenir un mandat pour utiliser la technologie de reconnaissance faciale afin de surveiller les personnes.

Une telle inflation législative outre Atlantique présente cependant le risque de procéder à un encadrement désordonné, par Etat ou par champ d'application. Procéder de la sorte pourrait aussi engendrer des frais importants de mise en conformité par Etat ou par secteur d'activité, une insécurité juridique pour les entreprises face à des régulations diverses et non unifiées mais également un manque de lisibilité pour les particuliers.

Par ailleurs il faut aussi noter que la FCC (Federal Communications Commission) a récemment adopté un plan favorisant la 5G (5G FAST Plan[8]) pour réduire la réglementation fédérale faisant obstacle au déploiement des infrastructures nécessaires à la 5G et l'IoT :

- Restoring Internet Freedom Order : définit une politique nationale cohérente pour les fournisseurs d'accès à l'Internet.
- One-Touch Make-Ready : La FCC a mis à jour ses règles régissant le raccordement de nouveaux équipements de réseaux aux poteaux électriques afin de réduire les coûts et d'accélérer le processus de déploiement de la 5G.
- Speeding the IP Transition : La FCC a révisé ses règles afin de permettre aux entreprises d'investir plus facilement dans les réseaux et services de nouvelle génération plutôt que dans les réseaux obsolètes.
- Business Data Services : Afin d'encourager les investissements dans les réseaux modernes en fibre optique, la FCC a mis à jour les règles relatives aux services dédiés au haut débit en supprimant la réglementation des tarifs le cas échéant.

Cette règlementation témoigne de la volonté américaine de favoriser le déploiement de la 5G et de faciliter l'utilisation d'objets connectés. Cette liste provisoire signale les risques de création d'un environnement juridique hétérogène et éclaté pour les objets connectés, au risque de renforcer les difficultés en termes d'encadrement et de régulation.


Photo by NASA on Unsplash

Ressources

[1] *Mireille Delmas-Marty, Les forces imaginantes du droit, op. cit., p. 18 et s.*

[2] *http://www.assemblee-nationale.fr/14/rap-info/i4362.asp*

[3] *https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwipgpTUq6roAhXizIUKHVoUCeoQFjACegQIBBAB&url=https%3A%2F%2Fec.europa.eu%2Fdocsroom%2Fdocuments%2F38941%2Fattachments%2F1%2Ftranslations%2Fen%2Frenditions%2Fnative&usg=AOvVaw1ErLyb5W5fS8tZ9ts1aBIs*

[4] *https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf*

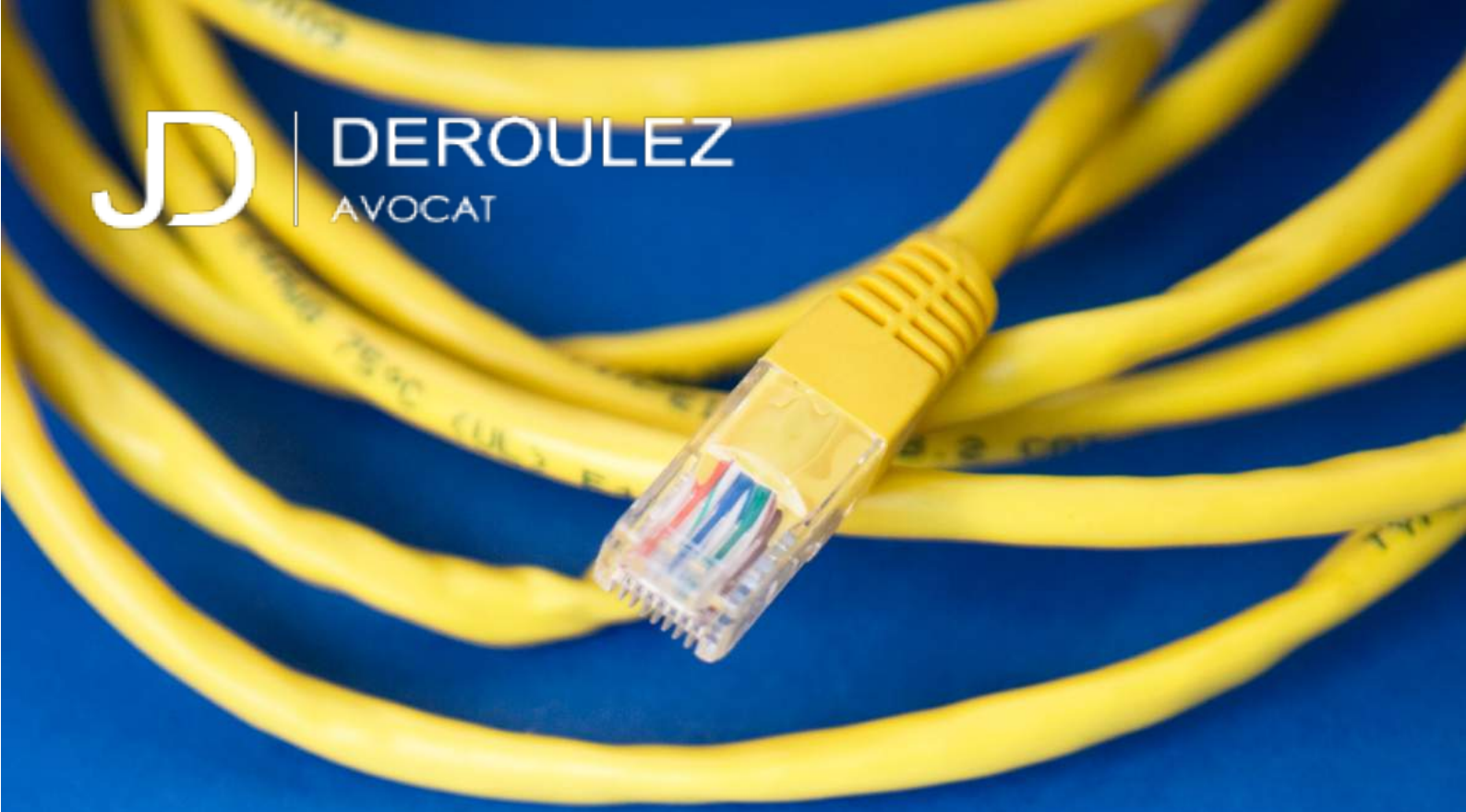
[5] *https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259-draft2.pdf*

[6] *https://www.natlawreview.com/article/product-liability-internet-things*

[7] *https://iapp.org/news/a/tracking-the-politics-of-federal-us-privacy-legislation/*

[8] *https://www.fcc.gov/5G*

DEROULEZ
AVOCAT



FICHE PRATIQUE N°2 – Responsabilité et objets connectés

Photo by Markus Spiske on Unsplash

« Le moment est venu de légiférer, afin de garantir que l'UE offre un cadre de protection aux consommateurs et une sécurité juridique pour les entreprises » [1]

Le cadre juridique des objets connectés est particulièrement large et couvre l'ensemble des champs du droit, de la protection des données personnelles à la cybersécurité en passant par la responsabilité du fait des produits ou le droit de la consommation. Ce cadre doit aussi s'apprécier selon les secteurs d'activité concernés et au vu de leurs spécificités (santé connectée, assistants vocaux à usage professionnel, jouets…).

La question de la responsabilité des objets connectés est un des sujets récurrents, du fait de leur « autonomisation » grandissante et de l'explosion des usages liée aux mutations technologiques.

Se pose ainsi la question de savoir si le cadre législatif et réglementaire actuel est adapté ou non à cette question ou si des modifications sont nécessaires ou envisageables à terme.

Un cadre spécifique pour la responsabilité du fait d'un objet connecté ?

L'émergence d'objets connectés « intelligents » pouvant prendre des décisions de manière autonome et sans recourir à une intervention humaine est susceptible de remettre en cause les canons du droit des contrats et de poser une série de questions :

- Au sujet de la licéité du contrat et du consentement des parties tout d'abord, alors qu'un objet connecté ou un robot connecté ne disposent pas de la personnalité juridique

- Au regard de l'appréciation des responsabilités en cas de dommage et pour déterminer ou répartir l'étendue de la responsabilité encourue

- Sur les conditions de la réparation du ou des dommages causés par un objet connecté.

En l'état du droit français, il n'existe pas de cadre juridique spécifique applicable à la responsabilité du fait des objets connectés ou de robots connectés, ce qui nécessite de renvoyer aux mécanismes de la responsabilité contractuelle et extracontractuelle applicables, par le biais notamment des dispositions sur les produits défectueux ou sur la garde de la chose.

De plus, il faut noter qu'aucun texte particulier sur la responsabilité du fait des objets connectés n'est envisagé à ce stade : à ce titre, le rapport parlementaire de Corinne Erhel et de Laure de la Raudière du 15 janvier 2017 ne propose pas d'intervention législative (la question du contrôle des objets connectés étant envisagée sous le seul angle de la protection des données[2]). Ce qui pourrait être interprété comme la preuve que le cadre juridique français ne constitue pas un frein au déploiement du marché des objets connectés aujourd'hui.

De la même façon, la résolution du Sénat sur la régulation des objets connectés et du développement de l'internet des objets en Europe en date du 22 mai 2018 soulignait d'abord la nécessité d'une politique industrielle européenne de soutien au développement de l'ioT, avant d'envisager certains aspects juridiques. A ce titre, seuls étaient évoqués le droit de la consommation et la protection des données comme points nécessitant un éventuel encadrement juridique.

Ainsi, la question de la responsabilité du fait d'un objet connecté pourrait échapper au seul prisme de la responsabilité civile et englober aussi les questions liées à la protection des données (et notamment aux responsabilités des responsables de traitement et sous-traitants) et au droit de la consommation.

La question des véhicules connectés et de leur responsabilité constitue ici un sujet autonome, du fait des perturbations probables du cadre applicable en France et de l'indemnisation des victimes : ces questions seront traitées dans le cadre de la fiche sur la mobilité connectée.

IoT et droit de la consommation

La question de la responsabilité du fait des objets connectés intéresse évidemment le droit de la consommation, comme cela a été signalé par les rapports parlementaires pré-cités.

A ce titre, il faut souligner que de nombreux outils existants permettent déjà de répondre à cet impératif de protection.

L'obligation d'information précontractuelle de droit commun - prévue à l'article 1112-1 du Code civil - impose en effet au professionnel de communiquer au consommateur une série d'informations et notamment sur les « *caractéristiques essentielles du bien* » visées à l'article L. 111-1, 1° du Code de la consommation. Pour l'association UFC Que choisir, tout traitement de données à caractère personnel lors de l'utilisation d'un objet connecté fait partie intégrante de son fonctionnement et constitue donc une caractéristique essentielle de ce type de produit. A ce titre, cette association a assigné la FNAC et AMAZON[3] pour au non-respect manifeste de leurs obligations d'informations précontractuelles en matière d'objets connectés et de conseil sur les fondements de pratiques commerciales trompeuses et en cessation d'agissements illicites.

Outre l'obligation précontractuelle d'information due par le vendeur, le consommateur a également la possibilité de se défendre sur le terrain des clauses abusives via les articles L.212-1 et L.212-2 du code de la consommation qui prévoient que toute clause déséquilibrante entre les droits et obligations des parties, dans un contrat entre un professionnel et un consommateur (ou non-professionnel) est nulle.

A titre d'exemple, des clauses par lesquelles le fabricant d'un objet connecté ne préciserait pas suffisamment les conditions de collecte et de traitement de données ou encore leurs finalités (concernant le dépôt de cookies ou encore la géolocalisation de l'utilisateur à des fins de publicité ciblée) pourraient constituer des clauses abusives au sens du droit de la consommation. Il en va de même de clauses par lesquelles le fabricant ne solliciterait pas le consentement de l'utilisateur de l'objet connecté concernant une analyse automatique de contenus pour proposer des fonctionnalités spécifiques à l'utilisateur. Enfin, l'acceptation de conditions générales d'utilisation qui prévoiraient un transfert de données personnelles à des tiers vers des pays hors U.E. ne saurait être présumée par l'utilisation de l'objet. L'utilisateur doit en effet être dûment informé et son consentement doit être expressément recueilli.

Autant de précautions contractuelles à ne pas négliger et qui doivent être considérées dans le cadre des objets connectés, ces derniers étant souvent commercialisés à l'international.

Par ailleurs, il faut aussi souligner que les dispositions de la directive relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques[4] entreront en application le 1er janvier 2022 (voir fiche pratique n°1) avec pour objectif d'harmoniser les droits de la consommation et de renforcer les obligations des professionnels. Ainsi que de permettre aux consommateurs de pouvoir demander que le service visé soit rétabli et si le fournisseur n'y procède pas, la réduction du prix ou la résiliation du contrat. Dispositions qui s'appliqueront bien évidemment aux objets connectés, même si ces derniers ne sont jamais directement évoqués par la directive.

Plus généralement, et c'est notamment rappelé par les considérants de cette directive 2019/770 et son article 3, les dispositions du droit de la protection des données personnelles trouvent à s'appliquer aussi lorsque des consommateurs veulent exercer leur droit d'accès ou de rectification ou leur droit à la portabilité. Ce qui pourra concerner des utilisateurs d'objets connectés.

Enfin, doit être mentionné le système européen d'alerte rapide (RAPEX) pour les produits présentant un risque grave pour les consommateurs[5] permettant l'information de la Commission européenne via des alertes émanant d'autorités nationales de l'UE/EEE et concernant des produits dangereux découverts sur leur marché qui pourra être utilisé au titre des objets connectés. Ce système concerne tous les produits de consommation (à l'exception des produits alimentaires, pharmaceutiques et appareils médicaux qui bénéficient d'alertes spécifiques) et bien évidemment les objets connectés. Ainsi la DGCCRF a déjà alerté sur les risques à connaître en matière d'objets connectés [6] et la Commission européenne a pu émettre une notice RAPEX en 2019 concernant des montres connectées pour enfants posant de sérieux risques en termes de sécurité des données[7]. Cette notice témoigne de ce que les obligations liées aux objets connectés recoupent à la fois la protection des consommateurs, la responsabilité du fait des produits et la protection des données personnelles (appréhendée le plus souvent sous l'angle de la sécurité des données).

Le système RAPEX constitue ainsi un bon indicateur des difficultés relevées, à l'échelon national comme européen et des problématiques juridiques inhérentes.

Clauses abusives et IoT

Se pose également la question de la prise en compte des dispositions relatives aux clauses abusives au sens du droit français, que ce soit dans le droit commun des contrats, dans le droit commercial ou encore en droit de la consommation. En effet, ces dispositions peuvent devoir être prises en compte de façons très différentes lors de la fabrication et de la commercialisation d'un objet connecté. Et notamment lorsqu'un utilisateur conclut un contrat avec un fabricant d'objet connecté, lorsque cet utilisateur va utiliser des services proposés par l'objet connecté, en cas de survenance d'un dommage ou quand l'objet connecté effectuera des transactions ou des opérations pour le compte d'un utilisateur ou d'un consommateur.

Photo by Markus Winkler on Unsplash

Dans le cadre de l'internet des objets, il apparait que peuvent être réprimées les clauses contractuelles abusives de droit commun au sens de l'article 1171 du Code civil et dans le seul contexte des contrats d'adhésion : à savoir toute clause non négociable d'un contrat d'adhésion qui créé un déséquilibre significatif entre les droits et obligations des parties. Tel serait le cas d'un contrat de vente portant sur un produit connecté et pour lequel le vendeur se réserverait par exemple le droit de modifier unilatéralement les CGU ou de prévoir un consentement implicite au traitement des données personnelles par la simple poursuite de la navigation… Serait encore sanctionné le fait d'insérer une clause qui viderait de sa substance l'obligation essentielle du fabricant d'IoT - article 1170 du code civil - telle qu'une clause élusive de responsabilité en cas de faille concernant la sécurité des données.

Ces dispositions – très débattues – sont inspirées du droit spécial des clauses abusives en droit de la consommation (article L212-1 et s.).

Le droit commercial sanctionne également le fait, par une personne exerçant des activités de production, de distribution ou services, d'obtenir ou de tenter d'obtenir de l'autre partie un avantage sans contrepartie ou manifestement disproportionné au regard de la valeur de la contrepartie consentie ou encore de soumettre ou de tenter de soumettre l'autre partie à des obligations créant un déséquilibre significatif dans les droits et obligations des parties. Tel serait le cas lorsqu'un professionnel soumettrait un second professionnel à des clauses qui lui seraient particulièrement défavorables, par exemple lorsqu'un fournisseur de software empêcherait un fabricant d'objets connectés de demander la réparation technique d'un logiciel atteint d'un dysfonctionnement par ce fournisseur.

L'article L.442-1 du code de commerce a vu ses conditions d'applications élargies depuis l'ordonnance du 26 avril 2019[8], permettant ainsi à tout commerçant de se défendre si des clauses abusives venaient à être stipulées dans un contrat, notamment de fourniture de composantes ou de distribution d'IoT.

Vers un droit européen de la responsabilité du fait des objets connectés ?

Alors que la Commission européenne s'était interrogée dès 2016 sur l'opportunité d'un dispositif européen en matière de responsabilité du fait des objets connectés[9], le Parlement européen a marqué son ambition à ce sujet à travers le rapport Delvaux adopté le 27 janvier 2017. Si les travaux de la Commission évoquaient les enjeux de responsabilité sous l'angle de modifications éventuelles des directives « commerce électronique » et « des produits défectueux », le Parlement a au contraire formulé des recommandations claires en faveur de règles de droit civil sur la robotique[10] (tout en endossant par ailleurs une approche large des objets connectés et des robots).

Dans ce rapport, le Parlement a estimé que la responsabilité civile pour des dommages causés par des robots « autonomes » était une question cruciale qui appelait une réponse à l'échelle de l'Union européenne, via un paquet législatif spécifique combiné à des lignes directrices et des codes de conduite.

A ce titre, le Parlement a d'abord appelé à une évaluation approfondie des régimes de responsabilité à mettre en place, distinguant le « principe de responsabilité stricte » du « principe de responsabilité fondée sur le risque ». Point intéressant, ce rapport a suggéré de prendre en compte le niveau réel d'instructions donné au robot et son niveau d'autonomie, élément qui pourrait être particulièrement délicat à déterminer en pratique.

Ce rapport militait ainsi pour un régime d'assurance obligatoire prenant en compte toutes les responsabilités potentielles.

A signaler également, le Parlement européen a milité en faveur de la création à terme d'une personnalité juridique « spécifique » pour les robots, ces derniers pouvant être dans certains cas considérés comme des personnes électroniques prenant des décisions et interagissant de manière indépendante avec des tiers.

Ce rapport relevait par ailleurs la question particulière des véhicules autonomes et des accidents de la circulation (à travers les conventions internationales à faire évoluer).

Si ce rapport n'a pas encore donné lieu à une intervention législative spécifique et ne figure pas au programme de travail de la Commission[11], ces travaux n'en devraient pas moins se poursuivre dans les prochaines années et au moins dans le domaine des véhicules connectés. A ce titre, toute évolution de la législation dans ce domaine devra en tout état de cause prendre en compte la législation européenne en matière de responsabilité du fait des produits défectueux ou les règles applicables à la protection des consommateurs. Une telle incitation est d'ores et déjà prévue, à l'instar de l'article 11 de la directive 2010/40 sur les systèmes de transports intelligents consolidée[12] qui appelle à veiller à la conformité entre ces derniers systèmes et le droit de la responsabilité du fait des produits défectueux.


Photo by Amanda Dalbjorn on Unsplash

Ces travaux soulignent ainsi que si un futur droit européen de la responsabilité du fait des robots et des objets connectés devait voir le jour, celui-ci resterait largement marqué par la législation existante et probablement par une approche sectorielle (par exemple pour les véhicules connectés), en renvoyant à une date ultérieure le régime de responsabilité civile appelé par le Parlement.

A ce titre, le document de travail de la Commission du 7 mai 2018[13] suite à la 5ème évaluation de la directive 85/374/CEE en matière de responsabilité du fait des produits défectueux est intéressant car il témoigne de son double souhait de prendre en compte les nouveaux développements technologiques dont l'IoT et de répondre à l'absence de législation spécifique pour ces nouveaux produits. Cette évaluation qui s'est inscrite dans le prolongement du rapport Delvaux traduit également le souhait de la Commission de mener une réflexion approfondie avant de réviser les textes en vigueur et cette directive en particulier.

Ces différents éléments traduisent ainsi la difficulté d'une appréhension d'ensemble du champ des objets connectés et de la difficulté de mettre en place des régimes juridiques cohérents. Les récents débats et travaux législatifs soulignent néanmoins la nécessité de confronter les outils juridiques existants aux questions posées par ces nouvelles technologies pour garantir à long terme une sécurité juridique renforcée.

Les objets connectés en pratique

- Réalisez un audit juridique de l'environnement de votre projet, dans toutes ses étapes (conception, partenariats, développement commercial, aire géographique de distribution, profil utilisateur et risques liés, etc.)
- Dressez une cartographie de l'ensemble de vos partenaires et sous-traitants afin d'identifier toutes les problématiques juridiques et les zones de risque (sécurité des données, confidentialité, propriété intellectuelle, etc.)
- Documentez les usages liés à vos objets connectés et leurs conséquences au regard de votre responsabilité
- Veillez aux questions d'assurances en fonction du type d'objet connecté mis en place
- Veillez à mettre en place des mesures de sécurité adaptées et à les renouveler continuellement

  Déterminez contractuellement la responsabilité de chacun des acteurs (fabricant, sous-traitant, client) en cas de problème lié aux données et autres dommages.
- Déterminez la dépendance de l'objet connecté par rapport aux technologies nécessaires à son usage (cloud, IoT hub…)
- Déterminez juridiquement les fonctionnalités de l'objet connecté et informez conformément les utilisateurs
- Déterminez les cas de cyberattaques dans le cadre de l'utilisation de l'objet connecté

Ressources :

[1] *Mady Delvaux, auteure du rapport Delvaux concernant les règles de droit civil sur la robotique*

[2] *http://www.assemblee-nationale.fr/14/rap-info/i4362.asp#P586_152431*

[3] *https://www.quechoisir.org/action-ufc-que-choisir-objets-connectes-l-ufc-que-choisir-assigne-la-fnac-et-amazon-n50080/*

[4] *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32019L0770*

[5] *http://solidarites-sante.gouv.fr/prevention-en-sante/risques-de-la-vie-courante/article/rappel-de-produits-systeme-europeen-rapex*

[6] *https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/objets-connectes*

[7] *https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/0157/19&lng=en*

[8] *https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=CF1C5F85FB8B3CC2B19862E3345DE8D8.tplgfr26s_1?cidTexte=JORFTEXT000038410002&idArticle=LEGIARTI000038410748&dateTexte=20200417&categorieLien=id#LEGIARTI000038410748*

[9] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110*

[10] *https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_FR.html*

[11] *https://eur-lex.europa.eu/resource.html?uri=cellar%3A7ae642ea-4340-11ea-b81b-01aa75ed71a1.0002.02/DOC_2&format=PDF*

[12] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02010L0040-20180109*

[13] *https://op.europa.eu/en/publication-detail/-/publication/a1fe6e2d-51d5-11e8-be1d-01aa75ed71a1/language-en/format-PDF/source-search*

DEROULEZ
AVOCAT

FICHE PRATIQUE N°3 - Objets connectés de santé

Photo by Kvistholt on Unsplash

« If you are against AI then you are arguing against super cars that aren't going to have accidents and against being able to better diagnose people when they are sick » Mark Zuckerberg.

L'irruption du numérique modifie profondément les pratiques en matière de santé comme l'exercice de la médecine, devenue un nouveau terrain de jeu pour les GAFAM. En effet, « l*es géants du numérique construisent des solutions technologiques pour résoudre les inefficacités du système de santé américain. Reste à convaincre les internautes de leur faire confiance alors que les scandales sur la protection des données se sont multipliés ces derniers mois […]. Selon un récent sondage auprès de 4.000 Américains, seuls 11 % d'entre eux sont prêts à partager leurs informations avec des compagnies technologiques, contre 72 % avec leur médecin*[1] ».

Aujourd'hui, le domaine de la santé est le secteur clé dans lequel les GAFAM et les industries pharmaceutiques investissent fortement et se concurrencent, dans la perspective d'une médecine préventive, prédictive et personnalisée. A ce titre, les industries pharmaceutiques ont déjà lancé leur transformation numérique pour intégrer les données de santé dans leur modèle économique. Tel est par exemple le cas de la plateforme collaborative Darwin construite par Sanofi qui regroupe une large variété de données de santé couvrant plus de 345 millions de patients, 218 maladies et 48 études cliniques. Cette plateforme ambitionne à ce titre de réduire de 70 % les coûts de développement d'un médicament[2]. Par ailleurs, le gouvernement britannique a annoncé le lancement d'une collaboration entre le NHS *(National Health Service)* et Amazon concernant les données des patients britanniques[3]. La firme américaine pourra ainsi accéder aux données de santé du NHS. Le dessein de ce projet est notamment de faire d'Alexa, l'assistant vocal d'Amazon, une aide médicale à domicile capable de prévenir les risques médicaux ainsi que de donner des conseils aux patients-consommateurs.

Se développe ainsi la notion de « *santé intelligente* » qui comprend toutes les technologies permettant d'obtenir de meilleurs outils de diagnostic, de meilleurs traitements pour les patients et les appareils qui améliorent la qualité de vie. Ce concept particulièrement large inclut aussi les services de santé en ligne et de santé mobile, la gestion des dossiers électroniques, les services à domicile intelligents et les dispositifs médicaux intelligents et connectés[4].

Autre notion en pleine configuration, celle du « *patient-consommateur* » ainsi qualifié par le fait qu'il considère la santé comme un droit et qu'il entend disposer de son pouvoir pour choisir les soins et les produits sur un marché de santé en pleine évolution numérique[5]. Si ce patient peut ainsi être amené à transmettre ses données personnelles, cette situation pose de nombreuses questions en raison de la nature des données transmises. Ce qui interroge sur la définition même des données de santé ou encore le périmètre très large couvert par les données de bien être (cycle de sommeil etc.). Avec de très nombreuses questions en lien : quelle sécurité pour les données de millions d'utilisateurs ? quel processus d'alerte en cas de faille cyber ou d'attaque ?

On le voit donc, s'agissant des objets connectés en lien avec la santé, deux grands axes se dégagent principalement, à savoir celui de la protection des données de santé et celui de la sécurité des objets connectés de santé.

Données de santé et objets connectés

Les données de santé recouvrent plusieurs notions, selon que les données sont strictement liées à l'état de santé de l'utilisateur ou qu'elles recouvrent des aspects plus larges.

Le RGPD donne une définition des « données concernant la santé » en son article 4, à savoir toute *« donnée à caractère personnel relative à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèle des informations sur l'état de santé de cette personne. »* Le considérant 35 du même règlement apporte des précisions et enjoint à apprécier comme donnée de santé *« 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. »* Ainsi, le RGPD apprécie de façon extensive les données de santé et ne différencie pas la source à l'origine de la donnée de santé, faisant potentiellement entrer les données collectées par des objets connectés dans son champ d'application.

Au sens du droit français, les données purement médicales sont celles couvertes par le secret professionnel et détenues de façon formalisée ou ayant fait l'objet d'échanges écrits, par les professionnels ou établissements de santé. Il s'agit notamment *« des résultats d'examen, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mis en œuvre, feuilles de surveillance, correspondances entre professionnels de santé »*, à l'exception des informations recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant un tel tiers (CSP art 1111-7).

A côté des données de santé, l'article 4 du RGPD prévoit une définition pour les données génétiques, i.e. « *les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.* »

En outre, un certain nombre de données qui n'entrent pas dans la définition des données de santé, constituent des données connexes aux données de santé. C'est le cas des données de bien-être ou de mesure de soi et qui concernent le mode de vie des utilisateurs. Ces données ont « *émergé avec le développement des objets connectés, notamment ceux disposant de capteurs permettant de collecter automatiquement des données liées aux habitudes de vie*

des porteurs (activité physique via la fréquence cardiaque ou le nombre de pas, périodes de sommeil, nutrition, etc.) »[6] et pourraient connaître un développement exponentiel à l'avenir.

A ce titre, dans son avis rendu le 29 mai 2019, le Comité Consultatif National d'Ethique a relevé que « *toute donnée primaire issue d'une activité humaine – même sans lien apparent avec la santé – peut contribuer – par son croisement avec d'autres données qui ne lui sont pas liées – à la création d'une information nouvelle relative à la santé d'une personne. Une donnée de santé ne peut plus se limiter aux seules données personnelles recueillies dans le cadre d'une prise en charge médicale (mesures biologiques, caractéristiques génomiques, données cliniques, etc.).* »[7]

Il faut aussi évoquer les « *wearables »* qui intègrent des technologies clés (par exemple la nanoélectronique, les composants organiques, la détection, la localisation, la communication, la collecte d'énergie, l'informatique à faible consommation, la visualisation et les logiciels intégrés) dans des systèmes intelligents afin d'apporter de nouvelles fonctionnalités aux vêtements, dispositifs d'aide, montres et autres dispositifs portés par les personnes physiques.[8]

Les *wearables* constituent ainsi un nouveau levier utilisé par les industries pharmaceutiques dans le cadre d'essais cliniques, afin de collecter des données in vivo en temps réel et de les partager pour la recherche clinique[9]. Exploiter tout le potentiel des objets connectés permet d'obtenir des résultats d'une meilleure qualité puisque les données sont recueillies tout au long de la vie du patient, en conditions réelles grâce notamment à des objets d'auto-mesure (rythme cardiaque, pourcentage d'oxygène dans le sang, etc.)[10]. Une telle technique permet alors de recueillir un plus grand nombre de données, tout en supprimant la contrainte des rendez-vous médicaux de recueil de données.

Photo by Kiran CK on Unsplash

Les objets connectés dans le domaine de la santé posent dès lors des questions très larges quant à l'encadrement qui s'impose en considération de la sensibilité des données de santé mais aussi du nombre de données traitées. Quelles diligences mettre en œuvre pour recueillir des données de santé ou affiliées ? Comment s'assurer de la qualité des données collectées ? Quelle relation contractuelle entre les acteurs de l'IoT ? Comment transférer légalement des données de santé ? Comment réutiliser des données de santé ? L'obligation d'information est-elle mise en œuvre également en cas de modification des conditions générales d'utilisation ? Ces questions font cependant l'objet d'un premier encadrement, comme évoqué ci-dessous.

L'interdiction et l'encadrement des traitements de données de santé par le droit de la protection des données

En matière de données de santé, l'article 9.1 du RGPD prévoit une interdiction de principe du traitement de telles données. Il en va de même des données génétiques. L'article 9.2 du même règlement prévoit cependant une liste d'exceptions limitatives, autorisant le traitement de données de santé et notamment :

- le consentement explicite de l'utilisateur pour une ou plusieurs finalités spécifiques - il est par conséquent primordial de bien définir les finalités du traitement de données de santé, au moyen de conditions d'utilisations suffisamment lisibles et intelligibles, en appliquant *le privacy by design* dès la conception des objets connectés. De plus, s'agissant du consentement la Haute Autorité de Santé (HAS) recommande une information lorsqu'il est possible de synchroniser les données sur plusieurs équipements appartenant à un même utilisateur[11]

- la nécessité du traitement pour l'exécution de certaines obligations - i.e. lorsque le traitement de données de santé est nécessaire à l'exécution d'une obligation contractuelle par exemple

- le traitement est nécessaire aux fins de la médecine préventive ou du travail, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou en vertu d'un contrat conclu avec un professionnel de la santé - tel est le cas de la télémédecine (télé-expertise, téléconsultation, télésurveillance, téléassistance). A cet égard, la CNIL et le Conseil national de l'Ordre des médecins ont publié un guide pratique avec une fiche relative à la télémédecine[12]. Le guide précise notamment les vérifications que le médecin doit réaliser dans sa relation contractuelle avec le sous-traitant qui propose un logiciel de télémédecine (traitement des données personnelles sur les instructions du médecin, engagement de confidentialité du personnel, mesures de sécurité, pas de recours à des sous-traitants ultérieurs sans autorisation, permettre l'exercice des droits des patients etc.)

Outre le respect des exceptions prévues, la Loi Informatique et Libertés comme le RGPD, prévoient que chaque traitement de données personnelles doit être réalisé en intégrant :

- une finalité déterminée, explicite et légitime

- le principe de minimisation de la collecte des données
- une durée de conservation des données limitée
- une obligation de sécurité
- l'information des personnes concernées
- le respect des droits des personnes (droit d'accès, droit à la portabilité, droit à la limitation, à l'effacement, droit d'opposition et de rectification).

Au-delà de ces obligations, tout traitement de données de santé par un objet connecté présente aussi des risques et notamment le traitement de données à l'insu de la personne concernée.

C'est l'exemple des applications de running qui permettent de suivre les performances physiques de l'utilisateur ainsi que bien souvent sa géolocalisation. L'utilisateur peut par la suite partager ses performances sur les réseaux sociaux. Dans une telle situation, il est impératif que les mentions d'informations soient claires et intelligibles, mais également que l'application ne soit pas paramétrée par défaut et surtout que l'utilisateur puisse à tout moment retirer son consentement. Là encore, la question du *privacy by design* joue un rôle majeur et il est impératif de se pencher sur ces questions pour les développeurs de logiciels. En effet, de telles applications mêlant géolocalisation et données de santé ou de bien-être sont au croisement des différents contrôles que la CNIL entend réaliser en 2020[13].

Une autre question primordiale en matière de traitement de données de santé par des objets connectés concerne les destinataires des données qui ne sont pas toujours bien identifiés. Ceux-ci peuvent en outre *« être établis hors de l'Union européenne. Apple avec son HealthKit, Samsung avec SAMI, Google avec Google Fit prévoient de stocker sur une plateforme une série d'informations comme le poids ou le rythme cardiaque, la tension…, transmis par le téléphone en lien avec différents objets connectés* [14] *»* Dans une telle situation il est nécessaire que les tiers éventuellement destinataires des données de santé soient portés à la connaissance des utilisateurs, surtout si des traitements ultérieurs sont susceptibles d'être effectués. Lorsqu'un transfert est réalisé vers un pays hors de l'Union européenne, il est alors nécessaire que le transfert soit réglé par des décisions d'adéquation, par des *binding corporate rules* en cas de transfert intra-entreprise ou par des clauses contractuelles types, sous réserve de la décision de la CJUE à ce sujet[15].

Autre obligation essentielle à la charge du fabricant d'IoT qui recueille et traite des données de santé : la réalisation d'une analyse d'impact. En effet l'article 35 du RGPD prévoit que tous les responsables de traitement sont dans l'obligation de conduire une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel, avant de mettre en place le traitement, si celui-ci est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Selon le RGPD, l'évaluation systématique et approfondie d'aspects personnels, fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire. Il en va de même du traitement à grande échelle de catégories particulières de données.

Le G 29 a également fourni une liste de critères pour déterminer si un risque élevé existe pour les utilisateurs[16] et entre autres :

- L'évaluation ou notation, y compris les activités de profilage et de prédiction, portant notamment sur la santé ou la localisation et les déplacements. L'exemple donné par le G 29 est celui d'une société de biotechnologie proposant des tests génétiques directement aux consommateurs afin d'évaluer et de prédire les risques de maladie/de problèmes de santé.

- Les données sensibles ou données à caractère hautement personnel. A titre d'exemple, le G 29 cite les dossiers médicaux que peut conserver un hôpital général, les données liées à des activités domestiques et privées (notamment les communications électroniques dont la confidentialité doit être protégée), dans la mesure où elles ont un impact sur l'exercice d'un droit fondamental (données de localisation dont la collecte met en cause la liberté de circulation, par exemple). A cet égard, « *il peut être pertinent de déterminer si les données ont déjà été rendues publiques par la personne concernée ou par des tiers. Le fait que les données à caractère personnel soient publiquement disponibles peut être pris en compte en tant que facteur dans l'analyse lorsqu'il est prévu une utilisation ultérieure des données pour certaines finalités. Ce critère peut également inclure les données*

telles que les documents personnels, les courriers électroniques, les agendas, les notes des liseuses équipées, de fonctions de prise de notes ainsi que les informations à caractère très personnel contenues dans les applications de life-logging » selon le G 29.

- Les données traitées à grande échelle, notamment en considération du nombre de personnes concernées, soit en valeur absolue, soit en proportion de la population considérée, le volume de données, la durée de l'activité de traitement de données ou encore l'étendue géographique du traitement…

On le voit, une grande partie des objets connectés sont concernés par la réalisation d'analyses d'impacts. La CNIL a publié un guide concernant l'analyse d'impact relative aux objets connectés[17] ainsi que deux listes des types d'opérations pour lesquelles une analyse d'impact est nécessaire[18] ou non[19].

Une analyse d'impact est ainsi nécessaire, concernant certains traitements de données de santé :

- dossier patients ;
- algorithmes de prise de décision médicale ;
- dispositifs de vigilances sanitaires et de gestion du risque ;
- dispositifs de télémédecine ;
- gestion du laboratoire de biologie médicale et de la pharmacie à usage intérieur, etc.
- mise en œuvre d'une recherche médicale portant sur des patients et incluant le traitement de leurs données génétiques.

A l'inverse, une AIPD n'est pas nécessaire pour les traitements permettant :

- la gestion des rendez-vous ;
- la gestion des dossiers médicaux et l'édition des ordonnances ;
- la gestion et la tenue des dossiers nécessaires au suivi du patient ;
- l'établissement et la télétransmission des feuilles de soins ;
- les communications entre professionnels identifiés participant à la prise en charge de la personne concernée.

Sécurité des objets connectés de santé

La sécurité des objets connectés en matière de santé est primordiale du fait du traitement régulier par ces objets de données sensibles, des coûts nécessaires pour prévenir tout type d'attaque et des risques potentiels de sanction en cas de violation des données. Les frais occasionnés par une cyber-attaque peuvent ainsi être particulièrement importants (150$ en moyenne par donnée personnelle perdue selon IBM [20]), outre les risques de réputation et d'image. Il semble ainsi que le secteur de la santé soit particulièrement exposé et que tout objet connecté commercial traitant de données de santé doit fait l'objet d'une attention très particulière.

De plus, il faut noter aussi que les organismes de santé (OMS[21], hôpitaux[22], etc.) sont des cibles privilégiées pour les hackers, les données de santé pouvant être revendues facilement sur le darknet. Récemment la société Greenbone Network a révélé que des millions

d'images médicales sont en vente, par manque de sécurité des centres hospitaliers et d'imageries médicales.

L'ENISA (Agence de l'Union européenne pour la cybersécurité) a dressé la liste des principaux risques en termes de cybersécurité dans le domaine de la santé[23] :

- Des actions malveillantes - dans cette catégorie se trouvent diverses menaces potentielles - les logiciels malveillants (virus, trojans, rootkits), piratage, attaques DoS, phishing, vol d'appareils, vol de données, effacement…
- Des erreurs humaines - elles sont dues à des actions humaines involontaires, qui ont pour conséquence de nuire aux systèmes de santé
- Des défaillances du système - elles peuvent avoir différentes causes, les plus courantes étant : les défaillances de logiciels ou de microprogrammes, progiciels, les pannes d'appareils, interruption ou défaillance du réseau, maintenance insuffisante.
- Des défaillances de la chaîne d'approvisionnement - cette menace peut être causée par le fournisseur de service de cloud, le fournisseur de réseau, le fournisseur d'électricité ou par le fabricant de dispositifs médicaux, n'ayant pas pris les précautions nécessaires pour garantir l'intégrité de sa chaîne d'approvisionnement.

- Les phénomènes naturels - il s'agit des incendies, inondations, tremblements de terre et d'autres catastrophes naturelles qui peuvent entraîner l'interruption du ou des services.

Par ailleurs en matière d'objet connecté de santé, il faut signaler l'approche de l'Agence nationale de sécurité du médicament et des produits de santé qui distingue dans ses lignes directrices[24], les dispositifs médicaux dont l'utilisation est encadrée (v. fiche pratique sur le droit applicable aux objets connectés) des dispositifs non médicaux.

Constituent notamment des dispositifs médicaux au sens du règlement du 5 mai 2017 sur les dispositifs médicaux entrant en vigueur le 26 mai 2020[25], tout appareil, équipement ou logiciel utilisé seul on en association à des fins de diagnostic, prévention, contrôle ou prédiction d'une maladie. Est ainsi concerné tout logiciel utilisé à des fins médicales, ne serait-ce que pour mieux prévoir certaines affections des utilisateurs d'objets connectés. A ce titre, le nouveau règlement appréhende les logiciels comme des dispositifs médicaux à part entière (pouvant être utilisés seuls) tandis que la directive 93/42/CE abrogée n'envisageait les logiciels que lorsqu'ils étaient nécessaires au fonctionnement d'un appareil (utilisés en combinaison avec un appareil). De plus, un logiciel peut être qualifié de dispositif médical quel que soit son emplacement (par exemple fonctionnement en cloud, sur un ordinateur, un téléphone portable ou une fonctionnalité supplémentaire sur un appareil médical matériel).

Pour être qualifié de logiciel entrant dans la définition de dispositif médical, le logiciel doit avoir une finalité médicale en soi. Il convient de noter que l'objectif décrit par le fabricant du produit est pertinent pour la qualification et la classification de tout appareil.

Selon le « *Medical Device Coordination Group* »[26] chargé de conseiller la Commission européenne, constituent par exemple des dispositifs médicaux, une application de montre intelligente est destinée à envoyer des notifications d'alarme à l'utilisateur et/ou à un praticien de santé lorsqu'elle reconnaît des battements cardiaques irréguliers dans le but de détecter une arythmie cardiaque. Plus généralement, sera considéré comme un dispositif médical, tout logiciel générant des alarmes basées sur la surveillance et l'analyse des paramètres physiologiques spécifiques au patient. C'est également le cas de tout appareil portables intelligent - moniteurs de fréquence cardiaque, de niveau de transpiration, de taux d'alcoolémie. Il en va de même des systèmes d'intervention d'urgence pour réagir aux alertes.

A l'inverse, ne constituent pas des dispositifs médicaux :

- Les systèmes d'information hospitaliers qui soutiennent le processus de gestion. Ils sont généralement destinés à l'admission des patients, à la prise de rendez-vous, à des fins d'assurance et de facturation

- Les applications et logiciels de surveillance de condition physique, de coaching ou tout autre appareil de bien-être qui ne servent pas à prévoir ou traiter une maladie ne constituent pas des dispositifs médicaux selon le règlement et n'y sont donc par principe pas soumis. Sauf si ces applications sont utilisées en association avec une application ou un appareil de santé.

Ainsi, tout logiciel entrant dans la définition des dispositifs médicaux au sens du règlement devra respecter les normes harmonisées (ISO) et un marquage CE qui devra être mis à jour.

L'ENISA[27] a d'ailleurs relevé que plus de 25 normes ISO avaient été élaborées en informatique médicale et notamment :

- *ISO/DTR 22696 Health informatics — Guidance for identification and authentication for connectable personal healthcare devices*
- *ISO/DTR 21332 Health informatics — Cloud computing considerations for health information systems security and privacy*
- *ISO/WD 13131 Health informatics — Telehealth services — Quality planning guidelines*
- *ISO/AWI 22697 Health informatics — Application of privacy management to personal health information*

En outre, le règlement sur les dispositifs médicaux impose aux fabricants d'énoncer *« les exigences minimales concernant le matériel informatique, les caractéristiques des réseaux informatiques et les mesures de sécurité informatique, y compris la protection contre l'accès non autorisé, qui sont nécessaires pour faire fonctionner le logiciel comme prévu »*[28], ceci au regard de l'état de l'art en matière de cybersécurité au moment du développement et de la fabrication. Obligations à prendre en compte lors de la mise en œuvre d'objets connectés dans le domaine de la santé, qu'il s'agisse de dispositifs médicaux ou non. Par ailleurs, des obligations spécifiques en matière de sécurité des données devront être mises en place.

Néanmoins, même si toutes les mesures adéquates sont mises en place pour garantir la sécurité des objets connectés, tout organisme peut faire l'objet d'une violation de données au sens du RGPD, comme cela a déjà été présenté (attaques malveillantes, vol de données ou autre perte). En sus des mesures de sécurité informatique appropriées, il est important de prévoir des actions de formation du fait des risques liés aux erreurs humaines notamment. Enfin, la mise en place d'une procédure d'alerte en interne doit permettre de signaler et de faire remonter les éventuelles violations de données, afin d'en informer l'autorité compétente et les personnes concernées si la situation le justifie.

Dans ce cadre, la mise en place d'une procédure d'alerte constitue un outil pour se conformer aux articles 33 et 34 du RGPD. Une telle procédure permet en effet de guider les salariés qui connaitraient d'une violation de données, gagner du temps dans la transmission d'informations. Plus encore, cette procédure permet au responsable de traitement de s'assurer de la conformité juridique de la réponse apportée, au regard de ses obligations au titre du RGPD. Par conséquent, la mise en place d'une procédure d'alerte doit être prise en compte lors de la conception et de la commercialisation d'objets connectés de santé, procédure prévue par la directive sur les réseaux et systèmes d'information[29]. Ladite directive fait d'ailleurs expressément référence aux lignes directrices de l'ENISA relatives à la cybersécurité dans le domaine de la santé.

Une autre question essentielle pour une utilisation efficace et sûre des services est d'assurer un niveau élevé d'interopérabilité et de garantir que les informations sont transmises en toute sécurité par les objets connectés de

santé. Par exemple, « le vocabulaire utilisé dans les enregistrements de santé électroniques, à savoir les terminologies, les classifications, les métadonnées ou les services de cloud entre différents fournisseurs de services de cloud, locaux ou externes, doit être basé sur des normes universellement appliquées et un cadre convenu ou sur certains protocoles/API ouverts pour l'échange d'informations et l'intégration de services sécurisés.» [30] Le manque d'interopérabilité peut affecter ainsi directement la disponibilité des données.

Enfin les garanties d'accès et d'authentification aux objets connectés de santé sont essentiels concernant la santé en ligne. En effet, le niveau de sécurité lié aux mesures d'authentification constitue une première étape clé pour permettre de valider les utilisateurs d'un objet, déterminer leur identité et l'autoriser à utiliser le système.

Une fois authentifiée, le niveau d'information que la personne est autorisée à consulter ou à partager doit aussi être défini par une politique de contrôle d'accès. A titre d'exemple, les nouvelles législations entrées en vigueur au 1er janvier 2020 en Californie et Oregon imposent ainsi aux fabricants d'IoT une authentification pour les utilisateurs d'objets connectés (v. fiche sur le droit applicable).

La mise en œuvre d'objets connectés en matière de santé intervient dans un cadre particulièrement contraint et encadré. Avec un fil rouge spécifique en matière de sécurité et de lutte contre les risques.

Les objets connectés en pratique

- Réalisez une étude d'impact pour vous assurer du cadre juridique du traitement de données envisagé et prenez toutes les mesures juridiques et techniques nécessaires
- Rédigez des documents de présentation des mesures mises en place au titre de la sécurité des données qui vous permettront de synthétiser vos dispositifs et de les encadrer, avant de les intégrer le cas échéant à votre registre des traitements
- Veillez à l'information des utilisateurs et des personnes concernées en privilégiant une information à deux niveaux (par exemple lors du paramétrage de l'objet connecté puis lors de l'activation de certaines fonctionnalités). Privilégiez des modalités d'information claires et lisibles
- Mettez en place une procédure d'alerte en cas de violation des données. Cette procédure vous permettra de former le personnel compétent et de dresser la liste des personnes impliquées ou devant être prévenues et intégrées au processus de décision
- Entreprenez des démarches de certification
- Le cas échéant, assurez-vous que vos données de santé sont hébergées dans un Cloud certifié HDS
- Enfin, référez-vous à l'annexe A du rapport de l'ENISA sur la cyber-sécurité en matière de santé qui constitue un guide utile

Ressources

[1] *Anaïs Moutot, « La santé, nouveau terrain de jeu des GAFA », Les Echos, 2019, p. 11*

[2] *https://www.entreprises.gouv.fr/files/files/directions_services/etudes-et-statistiques/prospective/technologies-de-sante/2019-06-IF-SANTE-Synthese-WEB.pdf*

[3] *https://www.forbes.com/sites/emmawoollacott/2019/12/09/uk-government-hands-nhs-data-to-amazon-for-free/*

[4] *https://aioti.eu/wp-content/uploads/2020/02/IoTInnovationClustersFinalReportFINALpdf.pdf*

[5] *Les objets connectés de santé et l'apparition du « patient-consommateur », Cahiers de droit de l'entreprise n°5, Sept. 2019, dossier 32 Béatrice ESPESSON*

[6] *Fasc. 945, données de santé à caractère personnel, Lexis Nexis*

[7] *https://www.ccne-ethique.fr/sites/default/files/avis_130.pdf*

[8] *https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG07Report2015-Wearables.pdf*

[9] *Manifeste pour l'innovation en cancérologie - https://www.roche.fr/content/dam/rochexx/roche-fr/roche_france/fr_FR/doc/Manifeste%20ROCHE%20290917%20VF.pdf*

[10] *https://solidarites-sante.gouv.fr/IMG/pdf/rapport_donnees_de_vie_reelle_medicaments_mai_2017vf.pdf*

[11] *https://www.has-sante.fr/upload/docs/application/pdf/2016-11/has_ref_apps_oc.pdf*

[12] *https://www.cnil.fr/sites/default/files/atoms/files/guide-cnom-cnil.pdf*

[13] *https://www.cnil.fr/fr/quelle-strategie-de-controle-pour-2020*

[14] *http://www.institutdroitsante.fr/wp-content/uploads/2017/01/jdsam-n15.pdf, A. Debet, Objets connectés et santé*

[15] *Conclusions de l'avocat général dans l'affaire C-311/18 - https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165fr.pdf*

[16] *https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf*

[17] *https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-fr.pdf*

[18] *https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf*

[19] *https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf*

[20] *https://databreachcalculator.mybluemix.net/?_ga=2.50017121.671316266.1585326777-52469742.1585326777&cm_mc_uid=01057019543915853267769&cm_mc_sid_50200000=41901471585326776909&cm_mc_sid_52640000=21317641585326792103*

[21] *https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN*

[22] *https://www.zdnet.fr/actualites/chu-de-rouen-un-ransomware-au-centre-de-l-attaque-39894213.htm*

[23] *https://www.enisa.europa.eu/publications/healthcare-certification*

[24] https://www.ansm.sante.fr/content/download/163697/2140145/version/1/file/pi-190719-Cybersecurite_Recommandations-Eng.pdf

[25] https://ec.europa.eu/growth/sectors/medical-devices/new-regulations_en

[26] https://ec.europa.eu/docsroom/documents/37581

[27] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[28] Considérant 17, Annexe 1 - https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32017R0745&from=EN

[29] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148&from=EN

[30] https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services

DEROULEZ
AVOCAT

FICHE PRATIQUE N°4 - Mobilité connectée

« Supprimer la distance, c'est augmenter la durée du temps. Désormais, on ne vivra pas plus longtemps ; seulement, on vivra plus vite » Alexandre Dumas.

Selon une étude réalisée par PWC[1], la valeur intégrée par les véhicules connectés serait répartie aujourd'hui entre 90 % pour la partie consacrée à l'infrastructure du véhicule et à 10% pour les aspects logiciels. Selon l'Institut national de recherche en sciences et technologies du numériques, ces derniers aspects devraient représenter plus de la moitié des coûts de développement du véhicule d'ici quelques années et le logiciel embarqué comptera alors pour la majeure partie de sa valeur ajoutée[2].

Une telle redistribution de la chaine de valeur constitue ainsi un risque pour les constructeurs automobiles et une opportunité pour les éditeurs de logiciels de redistribution des revenus de l'industrie automobile. Avec un enjeu pour développer une offre attractive de véhicules connectés et de logiciels afférents. De plus l'attrait exercé par la masse de données collectée par les véhicules connectés constitue aussi un enjeu considérable, qu'il s'agisse de données personnelles ou non.

Le lien entre véhicule connecté et données personnelles connaît une très forte actualité. Ainsi et selon l'EDPB, un véhicule connecté peut être défini comme *« un véhicule équipé de nombreuses unités de contrôle électronique qui sont reliées entre elles par un réseau embarqué, ainsi que de moyens de connectivité lui permettant de partager des informations avec d'autres dispositifs à l'intérieur et à l'extérieur du véhicule. »*[3]

Un véhicule connecté traitant de données personnelles suppose donc :

- des données à caractère personnel recueillies par le véhicule
- que ces données soient issues des dispositifs internes aux véhicules ou des appareils personnels qui lui sont connectés (par exemple, le smartphone de l'utilisateur)
- que ces données soient exportées vers des intermédiaires externes (par exemple, les constructeurs automobiles, les éditeurs de logiciels, les compagnies d'assurance, les garagistes) en vue d'un traitement ultérieur.

Il faut encore souligner que le nombre de données échangées par un véhicule connecté va croissant avec le degré d'autonomie dudit véhicule puisqu'un degré d'automatisation avancé suppose pour le véhicule d'interagir avec son environnement.

6 niveaux d'autonomie peuvent être distingués notamment en reprenant les critères de la NHSTA[4] (*National Highway Traffic Safety Administration*) :

- Niveau 0 : Le conducteur conduit sans aucune assistance.
- Niveau 1 : Un système avancé d'aide à la conduite installé sur le véhicule peut parfois aider le conducteur à diriger ou à freiner/accélérer, mais pas les deux simultanément.

- Niveau 2 : Un système avancé d'assistance au conducteur sur le véhicule peut lui-même, dans certaines circonstances, contrôler simultanément la direction et le freinage/l'accélération. Le conducteur doit continuer à être pleinement attentif à tout moment et conduire seul.

- Niveau 3 : Un système de conduite automatisé installé sur le véhicule peut lui-même, dans certaines circonstances, assurer tous les aspects de la conduite. Dans ces circonstances, le conducteur doit être prêt à reprendre le contrôle du véhicule à tout moment lorsque le système le lui demande.

- Niveau 4 : Un système de conduite automatisé installé sur le véhicule peut lui-même effectuer toutes les tâches de conduite et prendre en considération l'environnement extérieur dans certaines circonstances. Le conducteur n'a pas besoin d'y prêter attention dans cette situation.

- Niveau 5 : Un système de conduite automatisé installé sur le véhicule peut effectuer toute la conduite dans toute circonstance. Le conducteur n'est qu'un passager et n'a pas besoin de participer à la conduite.

Au regard des différents éléments présentés, de nombreuses questions se posent en termes de cybersécurité et de traitement de données personnelles appliqués aux véhicules connectés. En plus de la problématique de la réparation du dommage causé par un véhicule connecté. Les nouvelles architectures technologiques ne cessent pas non plus de modifier le champ des possibles en matière d'objets connectés et perturbent l'encadrement juridique de ces véhicules.

Edge computing et véhicules connectés

Un premier défi consiste à concevoir et à déployer les réseaux de communication et l'écosystème informatique nécessaires pour fournir et traiter efficacement les données générées par les véhicules connectés. En effet, pour être autonome, un véhicule doit prendre des renseignements quant à son environnement. Cela suppose que des capteurs liés à un véhicule puissent identifier des signaux et s'informer via des relais d'information extérieurs au véhicule. C'est ce que l'*edge computing* et l'arrivée de la 5G vont notamment faciliter.

En effet, le déploiement de la 5G, qui est le cinquième réseau de télécommunication mobile et dont la rapidité a pour but de répondre à l'extension des échanges de données, va favoriser l'*edge computing*. Cette notion peut être définie comme *« une architecture informatique distribuée ouverte qui présente une puissance de traitement décentralisée »*[5] permettant le déploiement des technologies de l'informatique mobile et de l'IoT. A l'inverse du cloud qui nécessite une centralisation des données, le traitement est réalisé par l'appareil lui-même ou par un serveur local.

L'utilisation de l'*edge computing* a du sens concernant les objets connectés puisque chacun de ces objets génère des données, souvent en grande quantité. Avec cette architecture, les systèmes de traitement et de stockage se trouvent également en périphérie, aussi près que possible de l'objet connecté, de l'application ou de l'utilisateur qui produit les données traitées. Une application de conduite contrôlée d'une flotte de véhicules nécessitera une latence ultra-faible de bout en bout pour des signaux

d'avertissement, et des débits de données plus élevés pour partager des informations vidéo entre les véhicules et les infrastructures.[6]

A titre d'exemple, des applications de sécurité avancées permettront d'atténuer les accidents de la route, d'améliorer l'efficacité du trafic et favoriser la mobilité des véhicules d'urgence (ambulances, pompiers, police). Un autre exemple est celui de la collecte intelligente de déchets, en recourant à une application de gestion des déchets qui surveille le niveau de remplissage et l'état des conteneurs en temps réel, permettant ainsi une programmation et un acheminement dynamique des camions à ordure dans les villes[7].

Ces applications prévoient non seulement une communication de véhicule à véhicule ou de véhicule à infrastructure, mais aussi la communication avec les usagers de la route vulnérables tels que les piétons et les cyclistes. Le V2X[8] - *vehicule to everything* – recouvre ainsi toutes les situations suivantes, de communication d'un véhicule vers son environnement :

- le V2I - *vehicule to infrastructure* - priorité, feu rouge, etc.
- le V2V - *vehicule to vehicule* - prévision des collisions, etc.
- le V2N - *vehicule to network* - trafic en temps réel, routage, connexion au cloud ou edge computing, etc.
- le V2P - *vehicule to pedestrian* - alertes de sécurité pour les piétons ou cyclistes, etc.

Ainsi *« les logiciels pour la détection des risques, le stockage, la collecte, l'analyse et la transmission des données sont déployés sur des plateformes informatiques mobiles (edge computing). En raison de leur répartition géographique, de leur proximité avec les véhicules et de la légèreté de leur mise en œuvre, le système fonctionne en temps réel, ce qui garantit des services IoT centrés sur le consommateur. La combinaison de toutes les phases résout le principal défi (de l'intégration de véhicules connectés dans l'IoT) et fait des plateformes d'informatique périphérique une alternative appropriée à la plateforme en cloud pour les véhicules connectés. »*

Pour autant, cette nouvelle architecture apporte certaines complexités que l'AECC (*Automotive Edge Computing Consortium*) cherche notamment à résoudre et aborde dans son rapport *« Driving Data to the Edge ».*[9]

L'AECC a ainsi identifié un ensemble de questions clés et notamment la problématique de « *l'edge data offloading* » lorsque les réseaux de télécommunications doivent permettre le transfert de données de manière efficace et souple vers le point de relais décentralisé de traitement de données. De plus, les ressources informatiques doivent être sélectionnées et allouées de manière dynamique ainsi que la capacité de rediriger le trafic de données afin de satisfaire à l'exigence de continuité des services. Se pose à cet égard la question de l'identification du véhicule lorsque ce dernier transite entre différents réseaux d'accès.

L'une des raisons du développement de la 5G est sa flexibilité permettant un déploiement à peu onéreux. Assurer la connectivité de toutes les zones concernées de manière viable requière cependant des infrastructures réseau, des dispositifs, un fonctionnement et une maintenance à très faible coût.[10] Ces avantages expliquent bien pourquoi l'*edge computing* pourrait se développer avec le déploiement de la 5G.

Il faut noter à ce titre le lien clairement établi par l'Union européenne entre le développement de la 5G et celui des véhicules connectés, comme en témoigne le projet de corridors 5G transfrontières[11].

Un second défi réside dans la question de l'interopérabilité[12] entre les objets connectés et plus particulièrement entre les véhicules connectés. Le département des transports américain a souligné ce point dans son plan stratégique 2020-2025 sur les systèmes de transports intelligents et insisté sur la nécessite suivante[13]: *« Aider à éliminer les cloisonnements de données et à établir des interfaces interopérables entre les propriétaires et les exploitants d'infrastructures, les fabricants d'équipements et les responsables de données sur des éléments clés tels que les cartes numériques ou les données opérationnelles à l'échelle du système ».*

Dans la mesure où les différents véhicules ont et auront des impératifs de communication entre eux, mais aussi avec des bases de données locales en *edge computing* ou à des *data centers,* le choix des canaux de communication est primordial pour le développement d'objets connectés et l'interopérabilité fait partie des questions stratégiques en termes de gouvernance des données.

Aussi, la convergence des technologies de communication V2X avec des capteurs avancés à l'intérieur du véhicule, combinée à une connectivité de réseau omniprésente et de données disponibles sur le trafic permettent une conduite coopérative automatisée. Pour autant, cette automatisation ne doit pas se faire au détriment du respect de la vie privée des utilisateurs.

Données, véhicules connectés et vie privée

En France, la loi du 24 décembre 2019 d'orientation des mobilités a notamment pour objet de favoriser le développement des véhicules connectés[14] en consacrant l'open data des données de mobilités. Sont concernées les données statiques (arrêts, horaires, tarifs...) et en

temps réel (perturbations, disponibilités...) des transports en commun ou à la demande et les données des réseaux routiers et de stationnements. La loi LOM autorise également le Gouvernement à rendre accessible, par voie d'ordonnance, toutes les données pertinentes des systèmes intégrés aux véhicules, nécessaires aux gestionnaires d'infrastructures routières, aux forces de l'ordre et aux services d'incendie et de secours[15]. Le Gouvernement peut aussi rendre accessibles, en cas d'accident de la route, les données des dispositifs d'enregistrement de données d'accident et les données d'état de délégation de conduite enregistrées dans la période qui a précédé l'accident aux officiers et agents de police judiciaire aux fins de détermination des responsabilités. Ces données peuvent aussi être transférées aux assurances qui garantissent les véhicules impliqués dans l'accident. De plus, pourront être disponibles, les données strictement nécessaires pour déterminer l'activation ou non de la délégation de conduite du véhicule aux fins d'indemniser les victimes en application de la loi Badinter du 5 juillet 1985. Pourront également avoir accès aux données, les autorités organisatrices de la mobilité, pour leur mission d'organisation de la mobilité, et les gestionnaires d'infrastructures routières à des fins de connaissance du trafic routier, les données produites par les services numériques d'assistance au déplacement.

Il s'agit de permettre que 100% des informations sur les solutions de transports disponibles soient accessibles en un clic. Aucune mesure réglementaire prévue par cette loi n'a été prise par le Gouvernement pour le moment mais l'entrée en vigueur est prévue au plus tard pour 2021.

L'ouverture des données va dès lors favoriser l'essor des véhicules connectés car, *« le partage de l'information d'une voiture connectée est un facteur de sécurité sur la route, d'optimisation des coûts, d'amélioration de l'expérience client. Cependant c'est aussi un sujet de confidentialité qui devra faire l'objet de règles sur le respect de la confidentialité et la construction de scénarios d'usage de la donnée (donnée d'intérêt général versus donnée confidentielle). »*[16]

La CNIL a publié un pack de conformité relatif aux véhicules connectés et aux données personnelles[17] avant même l'entrée en vigueur du RGPD. L'EDPB a plus récemment approfondi le sujet en publiant des lignes directrices sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité[18].

Quelles sont les données personnelles concernées ? Ces données personnelles comprennent l'ensemble des données associées ou pouvant l'être à une personne physique (conducteur, titulaire de la carte grise, passager, etc.), notamment via le numéro de série du véhicule. Selon la CNIL, il peut s'agir de données directement identifiantes (état civil) comme de données indirectement identifiantes. Constituent des données indirectement identifiante, les données recoupées avec d'autres informations et qui permettent ainsi de déterminer l'identité d'une personne. Par exemple, une adresse IP du système du véhicule peut très bien constituer une donne personnelle dans la mesure où celle-ci serait recoupée avec d'autres informations telles que des données relatives aux trajets réguliers, immatriculation, au nombre de kilomètres parcourus, au lieu d'achat, au lieu de réparation habituel ou à des habitudes de consommation etc.

Photo by NESA by Markers van den Brik on Unsplash

Les données de géolocalisation sont par ailleurs des données qui proviennent de la fonction même du véhicule. Pour autant, les responsables de traitements et sous-traitants doivent garder à l'esprit que les données de géolocalisation peuvent également révéler des habitudes personnelles des personnes concernées. Ainsi, les trajets effectués peuvent permettre de déduire le lieu de travail et de résidence, les centres d'intérêt d'un conducteur. A ce titre, l'EDPB souligne que des informations sensibles peuvent être déduites des données de géolocalisation, telles que la religion à travers le lieu de culte. En conséquence, le fabricant de véhicules et d'équipements, le prestataire de services et les autres responsables du traitement des données doivent respecter le principe de minimisation des données. À titre d'exemple, lorsque le traitement consiste à détecter le mouvement du véhicule, le gyroscope est suffisant pour remplir cette fonction, sans qu'il soit nécessaire de collecter des données de localisation.

L'EDPB a apporté dans ses lignes directrices des directives concrètes aux responsables de traitement en les invitant notamment à :

- informer systématiquement les utilisateurs sur les finalités du recueil des données de géolocalisation
- obtenir le consentement des utilisateurs spécifiquement pour la question de la géolocalisation et en fonction de la finalité envisagée
- ne pas recueillir les données de géolocalisation en continue
- favoriser l'utilisation d'icônes pour signaler à l'utilisateur les situations où sa position est géolocalisée
- ne pas configurer par défaut la géolocalisation
- prévoir la possibilité de désactiver la géolocalisation à tout moment

- limiter la durée de conservation des données de géolocalisation.

Au titre de la mise en œuvre du principe de *privacy-by-design*, il est par ailleurs recommandé d'utiliser des procédés qui ne transfèrent pas de données à caractère personnel à l'extérieur du véhicule (c'est-à-dire que les données sont traitées en interne par le système du véhicule). Ce scénario présente l'avantage de garantir à l'utilisateur le contrôle complet de ses données personnelles. Avec cette conception, c'est l'architecture même de l'objet connecté qui prend en compte et intègre le principe de *privacy-by-design*. Notamment en interdisant tout traitement de données par des tiers à l'insu de l'utilisateur. Cette architecture permet également de traiter des données sensibles telles que des données biométriques ou des données relatives à des infractions, ainsi que des données de localisation détaillées tout en présentant moins de risques en matière de cybersécurité. Le recours à l'*edge computing* semble à ce titre plus adapté aux véhicules connectés que le recours au *cloud*. En plus d'être plus efficace, une telle architecture permet de garantir une meilleure sécurité et un traitement de données conforme au respect de la vie privée des personnes. Ceci d'autant plus que l'*edge computing* permet de ne pas faire transiter de données personnelles par un *cloud* parfois situé en dehors de l'Union européenne et qui peut poser alors la question des garanties liées à ces transferts.

Au regard des transferts de données personnelles hors du système interne au véhicule, l'EDPB souligne qu'il est probable qu'une telle pratique ait pour conséquence de créer un risque pour les droits des utilisateurs. Dès lors, il sera probablement nécessaire de procéder à une analyse d'impact pour déterminer quels droits sont potentiellement touchés et quelles garanties mettre en place pour contrebalancer cette atteinte éventuelle.

Par ailleurs, il est recommandé le cas échéant de procéder à l'anonymisation des données qui auraient vocation à quitter le système du véhicule, sous réserve de disposer d'un processus d'anonymisation efficace et effectif.

L'interface utilisateur du véhicule connecté doit également permettre au conducteur et à ses passagers d'aisément comprendre leurs droits lorsqu'ils utilisent le système de bord ou l'un des logiciels embarqués. Un système d'information à deux niveaux est là encore recommandé, c'est-à-dire que l'utilisateur doit pouvoir accepter les conditions générales d'utilisation du système au moment de la mise en service du véhicule mais il doit également être informé en cours d'utilisation du système lorsque de nouveaux logiciels ou services sont utilisés. A chaque fois il sera nécessaire que soient exposés les mentions obligatoires relatives au traitement de données personnelles (contact du responsable de traitement, moyens et finalités du traitement, nature des données personnelles recueillies, durée de conservation des données personnelles, droits de l'utilisateur, etc.)

Il nous semble aussi que la question de la responsabilité conjointe des différents acteurs impliqués sur un projet de véhicule connecté doit être soulevée au regard de la jurisprudence récente de la CJUE [19] et de l'élargissement de cette notion. En effet, la frontière est parfois complexe entre la qualité de responsable de traitement, de responsable de traitement conjoint et de sous-traitant. Par conséquent, il est conseillé aux constructeurs automobiles de

prévenir tout risque, en évaluant et en analysant la nature de chaque partie intervenant et participant au fonctionnement d'un véhicule connecté lorsque des données personnelles sont concernées. Dans le cas d'une responsabilité conjointe, ces responsables de traitement devront contractualiser leurs relations et devront en informer les utilisateurs.

Cybersécurité et véhicules connectés

La question de la sécurité des véhicules connectés est cruciale. L'ENISA a ainsi publié deux guides de bonnes pratiques[20] à destination des constructeurs et prestataires de logiciels, composants et autres pièces, au sujet de la sécurité des véhicules connectés. Ces deux guides de bonnes pratiques détaillent de façon exhaustive les mesures à mettre en place pour garantir la sécurité des véhicules connectés.

Les constructeurs de véhicules connectés doivent d'abord identifier les risques éventuels, risques qui sont potentiellement très larges[21] :

- la clé connectée du véhicule
- la prise USB, le Bluetooth, le Wifi, une des puces téléphoniques embarquées
- un smartphone ou montre connectée reliée au véhicule
- le point de recharge électrique
- le boîtier OBD, qui sert de prise de diagnostic pour les réparateurs en fournissant les données sensibles du véhicule (emplacement, informations sur la conduite…) ou par la valise diagnostic que les dépanneurs branchent dessus
- les dispositifs de connexion d'*edge computing*
- le *data center* du constructeur automobile qui présente un risque pour des millions de véhicules.

Parmi les risques les plus problématiques, l'ENISA relève notamment les attaques visant à exploiter une vulnérabilité de la console de communication du système de bord (absence de protection contre le *relay attack*, absence d'authentification, etc.), les attaques directes contre le logiciel de contrôle du véhicule, attaque sur des serveurs de télécommunication pour influencer le comportement des voitures en compromettant les données cartographiques dans le but d'affecter les contrôles de vérification ou même de modifier les données sur les conditions de circulation pour changer l'itinéraire de la voiture…. Il existe aussi l'utilisation de fausses communications pour déployer des microgiciels malveillants avec l'utilisation d'une unité de communication malveillante via l'infrastructure de télécommunication, telle qu'une station émettrice-réceptrice, un routeur Wi-Fi, une *Roadsite Unit*, dans le but de diffuser un logiciel malveillant ou simplement de perturber les communications de l'infrastructure. Il faut encore citer le déploiement à grande échelle de microgiciels malveillants après le piratage de serveurs de prestataires. Ces quelques attaques ne sont que des façons d'entrer de pénétrer le système du véhicule connecté et les applications n'ont de limite que l'imagination des hackers.

En termes de sécurité, l'EDPB recommande donc plusieurs préconisations aux acteurs de l'automobile :

- le cryptage des canaux de communication au moyen d'un algorithme
- la mise en place d'un système de gestion des clés de cryptage qui soit unique à chaque véhicule, et non à chaque modèle
- le cryptage des données lorsqu'elles sont stockées à distance, au moyen d'algorithmes
- le renouvellement régulier des clés de cryptage
- l'authentification des dispositifs de réception des données
- une garantie de l'intégrité des données (par exemple, par le hachage)
- un accès aux données à caractère personnel via des techniques fiables d'authentification des utilisateurs (mot de passe, certificat électronique, etc.).

En ce qui concerne plus particulièrement les constructeurs de véhicules, l'EDPB recommande la mise en œuvre des mesures de sécurité suivantes et notamment de :

- séparer les fonctions vitales du véhicule de celles qui reposent toujours sur les capacités de télécommunication (par exemple, l'*infotainment*)
- de permettre aux constructeurs de véhicules de corriger rapidement les vulnérabilités de sécurité pendant toute la durée de vie du véhicule
- de donner la priorité à l'utilisation de fréquences sécurisées spécifiquement dédiées aux transports
- mettre en place un système d'alarme en cas d'attaque des systèmes du véhicule, avec la possibilité de fonctionner en mode dégradé
- conserver un historique de tout accès au système d'information du véhicule, par exemple en remontant jusqu'à six mois au maximum, afin de permettre de com-

prendre l'origine de toute attaque potentielle et de procéder périodiquement à un examen des informations enregistrées afin de détecter d'éventuelles anomalies.

De plus et afin de garantir la sécurité des données personnelles des utilisateurs, il est aussi recommandé de procéder à une certification des systèmes embarqués dans le véhicule connecté (ISO/TC 204, ISO 26262, ETSI TS 102 940, ETSI TS 102 941, ETSI TS 103 097, etc.)

Ce point est en tout état de cause particulièrement important et a été intégré par la Commission européenne dans son programme ambitieux en matière de véhicules connectés[22].

Responsabilité et véhicules connectés

« Une décision prise par un véhicule autonome, sans intervention humaine, n'est en définitive que le résultat de l'exécution d'un programme informatique : qui définira les règles éthiques inscrites dans ce programme ? Qui vérifiera que les bases de données utilisées pour l'apprentissage des intelligences artificielles sont suffisantes et n'induisent pas des biais ? »[23]

Avant de chercher à déterminer toute responsabilité, il est nécessaire de mettre en avant l'opportunité que représente la certification des intelligences artificielles dans ce cadre. En effet et à ce titre, le livre blanc de la Commission européenne sur l'intelligence artificielle rappelle que les données d'entrainements des IA devraient utiliser un ensemble de données suffisamment large pour éviter tout mécanisme de discrimination mais aussi pour que tous les scénarios possibles soient envisagés. La question de la certification des IA va de pair avec celle de la responsabilité civile voire pénale lorsque le conducteur a délégué la conduite à la machine. Une éventuelle certification permettrait de mieux contrôler qui du constructeur, de l'IA ou du conducteur a commis une faute.

En France, la réparation des accidents de la route est encadrée par la loi Badinter sur les véhicules terrestres à moteur du 5 juillet 1985, avec pour principe que les dommages causés par un véhicule sont en principe quasiment toujours imputables au conducteur du véhicule. Quid de son application à des véhicules autonomes connectés ? Ne nécessitant que l'implication d'un véhicule terrestre à moteur dans un accident de la route, la loi Badinter pourrait très bien s'appliquer aux voitures autonomes. En effet, le conducteur n'est envisagé qu'en tant que responsable et son action ne constitue pas une condition d'application de la loi Badinter. Dans une telle situation, le conducteur aurait par la suite la possibilité de se retourner contre le fabricant (constructeur automobile), au moyen de la législation sur les produits défectueux ou encore en invoquant un vice caché.

Pour autant, la convention de Vienne sur la circulation routière[24] à laquelle la France est partie, impose la présence d'un conducteur responsable dans tout véhicule. L'étude d'impact de la loi d'orientation des mobilités souligne qu'il est par conséquent nécessaire de modifier la convention de Vienne, afin de pouvoir recourir aux véhicules connectés sur les voies publiques. Ce préalable de révision s'impose à l'entrée en vigueur de l'ordonnance que le Gouvernement est habilité à prendre avec la loi d'orientation des mobilités, concernant la circulation de véhicules connectés sur les voies publiques. Le Gouvernement aura également à

se prononcer par ordonnance pour éventuellement adapter le régime de responsabilité des véhicules, aux véhicules autonomes. A noter toutefois, les dispositions de la loi PACTE[25] prévoient en matière d'expérimentation de « véhicules à délégation de conduite », que le conducteur n'est responsable pénalement des dommages causés par le véhicule que lorsqu'il dirige le véhicule ou que le véhicule lui demande de reprendre la main. Lorsque le conducteur a délégué la conduite, c'est - pour le moment et dans le cadre des expérimentations – le titulaire de l'autorisation d'expérimentation qui peut voir sa responsabilité engagée si le véhicule autonome est la cause d'un accident.

Le développement des véhicules connectés constitue ainsi un chantier particulièrement intéressant et susceptible d'entraîner une modification du cadre juridique et réglementaire à court terme.

Les objets connectés en pratique

- Identifiez les parties prenantes à ce projet et leur rôle, ainsi que leurs responsabilités en matière de données personnelles
- Évaluez l'ensemble des données potentiellement concernées ainsi que les données personnelles et données sensibles
- Auditez les enjeux de protection des donnée personnelles
- Recourez à l'anonymisation des données personnelles et mettez en place un processus d'authentification des utilisateurs
- Favorisez une information graphique et en plusieurs niveaux

Ressources :

---

[1] https://www.pwc.fr/fr/decryptages/mobilite/le-vehicule-connecte-et-la-conduite-autonome.html

[2] https://www.inria.fr/sites/default/files/2019-10/inrialivreblancvac-180529073843.pdf

[3] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en

[4] https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety#issue-road-self-driving

[5] https://www.hpe.com/fr/fr/what-is/edge-computing.html

[6] https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf

[7] https://access.atis.org/apps/group_public/download.php/51129/ATIS-I-0000075.pdf

[8] https://www.3gpp.org/v2x

[9] https://aecc.org/resources/publications/

[10] https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf

[11] https://ec.europa.eu/digital-single-market/en/cross-border-corridors-connected-and-automated-mobility-cam

[12] https://lepoool.tech/acklio-leve-2-millions-deuros-pour-devenir-le-leader-mondial-de-linteroperabilite-et-de-la-securite-des-reseaux-iot/

[13] https://www.its.dot.gov/stratplan2020/ITSJPO_StrategicPlan_2020-2025.pdf

[14] http://www.senat.fr/dossier-legislatif/pjl18-157.html

[15] https://www.actualitesdudroit.fr/browse/tech-droit/objets-connectes/25289/lom-et-vehicules-connectes-les-forts-enjeux-de-l-ouverture-des-donnees

[16] https://www.pwc.fr/fr/decryptages/mobilite/le-vehicule-connecte-et-la-conduite-autonome.html

[17] https://www.cnil.fr/sites/default/files/atoms/files/pack_vehicules_connectes_web.pdf

[18] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en

[19] http://curia.europa.eu/juris/document/document.jsf;jsessionid=6550692C0E28C6A237502B8B1F45ABCA?text=&docid=216555&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=5811351 ; http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130da9f0ec7f929864a3ba51fde3524183ae3.e34KaxiLc3eQc40LaxqMbN4Pb3iPe0?text=&docid=202543&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=501792

[20] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars ; https://www.enisa.europa.eu/publications/smart-cars

[21] *https://lemag.bureauveritas.fr/a-la-une/proteger-les-vehicules-connectes-des-cyber-attaques/*

[22] *https://ec.europa.eu/digital-single-market/en/connected-and-automated-mobility-europe*

[23] *https://www.inria.fr/sites/default/files/2019-10/inrialivreblancvac-180529073843.pdf*

[24] *https://www.unece.org/fileadmin/DAM/trans/conventn/Conv_road_traffic_FR.pdf*

[25] *https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000037080861&type=general&legislature=15*

www.cabinetderoulez.com

contact@cabinetderoulez.com

Twitter : @Deroulez_Avocat

Linkedin : Jerome Deroulez

Github : Jérôme Deroulez