INSTITUT DE LA SOUVERAINETÉ NUMÉRIQUE

afnic

INTERNET DES OBJETS & SOUVERAINETÉ NUMÉRIQUE

PERSPECTIVES INDUSTRIELLES ET ENJEUX DE RÉGULATION

INTERNET DES OBJETS & SOUVERAINETÉ NUMÉRIQUE

PERSPECTIVES INDUSTRIELLES ET ENJEUX DE RÉGULATION

Coordonné par Bernard Benhamou
secrétaire général de l'Institut
de la Souveraineté Numérique

Ce rapport a été réalisé par l'Institut de la Souveraineté Numérique (ISN) en partenariat avec l'Afnic et il a été coordonné par Bernard Benhamou, secrétaire général de l'ISN bernard.benhamou@souverainetenumerique.fr.

Les technologies les plus profondes sont celles qui disparaissent. Elles se fondent dans la trame de la vie quotidienne jusqu'à en devenir indiscernables.

Mark Weiser, *directeur des technologies au Xerox Palo Alto Research Center (1991)*[1]

L'Internet des objets ne consiste pas seulement à localiser des objets et à les utiliser pour détecter les modifications de l'environnement ou pour accomplir des tâches automatisées. C'est un moyen de surveiller, de mesurer et de comprendre le mouvement continu du monde et des actions que nous menons. [...] Les données générées par l'Internet des objets permettront de mieux comprendre les relations physiques, les comportements humains et même les règles physiques de notre univers.

Samuel Greengard

The Internet of Things (2015)[2]

1. *The Computer for the 21st Century* (Mark Weiser, Scientific American 1991) courses.cs.washington.edu/courses/cse440/07au/readings_files/Weiser-Computer21stCentury-SciAm.pdf

2. The Internet of Things Samuel Greengard (MIT Press, 2015)

TABLE DES MATIÈRES

INTRODUCTION

En l'espace de quelques années, le champ d'application des technologies de « *l'Internet des objets* » n'a cessé de s'étendre : de l'optimisation des processus industriels à la maîtrise de l'énergie, des transports autonomes au contrôle environnemental, de la sécurité sanitaire à l'agriculture. Ces technologies contribuent au développement de nouvelles filières industrielles et aident à la mise en œuvre des politiques publiques en particulier dans le domaine environnemental. Les projets des gouvernements, des administrations et des collectivités territoriales intègrent déjà de nombreux volets basés sur l'Internet des objets, qu'il s'agisse de l'organisation des transports, de la sécurité sanitaire ou encore des villes intelligentes[3]. La connexion à l'Internet de l'ensemble des objets qui nous environnent, constitue ainsi un défi stratégique et politique pour l'ensemble des acteurs industriels et des États européens.

Pour les pays de l'Union, la souveraineté numérique ne consiste plus seulement à conserver la maîtrise de leurs infrastructures informationnelles ou garantir leur indépendance vis-à-vis des technologies extra-européennes. Il s'agit aussi de veiller à ce que ces technologies ne remettent pas en cause nos libertés fondamentales ou même les bases de nos systèmes de protection sociale. En effet, l'Internet des objets pose des questions nouvelles sur l'intrusion de ces technologies dans la vie privée des citoyens ainsi que sur les nouvelles menaces qu'elles pourraient faire peser sur le fonctionnement de nos démocraties. Pour la France comme pour l'Europe, l'objectif est désormais de créer les technologies et les réglementations qui permettront de développer un Internet des objets en accord avec les principes

3. *Internet of Things: The New Government To Business Platform a Review of Opportunities, Practices, and Challenges* (Banque Mondiale, 3 novembre 2017) http://documents1.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf

partagés par les Européens. En effet, ces technologies pourraient conditionner à l'avenir l'exercice des droits et libertés fondamentaux des citoyens et plus largement la protection de l'État de droit et de la démocratie.

La souveraineté numérique est aussi devenue un objectif stratégique pour la Commission européenne dans le cadre du développement des technologies de l'Internet des objets. Pour Thierry Breton, commissaire européen au Marché intérieur, l'Union doit en finir avec la naïveté qui a marqué jusqu'ici son action dans le domaine des technologies :

> Nous allons renforcer la protection de notre espace informationnel, encore trop largement dominé par des acteurs géo-économiques non européens. Établir les règles permettant de créer un espace unique européen de la donnée. L'Europe a manqué la première vague de l'économie des données personnelles. Elle ne perdra pas la main sur l'énorme potentiel des données industrielles qui attisent tous les regards, au premier rang desquels les *GAFAMs* et autres *BATX*. Sécuriser les réseaux *5G* est un impératif : aucune vulnérabilité n'est permise dans ces infrastructures critiques. Nous y travaillons. En outre, nous finalisons une nouvelle stratégie de cybersécurité - un « bouclier cyber européen » - pour prendre en compte l'arrivée de milliards d'objets connectés, de la voiture jusqu'aux jouets d'enfants en passant par les appareils de santé ou l'électroménager. Données industrielles, *5G*, cyber sécurité, puissance de calcul vont conditionner notre souveraineté pour des décennies[4].

4. *La fin de la naïveté*, tribune de Thierry Breton, Les Échos 10 août 2020) www.lesechos.fr/idees-debats/cercle/la-fin-de-la-naivete-1229485

1

TECHNOLOGIES ET ÉVOLUTIONS DES OBJETS CONNECTÉS

Les premières générations d'objets connectés disponibles auprès du grand public correspondaient à des appareils électroniques complexes (smartphones, tablettes, enceintes connectées, voitures connectées…), l'autre versant des technologies de l'Internet des objets, correspondait à des capteurs, puces *RFID* et dispositifs connectés pour le contrôle, le suivi et l'optimisation des processus de production et de logistique. Ces technologies des *« usines intelligentes »* représentent actuellement l'un des plus importants marchés mondiaux pour l'Internet des objets. Le cabinet d'étude *Gartner* prévoit que, d'ici à 2024, plus de la moitié des applications utilisées en entreprise seront conçues pour l'Internet des objets[5].

Désormais, nous pourrions assister à une convergence des technologies de l'Internet industriel et des technologies des objets connectés au-delà des appareils électroniques traditionnels. Cette nouvelle phase du développement de l'Internet des objets pourrait correspondre à l'essor de services autour des produits connectés et au-delà des *« environnements connectés »*. L'Internet des objets connaît ainsi de nombreuses appellations différentes en fonction de l'origine de ces technologies ou des stratégies des acteurs industriels. Certaines de ces appellations correspondent à des marques déposées et, au-delà des objets ou des produits connectés, elles anticipent l'évolution vers un *« monde connecté »* (cf. tableau 1).

5. *Gartner's IT Automation Predictions for 2020* (Advanced Systems Concepts - IT Automation Without Boundaries 2020) info.advsyscon.com/it-automation-blog/gartner-it-automation

INTERNET DES OBJETS (IdO)
SYNONYMES ET ORIGINES

- **Machine to Machine** (M2M, Theodore Paraskevakos, 1968[1])
- **Ubiquitous Computing** (Mark Weiser, 1993[2])
- **Internet of Things** (IoT, Kevin Ashton, 1999[3])
- **Ambient Intelligence** (*Philips* 1998[4]/*Commission européenne,* 2001[5])
- **Everyware** (Adam Greenfield, 2006[6])
- **Object Hyperlinking** ou **Phylinking** (*Microsoft* Tags, 2009[7])
- **Web of Things** (*Ericsson,* 2012[8])
- **Smarter Planet** (*IBM,* 2008[9])
- **Industrial Internet** (*General Electric,* 2012[10])
- **Programmable World** (*Wired Magazine,* 2013[11])
- **Internet of Everything** (*Cisco,* 2013[12])
- **Physical Web** (*Google,* 2014[13])
- **Systèmes cyber-physiques** (Programme *Industrie 4.0,* 2015[14])
- **OMO (Online-Merge-Offline), O2O (Online-to-Offline)** (Kai-Fu Lee, 2018[15])

1. *The machines are coming: how M2M spawned the internet of things* (John Kennedy, Silicon Republic, 18 mai 2016) www.siliconrepublic.com/machines/m2m-cutting-edge-machines-internet-of-things-explained
2. *Some Computer Science Issues in Ubiquitous* Computing (Mark Weiser CACM, juillet 1993) graphics.stanford.edu/courses/cs428-03-spring/Papers/readings/General/Weiser_Ubi_CACM93.html
3. *Interview with Kevin Ashton – inventor of IoT: Is driven by the users* (Smart Industry 11 février, 2018) www.smart-industry.net/interview-with-iot-inventor-kevin-ashton-iot-is-driven-by-the-users/
4. F*rom Devices to "Ambient Intelligence": The Transformation of Consumer Electronics presentation* by E. Zelkha, B. Epstein, S. Birrell, C. Dodsworth and R. Pieper (Philips Research 1998) epstein.org/wp-content/uploads/DLR-Final-Internal.ppt
5. *Scenarios for Ambient Intelligence in 2010* (European Commission, février 2001) cs.millersville.edu/~bliffick/cs425/docs/ISTAG-Final.pdf
6. *Everyware: The Dawning Age of Ubiquitous Computing* (Adam Greenfield ,Ed. New Riders 2006)
7. *Microsoft and Object Hyperlinking* (Dr Dobbs, 6 janvier 2009) www.drdobbs.com/architecture-and-design/microsoft-and-object-hyperlinking/228701102
8. *A Social Web of Things* (Ericsson, 2012) www.ericsson.com/en/blog/2012/4/a-social-web-of-things

9. *IBM Smarter Planet* 2008
www.ibm.com/ibm/history/ibm100/us/en/icons/smarterplanet/

10. *Industrial Internet* (General Electric, 2012)
www.ge.com/europe/industrial-internet

11. *In the Programmable World, All Our Objects Will Act as One* (Wired Magazine, 14 mai 2013)
www.wired.com/2013/05/internet-of-things-2/

12. *The Internet of Everything Global Private Sector Economic Analysis* (Cisco 2013)
www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf

13. *The Physical Web* (Scott Jenson, Google 2014) github.com/google/physical-web

14. *Germany Industrie 4.0 Cyber Physical Systems – IoT Innovation* (RCR Wireless News, 29 octobre 2015)
www.rcrwireless.com/rcrtv/germany-industrie-4-0-cyber-physical-systems-iot-innovation-episode-22

15. *AI Superpowers: China, Silicon Valley, and the New World Order* (Kai-Fu Lee, HMH Books 2018)

1.1 Vers un monde « intrinsèquement numérique »

Lorsqu'il évoquait le principe qui régit la civilisation technologique, le prix Nobel de physique Dennis Gabor l'énonçait ainsi : *« Ce qui peut être fait le sera. Le progrès tend à appliquer de nouvelles techniques et à créer des industries, qu'elles soient réellement souhaitables ou non… »*[6]. Ce principe lorsqu'il s'applique à l'Internet des objets, pourrait être reformulé : *« Tout objet qui pourra être connecté le sera, que cela soit souhaitable ou non… »*.

> **“ Tout objet qui pourra être connecté le sera, que cela soit souhaitable ou non…**

Après l'automatisation des processus de l'Internet industriel, nous pourrions entrer dans l'ère des produits intelligents. Ainsi, au-delà de la connexion des appareils électroniques, la deuxième phase de développement de l'Internet des objets pourrait correspondre à la connexion de l'ensemble des objets du quotidien : vêtements, produits manufacturés, denrées alimentaires, médicaments… Comme le précise Niall Murphy, PDG de la société *Evrythng* : *« Chaque année, 3 500 milliards de produits manufacturés sont vendus dans le monde, et de nombreuses technologies leur permettent d'être identifiés pour ajouter des fonctions supplémentaires à ces produits… »*[7]. Pour l'équipementier

6. *Can We Survive Our Future ? A Conversation with Dennis Gabor* (Encounter Vol.38, No.1-6 janvier-juin 1972) archive.org/details/dli.bengal.10689.15707/page/n157/mode/2up

7. *By 2020, everything from clothes to food will be connected to the web (Wired Magazine UK,* 11 octobre 2017) www.wired.co.uk/article/niall-murphy-evrythng-internet-of-things-shopping-products

Cisco, le potentiel économique de ce qu'il nomme *"Internet of Everything"* provient du fait que 99,4 % des objets physiques qui pourraient un jour en faire partie sont encore *« non connectés »*[8].

La montée en puissance de l'Internet des objets ne résulte donc pas d'une forme de déterminisme liée à une évolution *« naturelle »* de l'Internet mais bien d'une convergence d'intérêts économiques, industriels et technologiques. Ainsi, l'effondrement du coût des capteurs, permet aujourd'hui une diversification massive de leurs usages au sein des objets connectés. De plus, l'augmentation des capacités de stockage et la diminution du coût des calculs rendent possible le traitement en masse des données issues des objets connectés. À cela s'ajoute désormais le caractère ubiquitaire des smartphones dont l'ergonomie et la « grammaire gestuelle » sont familières à plus de 3 milliards d'usagers dans le monde. Les terminaux mobiles sont ainsi devenus les *« télécommandes »* et les *« exo-cerveaux »* de nombreux autres objets connectés. Les capacités de mémoire et de traitement auparavant présentes sur les objets ont ainsi été transférées vers les terminaux mobiles. Cette division des tâches a permis de concevoir des objets plus économiques qui disposent du minimum d'intelligence et d'énergie nécessaires à leur fonctionnement.

Dans le même temps, le développement des technologies d'intelligence artificielle a permis d'automatiser le traitement des données recueillies pour faciliter la prise de décisions, par exemple dans l'aide au diagnostic médical, ou être en mesure d'effectuer des tâches complexes jusqu'alors réservées à des utilisateurs humains, comme le pilotage des véhicules autonomes. On assiste ainsi à la convergence des technologies de l'Internet traditionnel et de l'Internet des objets qui s'appuient sur des systèmes d'intelligence artificielle pour analyser et traiter les données issues de ces nouvelles générations d'objets connectés. Cette *« perception augmentée via l'intelligence artificielle »* pourrait constituer un levier essentiel pour la création

8. *The Internet of Everything Global Private Sector Economic Analysis* (Cisco 2013) www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf

de service à haute valeur ajoutée. Pour le spécialiste de l'intelligence artificielle, Kai-Fu Lee :

> Quand votre réfrigérateur indique à votre chariot de supermarché qu'il faut racheter du lait, évoluez-vous dans un monde physique ou numérique ? Ces nouveaux environnements intégrés forment ce que j'appelle l'*OMO*, pour online-merge-offline. En passant du commerce électronique aux services *O2O* (online-to-offline), nous avons déjà franchi un certain nombre d'étapes, chacune construisant de nouveaux ponts entre le virtuel et le réel. L'*OMO* représente un pas supplémentaire : la fusion totale de ces deux univers[9].

1.2 Des télécommunications dédiées à l'Internet des objets

Face au développement des objets connectés, des offres de télécommunication spécifiquement conçues pour l'Internet des objets ont été créées. Ces offres permettent d'articuler les systèmes de communication à courte portée (*NFC, RFID, Bluetooth, ZigBee*) avec des technologies de communication à moyenne et longue portée (*NB-IoT, LTE-M*) auxquels s'ajoutent désormais les communications *5G* et les systèmes à très longue portée via les communications satellitaires. En plus, des différences de portées, le « spectre » de ces technologies s'étend des communications à bas débit (*LoRa, Sigfox*) pour les capteurs les plus simples jusqu'aux communications à très haut débit ou à haute capacité. Ces technologies de communication concernent en particulier la gestion d'importantes flottes d'objets ou les applications temps réel les plus exigeantes en bande passante comme les dispositifs de réalité augmentée ou de réalité virtuelle. Une enquête réalisée en 2019 par *Ericsson* auprès de dirigeants de 100 opérateurs de télécommunications mondiaux a révélé que 92 % d'entre eux pensaient

9. *AI Superpowers: China, Silicon Valley, and the New World Order* (p. 118 Kai-Fu Lee, HMH Books 2018).

que la fonctionnalité *5G* la plus importante était liée au fait qu'elle ouvrirait la voie à d'autres innovations technologiques pour l'Internet des objets[10].

1.3 Technologies spatiales et Internet des objets européen

L'espace constitue déjà un nouveau territoire d'affrontement industriel, politique et militaire pour le suivi et la connexion des prochaines générations d'objets connectés. Les technologies spatiales (*space tech*) jouent en effet un rôle crucial dans le suivi des objets et des véhicules connectés. Ainsi, le système de géolocalisation satellitaire européen *Galileo*, dont la nouvelle génération de satellites vient d'être annoncée[11], devrait permettre d'améliorer encore la précision du suivi des objets en mouvement. Le programme *Galileo* participera ainsi à l'autonomie stratégique des pays de l'Union européenne pour la gestion de flottes d'objets connectés dans le domaine des transports, dans la gestion des infrastructures énergétiques ou encore dans l'urbanisme. Ce programme constitue la réponse européenne aux trois systèmes de géolocalisation satellitaire : *GPS* américain, *GLONASS* russe et *Beidou* chinois.

En plus de la géolocalisation des objets, c'est aussi l'échange d'informations issues de ces objets qui pourrait emprunter la voie de la communication satellitaire. Ainsi, parallèlement aux constellations satellitaires conçues pour assurer la connectivité mondiale à l'Internet (*Starlink de SpaceX, Kuiper Systems* d'Amazon, *OneWeb*) de nouvelles constellations de satellites en orbite basse ont été spécifiquement développées pour l'Internet des objets[12]. C'est le cas des constellations de nanosatellites *ELO* d'*Eutelsat*, de *Sateliot* pour la connexion *5G*, ou encore la constellation de la société

10. *5G and IoT: An in-depth review of how next gen mobile connectivity will unlock new opportunities* (UK Tech News, 22 septembre 2020) www.uktech.news/news/5g-and-iot-an-in-depth-review-of-how-next-gen-mobile-connectivity-will-unlock-new-opportunities-20200921

11. *Galileo next-gen satellites to be more powerful, reconfigurable* (GPS World, 14 août 2020) www.gpsworld.com/galileo-next-gen-satellites-to-be-more-powerful-reconfigurable/

12. *Internet of Things (IoT) via Satellite* (Fraunhofer Institute for Integrated Circuits IIS) www.iis.fraunhofer.de/en/ff/kom/satkom/satellite_iot.html

française *Kinéis*, dont les 25 satellites devraient être lancés en 2022[13]. Ces constellations de satellites devraient permettre de connecter potentiellement plusieurs dizaines de millions d'objets connectés.

1.4 Des freins progressivement levés…

En 2015, une étude du *Forum économique mondial* estimait que les principaux freins au développement de l'Internet des objets dans l'industrie étaient liés au défaut d'interopérabilité entre les solutions proposées, à l'absence de sécurité des objets connectés ainsi que l'immaturité des solutions technologiques proposées. Aux aspects technologiques s'ajoutaient des inquiétudes quant à l'acceptabilité sociale de ces technologies et en particulier leur impact sur la vie privée. Les personnes interrogées durant cette étude mentionnaient aussi les conséquences sociétales de ces technologies sur les organisations et sur l'évolution des métiers et donc sur l'emploi dans les prochaines années.

En l'espace de 5 ans, certains de ces obstacles technologiques ont été levés et de nombreuses filières industrielles ont développé des usages pour les capteurs connectés. Cependant, l'interopérabilité entre les différentes familles d'objets connectés n'est pas encore assurée et les failles de sécurité restent l'une des faiblesses majeures de ces technologies. Conscientes de l'impact de la sécurité des objets connectés sur le développement de ce marché, les autorités tant aux États-Unis qu'en Europe commencent à mettre en place des régulations spécifiques visant à renforcer la sécurité des objets connectés. En revanche, les questions liées aux conséquences de l'Internet des objets sur la vie privée des usagers n'en sont qu'à leurs premiers stades de formalisation par les régulateurs.

13. *Constellation de satellites: Kineis, le nouveau champion du New Space français* (Challenge, 3 février 2020) www.challenges.fr/entreprise/aeronautique/constellation-de-satellites-kineis-le-nouveau-champion-du-new-space-francais_697061

1.5 ...et des perspectives de croissance considérables

Pour les experts du *Forum Économique Mondial* : *« À elle seule, la contribution de l'Internet des objets industriel à l'économie mondiale pourrait s'élever à 14 000 milliards de dollars d'ici à 2030. Sa valeur économique augmenterait davantage encore si l'on y ajoute l'Internet des objets destinés aux consommateurs et au secteur public »*[14]. Les acteurs industriels impliqués dans les transformations de l'Internet des objets anticipent déjà une croissance considérable des besoins informatiques liés à ces technologies, ainsi : *« La société ARM conçoit les puces qui dominent le marché des microprocesseurs à faible consommation, et équipent une grande variété d'appareils, depuis les smartphones jusqu'aux téléviseurs. ARM planifie ses activités sur l'hypothèse qu'il devrait y avoir dans le monde 1000 milliards d'ordinateurs d'ici à 2035 »*[15].

En 5 ans, on a déjà observé dans le monde, un quadruplement des dépenses liées à l'Internet des objets. Cette progression concerne particulièrement les domaines de la fabrication industrielle, des transports, de l'énergie et des grands réseaux d'infrastructures. Ces secteurs de l'« *Internet des objets industriel* » représentent à eux seuls un marché de 40 milliards de dollars en 2020. Pour le cabinet *Statista,* les dépenses mondiales consacrées à l'Internet des objets pourraient atteindre 1600 milliards de dollars en 2025 (cf. étude *Statista 2020*)[16].

1.6 « Intelligent, piratable et ne vous appartient plus vraiment... »

L'introduction de systèmes de communications et de capteurs au sein des objets permet d'ajouter des fonctionnalités à cet objet et d'en

14. *Internet of Things Guidelines for Sustainability* (World Economic Forum, janvier 2018) www3.weforum.org/docs/IoTGuidelinesforSustainability.pdf

15. *The Internet of Things* - The Economist Technology Quarterly (septembre 2019)

16. *Global spending on IoT in 2015 and 2020, by industry sector in billion U.S. dollars* (Statista, 1er septembre 2020) www.statista.com/statistics/1095375/global-spending-on-iot-by-industry-sector/

modifier les usages. L'analyse des données issues des objets connectés apporte un surcroît d'information essentiel aux acteurs industriels pour leur permettre d'améliorer les services rendus par ces objets. Mais les informations issues de ces objets connectés permettent aussi d'améliorer la connaissance des comportements de leurs utilisateurs. Quelles pourront être les conséquences industrielles, sociales et politiques de l'essor des objets connectés dans nos sociétés ?

Loin de constituer un prolongement des services qui existaient jusqu'ici sur Internet, la connexion des objets du quotidien produira des effets nouveaux tant sur le paysage industriel et technologique que sur la relation que les usagers entretiennent avec leurs objets. En 2014, Alexis Madrigal et Robinson Meyer annonçaient ainsi dans *The Atlantic* que trois choses se produisent lorsqu'un objet se connecte à l'Internet : « *Il devient intelligent, il devient piratable et enfin il ne vous appartient plus vraiment…* »[17].

1.7 Les objets connectés : maillons faibles de la cybersécurité

Comme pour chaque appareil connecté à l'Internet, la possibilité d'accès distants crée aussi les conditions de nouvelles formes de vulnérabilité et d'attaques informatiques sur ces objets. La progression des différentes catégories d'objets connectés démultiplie la « surface d'attaque » et crée de nouvelles opportunités pour des hackers malveillants. Qu'il s'agisse d'attaques visant à utiliser ces objets connectés contre des infrastructures traditionnelles de l'Internet ou d'attaques visant spécifiquement les objets ou leurs utilisateurs. L'Internet des objets est devenu l'un des maillons faibles de la sécurité informatique mondiale et pourrait l'être plus encore avec l'essor de nouvelles générations d'objets connectés. Ainsi, en 2016, l'une des plus importantes attaques par déni de service massive (*DDoS*) jamais observée a été menée contre le service

17. *When Everything Works Like Your Cell Phone* (Alexis C. Madrigal & Robinson Meyer, The Atlantic, 28 septembre 2014) www.theatlantic.com/technology/archive/2014/09/when-everything-works-like-your-cell-phone/379820

Dyn Managed DNS via le malware *Mirai*. Cette attaque a affecté des entreprises majeures comme *Amazon*, *Twitter*, *Netflix*, *Github*, *Spotify* ou encore *OVH*. Elle a été menée en prenant appui sur des objets connectés autres que des ordinateurs traditionnels à la différence des précédentes générations d'attaques qui utilisaient des ordinateurs « zombies » contrôlés à l'insu de leurs utilisateurs : *« L'une des sources de l'attaque était constituée par des produits connectés à Internet tels que des imprimantes, des enregistreurs vidéo numériques et d'autres appareils de ce que l'on nomme « l'Internet des objets »*[18].

“La sécurité de l'Internet des objets, en plus d'être une préoccupation majeure pour les usagers, est devenue un enjeu de sécurité nationale pour les États...

Cette attaque constituait la première utilisation à grande échelle des objets connectés comme vecteur d'attaque contre les infrastructures « traditionnelles » de l'Internet. Depuis lors, d'autres types d'attaques ont été observés par les spécialistes de la cybersécurité de l'Internet des objets. Ces attaques étaient dirigées contre les objets connectés, les données qu'ils pouvaient recueillir, voire contre les utilisateurs eux-mêmes.

La sécurité de l'Internet des objets, en plus d'être une préoccupation majeure pour les usagers, est aussi devenue un enjeu de sécurité nationale pour les États. Depuis 2014 déjà, la *CIA* a fait savoir à quel point elle craignait que l'Internet des objets ne devienne le nouveau théâtre de conflits internationaux[19]. Ainsi en 2014 déjà, Dan Geer, responsable cybersécurité de la société de capital-risque de la *CIA* (*In-Q-Tel),* appelait les États et les citoyens à analyser lucidement leur dépendance vis-à-vis des services et des technologies de l'Internet des objets :

> À mesure que nos sociétés deviennent plus technologiques, le monde entier en vient à dépendre de la qualité informatique de dispositifs distants. Pour ne prendre qu'un exemple, notre chaîne d'approvisionnement alimentaire correspond à moins

18. *A massive cyberattack knocked out major websites across the internet* (Business Insider, 21 octobre 2016) www.businessinsider.fr/us/amazon-spotify-twitter-github-and-etsy-down-in-apparent-dns-attack-2016-10/

19. The CIA Fears the Internet of Things (Defense One, 24 juillet 2014) www.defenseone.com/technology/2014/07/cia-fears-internet-things/89660/

> d'une semaine de réserves, et cette chaîne dépend en tout point des services numériques, depuis les tracteurs agricoles pilotés par *GPS* aux dispositifs d'irrigation surveillés par drones, des robots de triage des légumes, à la logistique transocéanique des marchandises jusqu'au bétail étiqueté par des puces *RFID*. Toute cette dépendance technologique, et les données qui la sous-tendent, nous rendent-elles plus résilients ou plus fragiles ? Est-il important que l'accroissement de cette dépendance soit issu des systèmes préexistants et anciens ? Est-il essentiel de conserver des moyens manuels pour réaliser ces tâches afin de ne pas avoir à les réinventer dans l'urgence[20] ?

Ces propos résonnent aujourd'hui différemment à l'issue de la crise liée au *Covid-19*. En effet, la pandémie a démontré la dépendance de nos sociétés à des technologies et des approvisionnements qui pour l'essentiel étaient extra-européens. Les citoyens des pays de l'Union européenne ont alors pris conscience de leur vulnérabilité sanitaire mais aussi de leur dépendance technologique et industrielle. Dan Geer concluait alors son intervention, par sa définition de la cybersécurité : *« C'est l'absence de surprise totale. Mon choix personnel comme objectif suprême de l'ingénierie de la sécurité serait qu'aucune défaillance ne soit « silencieuse ».*[21] Cette définition issue d'un spécialiste de la cybersécurité, est aussi pertinente pour les usagers des technologies de l'Internet des objets. Cette sécurité et cette « absence de surprise » constituent des prérequis essentiels pour maintenir une acceptabilité sociale de ces technologies et éviter à l'avenir un rejet massif des technologies de l'Internet des objets.

Les technologies et les services liés à la sécurité des objets connectés constituent un marché essentiel pour l'ensemble des acteurs des technologies[22]. Or la sécurité de ces objets est longtemps restée rudimentaire. De l'absence de mécanismes de chiffrement pour la transmission des données[23], jusqu'à l'impossibilité d'intégrer des mises à jour

20. *Dan Geer, Security of Things* (7 mai 2014) geer.tinho.net/geer.secot.7v14.txt

21. *Ibid*.

22. *How the 'insecurity of things' creates the next wave of security opportunities* (TechCrunch 26 juin 2016) techcrunch.com/2016/06/26/how-the-insecurity-of-things-creates-the-next-wave-of-security-opportunities/

23. *Internet of Things Security Study : Smartwatches* (Étude Hewlett Packard Entreprise 2015) www.ftc.gov/system/files/documents/public_ments/2015/10/00050-98093.pdf

de sécurité, la sécurité des objets connectés constitue aujourd'hui l'un des maillons les plus faibles des infrastructures de l'Internet. Dans certains secteurs liés à la sécurité des personnes, comme les technologies de santé, ces failles deviennent même critiques. Ainsi, David Talbot dans la revue *MIT Technology Review* avertissait déjà en 2012 : « La présence de virus informatiques est devenue endémique dans les appareils médicaux connectés des hôpitaux. »[24]. Cinq ans plus tard, en 2017, ces mêmes vulnérabilités des objets médicaux connectés étaient encore pointées du doigt par le magazine *Wired* comme le cauchemar à venir pour les spécialistes de la cybersécurité[25]. Plus récemment dans son ouvrage sur Internet des objets et cybersécurité, Bruce Schneier faisait état de menaces inédites sur les personnes et plus seulement sur les infrastructures informationnelles : *« Nous vivons déjà dans un monde où les cyberattaques peuvent créer des accidents de voiture et paralyser des centrales électriques ; des actions qui, à grande échelle, peuvent facilement entraîner des décès en masse. Ajoutez à cela des attaques contre les avions, les appareils médicaux et à peu près toutes nos infrastructures critiques, et nous avons à envisager des scénarios assez effrayants… »*[26].

> **“Les cyberattaques peuvent créer des accidents de voiture et paralyser des centrales électriques ; des actions qui, à grande échelle, peuvent entraîner des décès en masse. Ajoutez à cela des attaques contre nos infrastructures critiques, et nous avons à envisager des scénarios assez effrayants…**
>
> **Bruce Schneier**

Dans son rapport sur la sécurité de l'Internet des objets élaboré pour l'*OTAN* (*Organisation du traité de l'Atlantique nord),* Matej Tonin précise qu'en matière de sécurité il conviendra d'intégrer des dispositifs de sécurité par défaut (*security by design*) dans les objets connectés plutôt que d'attendre que les industriels ne se décident spontanément à les adopter. Ceci d'autant plus que les risques associés aux failles

24. *Computer Viruses Are "Rampant" on Medical Devices in Hospitals* (MIT Technology Review, 17 octobre 2012) www.technologyreview.com/s/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

25. *Medical Devices Are the Next Security Nightmare* (Wired, 2 mars 2017) www.wired.com/2017/03/medical-devices-next-security-nightmare/

26. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (p. 9) Bruce Schneier, (Ed. Norton & Company, 2018)

de sécurité de l'Internet des objets peuvent avoir des conséquences « systémiques » pour les États :

> L'un des principaux débats sur la sécurité de l'Internet des objets et la protection de la vie privée consiste à savoir s'il faut « intégrer » d'emblée des protections solides ou si le marché doit d'abord décoller avant de mettre en place des sécurités supplémentaires. Pour les partisans de la première solution, les régulateurs peuvent éviter certains des défauts du développement de l'internet, conçu à l'origine pour des réseaux d'ordinateurs de confiance à petite échelle - et non pour un marché de masse rempli de ses cybercriminels. L'opinion selon laquelle cette « sécurité par défaut » devrait être l'objectif de la conception des dispositifs et des services est la position la plus répandue. [...] Un expert fait valoir que tous les dispositifs de l'Internet des objets n'ont pas besoin du même niveau élevé de sécurité et de protection de la vie privée. Il propose d'évaluer trois paramètres : la valeur des données collectées, la criticité des données et l'évolutivité de la défaillance. La protection devrait être maximale si les dispositifs et services de l'Internet des objets collectent et transmettent des données de grande valeur et/ou critiques, et/ou si la défaillance d'un élément peut se transformer en une défaillance généralisée[27].

Il est à noter que c'est la constatation d'une vulnérabilité « endémique » des objets connectés qui avait poussé la *NSA (National Security Agency) à financer le développement par l'Université d'Alabama* de systèmes de sécurité pour les objets connectés et leurs systèmes de stockage d'informations sur le cloud[28]. Cette préoccupation de sécurité répondait à une double injonction : assurer de manière « défensive » la résilience de l'Internet des objets américain en cas d'attaque ou d'intrusion et probablement aussi veiller à ce que les solutions de sécurité développées par les industriels puissent inclure des

27. *The Internet of Things: Promises and Perils of a Disruptive Technology,* Matej Tonin, Rapporteur Sub-Committee on Technology Trends and Security (NATO Parliamentary Assembly 8 octobre 2017) www.nato-pa.int/document/2017-internet-things-tonin-report-175-stctts-17-e-bis

28. *UAH developing architecture to build design-phase cybersecurity into systems* (The University of Alabama in Huntsville, 6 août 2015) www.uah.edu/news/research/uah-developing-architecture-to-build-design-phase-cybersecurity-into-systems

dispositifs de portes dérobées pour faciliter les travaux d'enquêtes ou de surveillance. Or, comme le rappelle Bruce Schneier[29], une des plus grandes erreurs que pourraient commettre les pays développés serait de créer volontairement des failles de sécurité au sein des objets connectés. En effet ces portes dérobées, si elles devenaient une obligation légale[30], finiraient nécessairement par être découvertes par des hackers malveillants.

Les réglementations sur la sécurité des objets connectés et plus largement le traitement des données issues de ces objets constituent des enjeux cruciaux en termes de protection des libertés mais aussi en termes de confiance pour l'ensemble des acteurs des technologies. Alors que se développent de nouvelles formes de cyberattaques basées sur les objets connectés, le devenir économique de cette filière pourrait dépendre de la capacité des industriels européens à développer des solutions de sécurité qui protégeront à la fois les données issues de ces objets ainsi que leurs utilisateurs. En ce sens, les mesures qui permettront de renforcer la sécurité des objets connectés (depuis la captation d'information par l'objet lui-même jusqu'au traitement à distance de ces informations) pourraient constituer un volet essentiel des politiques industrielles européennes de ce secteur.

Lors de la mise en place de la loi californienne sur la sécurité des objets connectés, Bruce Schneier évoquait la fin d'un chapitre industriel marqué par la négligence des constructeurs en matière de sécurité. Il annonçait aussi l'ouverture d'une ère où les constructeurs de ces objets seraient progressivement contraints d'adopter des comportements plus responsables :

> L'insécurité n'est « rentable » que si vous pouvez vous le permettre dans le monde entier. Lorsque ce n'est plus le cas, vous devriez plutôt faire de nécessité vertu. Ainsi, tous les utilisateurs bénéficieront de la réglementation californienne, et des réglementa-

29. *Data and Goliath* (Bruce Schneier, Ed. Norton & Company 2015)

30. *'Five Eyes' governments call on tech giants to build encryption backdoors - or else* (TechCrunch, septembre 2018) techcrunch.com/2018/09/03/five-eyes-governments-call-on-tech-giants-to-build-encryption-backdoors-or-else/

> tions de sécurité similaires adoptées dans d'autres marchés importants dans le monde, et tous les utilisateurs bénéficieront de la conformité à la partie du *RGPD* qui concerne la sécurité des données. Plus important encore, des lois comme celles-ci stimuleront les innovations en matière de cybersécurité. À l'heure actuelle, nous assistons à une défaillance du marché. Parce que les tribunaux ne tiennent pas les éditeurs de logiciels responsables pour les vulnérabilités de leurs produits, et que les consommateurs n'ont pas l'expertise suffisante pour faire la différence entre un produit sécurisé ou non, les fabricants ont donné la priorité à des prix bas, à la rapidité de mise sur le marché et à des fonctionnalités supplémentaires au détriment de la sécurité[31].

En Europe, parmi les mesures adoptées par le *RGPD*, figurait l'encouragement à la mise en place de codes de conduite[32] et « *des* mécanismes de certification en matière de protection des données ainsi que de labels et de marques »[33]. À l'instar des *étiquettes-énergie* qui permettent de guider le choix des consommateurs en fonction des performances énergétiques des appareils électriques, une certification ou un label de confiance de conformité basé sur le *RGPD* pourraient être créés afin d'informer les citoyens sur le niveau de confidentialité et de sécurité des objets connectés. Les services de la Commission européenne ont dans un premier temps envisagé un dispositif de certification des objets connectés qui disposeraient de technologies d'authentification sécurisée, depuis le matériel jusqu'aux couches réseau[34]. Ce dispositif de certification nécessite de la part des constructeurs une analyse des fonctions de chaque objet ainsi qu'un traitement sécurisé des données. À cette fin, le *Cybersecurity Act*[35] a été définitivement adopté en juin 2019 par l'Union européenne. L'*ENISA*, l'agence de cybersécurité européenne, a ainsi été chargée d'un mandat permanent pour élaborer un cadre de certification pour la sécurité des objets connectés en Europe.

31. *Bruce Schneier, New IoT Security Regulations* (Blog Post novembre 2018) www.schneier.com/blog/archives/2018/11/new_iot_securit.html

32. Art. 40 du RGPD.

33. Art. 42 du RGPD.

34. *Advancing the Internet of Things in Europe (page 31) Commission Staff Working* Document 19 avril 2016 eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:52016SC0110&from-EN

35. *Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité) (Texte présentant de l'intérêt pour l'EEE)* eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX-:32019R0881&from=FR

1.8 La fin de la propriété des objets ?

Un autre type de changement induit par ces objets connectés est lié au fait que leurs fonctionnalités et leur valeur proviennent de leur connexion à des serveurs distants. Si cette connexion aux serveurs distants est suspendue pour des raisons économiques, du fait de la cessation d'activité d'une société, ou technologiques, par l'absence de mise à jour, le fonctionnement de ces objets connectés (et leur utilité même) s'en trouve remis en cause. Les usagers de ces objets peuvent ainsi être « dépossédés » de ces objets sans qu'il soit besoin de les leur reprendre.

L'une des illustrations de ces changements dans la notion même de propriété à l'ère des objets connectés est venue de la société *Amazon*. Ainsi, en 2009, une controverse juridique a opposé la division *Kindle* d'*Amazon* et l'éditeur de l'ouvrage *1984* de George Orwell. Du jour au lendemain, l'ensemble des exemplaires en circulation de l'ouvrage qui décrivait la fin possible des livres dans une société totalitaire furent retirés des *Kindle*. Les usagers se rendant compte alors que des ouvrages dûment payés pouvaient leur être retirés. Les réactions des usagers confrontés à cette « expropriation forcée » furent telles que Bobbie Johnson avançait alors cette explication dans le journal *The Guardian* : « *Pourquoi les gens étaient-ils si outragés ? Les clients n'étaient pas vraiment en colère contre leur gadget ou la légalité des livres en question - ils étaient furieux du tour de passe-passe que leur avait joué Amazon en les retirant secrètement de leurs machines. Ils ont été lésés parce qu'ils pensaient avoir acheté les livres alors qu'en fait, il s'est avéré qu'ils ne faisaient que les louer* »[36].

> **“ Ils ont été lésés parce qu'ils pensaient avoir acheté les livres alors qu'en fait, ils ne faisaient que les louer…**
>
> **Bobbie Johnson**

Face aux controverses générées par ce retrait, et conscient des risques que cette décision faisait peser sur la pérennité de la

36. *Why did Big Brother remove paid-for content from Amazon's Kindles?* (The Guardian, 22 juillet 2009) www.theguardian.com/technology/2009/jul/22/kindle-amazon-digital-rights

plateforme *Kindle*, Jeff Bezos, le patron d'*Amazon*, fut contraint de produire une lettre d'excuses en des termes inhabituels aux utilisateurs de *Kindle* : *« Nous nous excusons pour la façon dont nous avons précédemment traité des copies illégalement vendues de 1984 [...] Notre « solution » à ce problème était stupide, irréfléchie et tristement en contradiction avec nos principes. Nous nous sommes infligés cela à nous-mêmes et nous méritons les critiques que nous avons reçues. Nous utiliserons la cicatrice de cette pénible erreur pour aider à prendre de meilleures décisions à l'avenir, celles qui correspondent à notre mission »*[37].

Dix ans plus tard, c'est *Microsoft* qui est venu rappeler que la propriété des objets connectés, et des services qui leur étaient associés, était toujours aussi peu durable. Lorsque *Microsoft* a fermé sa boutique de livres électroniques en juin 2019, l'ensemble des ouvrages téléchargés sont devenus inaccessibles aux usagers qui là encore les avaient acquis légalement. Dans ce cas, ce n'était pas en raison d'un conflit juridique, mais du fait du verrouillage lié aux technologies de *DRM* (*Digital Rights Management*) mises en place par *Microsoft*. Brian Barret, le directeur du magazine *Wired,* remarquait alors que ces technologies devenaient le bras armé d'une logique d'enfermement des usagers des objets connectés et de leurs contenus autour de quelques grandes plateformes :

> Plus que tout, la disparition des ebooks de Microsoft souligne les dangers cachés du système des *DRM* qui sous-tend la plupart des achats numériques. Initialement conçus comme une mesure antipiratage, les *DRM* fonctionnent désormais essentiellement comme un moyen de verrouiller les clients dans un écosystème, pour éviter qu'ils ne lisent, visualisent ou écoutent leurs achats là où ils le souhaitent. Ce cycle dure depuis plusieurs décennies et ne montre aucun signe de d'essoufflement[38]...

37. *Amazon's Jeff Bezos apologises for Kindle deletions* (The Telegraph, 24 juillet 2009) www.telegraph.co.uk/technology/news/5901667/Amazons-Jeff-Bezos-apologises-for-Kindle-deletions.html

38. *Microsoft's Ebook Apocalypse Shows the Dark Side of DRM. Microsoft has closed its ebook store - and will soon make its customers' libraries disappear along with it.* (Wired, 30 juin 2019) www.wired.com/story/microsoft-ebook-apocalypse-drm/

Une autre forme de « dépossession » des objets connectés est liée à l'absence de mise à jour logicielle. Cette absence de mise en jour, en plus d'augmenter les risques de piratage, peut aussi rendre certains de ces objets inutilisables. Ainsi, plusieurs constructeurs d'objets connectés ont été accusés par leurs utilisateurs de pratiquer de nouvelles formes d'obsolescences programmées. Cela a été le cas du fabricant d'enceintes connectées *Sonos* qui, face aux critiques de ses acheteurs, a été contraint de poursuivre le support technique de ses enceintes[39].

> **“Nous avons moins de droits en tant que locataires de nos appareils numériques que nous n'en avons en tant que locataires d'un bien immobilier… On ne devrait pas laisser la notion de propriété se perdre dans une sorte d'amnésie…**
>
> **Zeynep Tüfekçi**

Il y a deux décennies déjà, Jeremy Rifkin évoquait dans son ouvrage *« L'âge de l'accès »* la fin possible de la propriété individuelle et nous invitait à imaginer à quoi ressemblerait un monde où *« toutes les activités seraient devenues payantes, un monde où les obligations entre individus seraient remplacées par des relations contractuelles, de droits d'entrée, de location ou encore des abonnements… »*[40]. Plus récemment, la sociologue turco-américaine Zeynep Tüfekçi mettait en garde les usagers des objets connectés sur les risques de remise en cause de normes sociales en matière de propriété : *« Nous avons moins de droits en tant que locataires de nos appareils numériques que nous n'en avons en tant que locataires d'un bien immobilier. En effet, l'expulsion d'un bien immobilier y est soumise à une procédure équitable. Si nous achetons quelque chose, cela devrait nous appartenir. On ne devrait pas laisser la notion de propriété se perdre dans une sorte d'amnésie… »*[41].

Protéger la souveraineté numérique européenne correspondra aussi à préserver les principes et valeurs culturelles sur lesquels ont été fondés les pays de l'Union. Au premier rang de ces principes figurent les droits de propriétés. Ces droits revêtent en effet une importante

39. *UK government introduces security rules for 'internet of things'* (Financial Times, 27 janvier 2020) www.ft.com/content/bfc6f2f4-412d-11ea-bdb5-169ba7be433d

40. *The Age of Access: The New Culture of Hypercapitalism, Where all of Life is a Paid-For Experience Jeremy Rifkin* (p. 9 Penguin Publishing 2000)

41. *Zeynep Tufekci: We Are Tenants On Our Own Devices* (Wired, juin 2019) www.wired.com/story/right-to-repair-tenants-on-our-own-devices/

particulière lorsque ces plateformes acquièrent un pouvoir considérable sur la conception, la diffusion ainsi que l'usage des idées et des créations culturelles. Établir un lien de confiance avec les usagers des objets connectés passera par la nécessaire refondation du droit de propriété pour les objets et services connectés. Ainsi, qu'il s'agisse de la durabilité des objets connectés ou de la possibilité de transférer les services ou des informations liées à ces objets, les dispositifs permettant d'assurer leur pérennité devront être mis en place dès leur conception. Sous réserve que ces mesures ne remettent pas en cause la sécurité de ces objets et de leurs usagers, le caractère « propriétaire » des technologies utilisées ne devra pas faire obstacle à la capacité d'utiliser durablement ces objets. À cette fin, il conviendra d'imposer des normes d'interopérabilité et des standards de conception qui assureront la portabilité et la pérennité des contenus et des services liés aux objets connectés. Cette transparence dans le fonctionnement et cette durabilité seront en particulier nécessaires lorsque ces objets seront liés aux activités culturelles, à la santé ou encore à l'éducation.

2

LES PRÉREQUIS À LA MONTÉE EN PUISSANCE DE L'INTERNET DES OBJETS

Afin de pouvoir étendre les technologies de l'Internet des objets à l'ensemble des produits et biens manufacturés, les concepteurs de ces technologies devront être en mesure de répondre à plusieurs types de contraintes. Ces technologies nécessiteront en premier lieu une importante robustesse pour fonctionner dans des environnements technologiques très divers et sous des contraintes de temps importantes. Elles devront aussi permettre une grande capacité de montée en charge *(scalabilité)* et un niveau de sécurité élevé pour éviter les fuites d'informations en particulier pour les informations sensibles mais aussi pour éviter que ces objets ne se retournent contre leurs utilisateurs lors de piratages.

En plus des fonctionnalités offertes par ces nouvelles générations d'objets connectés, la sécurité et la confiance pourraient ainsi devenir des éléments clés dans les choix des utilisateurs vis-à-vis des technologies de l'Internet des objets[42]. D'autres spécificités industrielles pourraient conditionner la « durabilité » des objets connectés. En effet, comme le rappellent les experts de la *Banque mondiale*, ces objets connectés fonctionnent différemment de la plupart des appareils électroniques en particulier lorsqu'ils sont déployés à l'extérieur ou dans l'espace

42. Voir sur ce point les conclusions du groupe de travail mis en place par l'ISOC sur la sécurité des objets connectés (ISOC 7 mars 2020) www.isoc.fr/iot-22-recommandations/

public. Ils doivent ainsi bénéficier de modalités contractuelles spécifiques pour limiter les risques de dysfonctionnements durant le cycle de vie des objets connectés :

> La durée de vie typique de 2 à 4 ans de l'électronique grand public ne convient pas au déploiement à grande échelle de l'IoT. Les coûts et la logistique de mise à jour et de remplacement des éléments d'un système IoT tous les 2 à 4 ans peuvent potentiellement dépasser les bénéfices économiques espérés. Toutes les solutions IoT devraient inclure un *Contrat de Maintenance Annuel (CMA)* qui prendrait en charge les appareils et les services pendant toute leur durée de vie. Ce contrat de maintenance incitera les producteurs à fournir des capteurs capables de résister aux conditions extérieures, en restant calibrés pour fournir des mesures correctes[43].

2.1 Identifiants uniques et interopérabilité logicielle

L'une des clés de voûte de l'interopérabilité des technologies de l'Internet des objets sera aussi liée à l'adoption de systèmes d'identifiants uniques et de protocoles de communication interopérables à l'échelle de l'ensemble des objets connectés. Actuellement, de nombreux systèmes d'identifications correspondent à des systèmes « propriétaires » comme c'est le cas pour les objets connectés des plateformes *iOS*, *Android* ou *Amazon AWS*. Cette interopérabilité des identifiants et des interfaces de programmation (*API*) sera nécessaire pour être en mesure relier des objets issus de « silos » informationnels différents (par exemple des objets dédiés au contrôle environnemental et des objets de santé ou encore des denrées alimentaires...). Pour être intégrées dans les différentes chaînes logistiques et différents environnements technologiques, ces identifiants uniques des objets devront être coordonnés par l'ensemble des acteurs industriels impliqués dans

43. *Internet of Things The New Government To Business Platform a Review of Opportunities, Practices, and Challenges* (World Bank Group 3 novembre 2017) documents1.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf

leur développement et leurs usages, comme c'est le cas aujourd'hui pour les codes des produits *GTIN (Global Trade Item Number)*. Mais, à la différence des codes produits actuels, essentiellement utiles à la logistique, l'objectif de ces nouvelles générations d'identifiants uniques sera de pouvoir suivre et interagir individuellement avec chaque objet depuis sa conception, son assemblage (ou sa production) puis durant l'ensemble de la vie de l'objet connecté jusqu'à son recyclage.

Ainsi, les technologies utilisées à grande échelle pour accéder aux ressources informationnelles sur Internet pourraient constituer l'une des bases de l'interopérabilité des identifiants uniques des objets connectés. C'est le cas du *DNS (Domain Name System),* le système utilisé pour traduire les noms de domaine Internet en adresse IP. Ce système distribué a fait, depuis sa création en 1983, la preuve de sa robustesse. À titre d'exemple, le réseau de diffusion de contenus *Akamai* « résout » quotidiennement plus de 2200 milliards de requêtes *DNS*[44]. Ainsi, dans le cadre des évolutions vers l'Internet des objets, des technologies dérivées du *DNS* comme l'*ONS (Object Naming Service)*[45] ont été envisagées pour accéder aux identifiants uniques des objets[46]. L'*ONS* a fait l'objet de travaux de normalisation[47] menés conjointement par l'*AFNIC* (l'organisation désignée par l'État français pour la gestion des noms de domaine en .fr) *et GS1* (l'organisme international de normalisation des codes produits *GTIN (Global Trade Item Number))*. Dans le prolongement de ses travaux sur l'*ONS*, l'*AFNIC* a aussi participé aux activités de l'*AIOTI* (*Alliance internationale des industriels pour l'innovation dans l'Internet des objets*), dans le domaine de la standardisation des identifiants uniques pour les objets connectés[48].

L'interopérabilité des objets connectés sera aussi liée aux modalités de leur connexion au réseau. De même que l'Internet permet de relier entre eux des ordinateurs, l'Internet des objets devra permettre de relier entre elles des technologies d'identification différentes. Il s'agira en particulier de répondre aux besoins des acteurs de marchés

44. *Learn How Trillions of Dns Requests Help Improve Security* (Akamai Technologies, 2018) blogs.akamai.com/2018/05/learn-how-trillions-of-dns-requests-help-improve-security.html

45. *The Internet of Things - GS1 France & Afnic major contributors to the ONS 2.0* (18 février 2013) www.afnic.fr/en/about-afnic/news/general-news/6703/show/the-internet-of-things-gs1-france-afnic-major-contributors-to-the-ons-2-0.html

46. *Why DNS should be the naming service for Internet of Things?* (Sandoche Balakrichenan – Afnic 2016) ant.isi.edu/events/dinr2016/P/p72.pdf

47. *GS1 ONS Version 2.0.1 Ratified Standard* (Issue 2, 31 janvier 2013) www.gs1.org/gsmp/kc/epcglobal/ons/ons_2_0_1-standard-20130131.pdf

48. *Identifiers in Internet of Things (IoT) Version 1.0*, février 2018 AIOTI WG03 – IoT Standardisation aioti.eu/wp-content/uploads/2018/03/AIOTI-Identifiers_in_IoT-1_0.pdf.pdf

industriels qui utilisent des technologies conçues pour répondre à des besoins ou des métiers spécifiques. Ainsi, le suivi des objets connectés nécessitera que soient mises en place des technologies d'itinérance (*roaming*) afin de permettre une communication continue avec ces objets et ce quel que soit leur environnement. Là encore, les technologies du *DNS* pourraient constituer l'une des solutions à la montée en puissance du suivi des objets[49].

2.2 Des étiquettes RFID sur l'ensemble des produits ?

L'une des technologies clés pour l'identification des objets correspond aux puces à radiofréquence ou puces *RFID (Radio-Frequency IDentification).* Ces puces représentent l'une des plus anciennes technologies de l'Internet des objets. En effet, le principe de ces puces a été imaginé en 1948 par le scientifique et inventeur Harry Stockman[50]. Dans les premiers temps, ces puces ont été utilisées pour des applications liées à la logistique militaire. Ces puces *RFID* permettent en effet d'assigner un identifiant à un objet et sont, pour les plus simples d'entre elles, dotées d'un processeur rudimentaire et d'une antenne. Cette antenne permet l'activation du processeur via une brève impulsion électromagnétique. Leur fonction est alors de répondre à cette impulsion en déclinant la série de chiffres codée sur leur processeur. Le prix unitaire de puces *RFID* les plus simples est de quelques centimes d'euros et elles ne contiennent ni source d'énergie interne qui pourrait s'épuiser, ni pièces mobiles qui pourraient s'user, ce qui les rend particulièrement durables.

Des puces *RFID* pourraient ainsi être utilisées pour remplacer les systèmes d'identification optique des produits manufacturés (code-barres, QR code, Datamatrix...). En effet, l'identifiant présent sur le code-barres est utile aux acteurs de la logistique et dans une moindre mesure à l'acheteur (pour établir des comparaisons de prix ou recueillir des informations sur la composition d'un produit).

49. Voir sur ce point les travaux menés par la *Wireless Broadband Alliance* autour de l'initiative *OpenRoaming* wballiance.com/openroaming

50. *"Communication by Means of Reflected Power"* Harry Stockman (Proceedings of the IRE, vol. 36, no. 10, pp. 1196-1204, octobre 1948) simson.net/ref/1948/stockman.pdf

Les puces *RFID* pourraient offrir la possibilité de mettre en place des services au-delà du point de vente. Les produits dotés de puces pourraient par exemple transmettre des informations à un appareil électroménager : d'un produit alimentaire à un réfrigérateur, ou encore d'un vêtement à un lave-linge… Ces puces pourraient aussi servir à informer les usagers sur les événements qui se produisent durant la vie d'un objet. Ainsi, le fabricant de pneus *Michelin* a expérimenté l'intégration de puces *RFID* qui permettent d'identifier les pneumatiques (chaque pneu disposant de son propre numéro d'identification) et de prendre connaissance de certains paramètres comme sa date de montage, son usure, sa pression, sa température[51]…

Pour la plupart, les puces *RFID* ne contiennent ni mécanismes de désactivation, ni mécanismes de chiffrement ou dispositifs de sécurité. Intégrer ces mécanismes pour protéger ces puces contre des interrogations issues d'utilisateurs indélicats (*skimming*) ou chiffrer leurs communications représente encore un surcoût significatif. Ces dispositifs de sécurité pourraient par exemple éviter qu'une donnée sensible issue d'un produit médical ne puisse être captée frauduleusement. Mais ce surcoût lié à la sécurité ne pourra être assumé par les producteurs ou distributeurs de ces objets (et *in fine* par les consommateurs) que s'il correspond à un service valorisable durant l'ensemble de la vie d'un objet (de sa conception jusqu'à son recyclage). Ces puces *RFID* pourraient alors devenir un maillon essentiel des services de l'Internet des objets.

L'adjonction de fonctions connectées sur des appareils électroniques « intelligents » s'avère déjà rentable. Mais le prix des capteurs ou des dispositifs d'identification *RFID* constitue encore un frein à la montée en puissance de l'Internet des objets jusqu'ici « stupides » (denrées alimentaires, vêtements, produits manufacturés, etc.). Si l'intégration de dispositifs de désactivation/réactivation ou des systèmes de sécurité cryptographique devenait une obligation légale, les constructeurs

51. Michelin dévoile la technologie RFID issue de la compétition sur le pneu Michelin Sport Cup 2 (4Legend, 26 septembre 2017) www.4legend.com/2017/iaa-2017-michelin-devoile-la-technologie-rfid-issue-de-la-competition-sur-le-pneu-michelin-sport-cup-2/

d'objets connectés pourraient ainsi être confrontés à un « effet de ciseau » lié au surcoût des capteurs connectés et des puces *RFID*.

En 2018, *Decathlon,* première chaîne de distribution mondiale de matériel sportif, a choisi d'étendre la pose de puces *RFID* à la quasi-totalité de ses articles[52]. Pour *Decathlon*, l'équation économique de la *RFID* était différente des acteurs traditionnels de la grande distribution. En effet, 80 % des produits vendus par l'enseigne sportive sont issus de ses propres marques[53] et permettent donc à la pose de puces *RFID* d'être intégrée verticalement dans le processus de production et de distribution. De plus, le prix moyen des articles sportifs étant plus élevé, l'impact du coût unitaire des puces ne constituait pas un obstacle majeur. Ainsi, le tarif unitaire des étiquettes *RFID* encodées s'établissait entre 5 et 10 centimes d'euros. À titre de comparaison, une étiquette antivol *EAS* coûte entre 2 et 3 centimes d'euros[54]. Pour des produits alimentaires de prix unitaires beaucoup plus réduits, ce surcoût reste encore trop élevé pour les acteurs de la distribution. Initialement choisies pour améliorer la visibilité des flux logistiques, les puces *RFID* peuvent aussi être utilisées pour améliorer l'expérience utilisateur dans les boutiques de l'enseigne sportive (par exemple pour connaître l'état des stocks)[55].

Le basculement vers l'étiquetage individuel des produits alimentaires correspondra au développement de nouvelles générations de services en lien avec d'autres objets ou produits connectés. Pour répondre à des objectifs environnementaux, d'autres pistes sont désormais envisagées pour identifier grâce à des puces *RFID* des emballages réutilisables pour les produits alimentaires. Ces identifiants uniques liés aux emballages pourraient par la suite être associés à un produit ou une denrée lors du passage en caisse. De nouveaux services à haute valeur ajoutée pourraient ainsi être créés pour connaître la disponibilité des produits au domicile de l'usager ou savoir s'ils sont consommables[56]. Des travaux de R&D visent aussi à créer des micro-capteurs

52. *Decathlon aura 100 % de produits étiquetés en RFID en juin* (Revue du Digital, 20 mars 2018) www.larevuedudigital.com/decathlon-atteindra-100-de-produits-etiquetes-rfid-en-juin/

53. *Decathlon : Le bilan financier 2018 et les perspectives pour 2019* (SportBuzzBusiness, 25 février 2019) www.sportbuzzbusiness.fr/decathlon-le-bilan-financier-2018-et-les-perspectives-pour-2019.html

54. *La RFID révolutionne les magasins Decathlon* (LSA-Conso, 13 janvier 2016) www.lsa-conso.fr/la-rfid-revolutionne-les-magasins-decathlon,228999

55. *The rise, fall and return of RFID* (Supply Chain Dive, 21août 2018) www.supplychaindive.com/news/RFID-rise-fall-and-return-retail/530608/

56. *IoT is about to tell you when your food is spoiled* (Network World, 22 août 2017) www.networkworld.com/article/3218120/internet-of-things/iot-is-about-to-tell-you-when-your-food-is-spoiled.html

biodégradables qui permettront de vérifier que des produits alimentaires n'ont pas subi de rupture de la chaîne de froid[57].

2.2.1 Supermarchés « Amazon Go » : le pari de l'intelligence artificielle

D'autres technologies peuvent aussi être utilisées pour identifier les produits dans les magasins. Ainsi, plutôt que de placer des puces *RFID* sur les produits, la société *Amazon* a choisi d'autres options technologiques pour développer ses supermarchés « sans caisse ». Pour analyser les mouvements des clients et savoir quels produits ils achetaient, *Amazon* a développé une combinaison de technologies basées sur l'intelligence artificielle *(Deep Learning,Object Detection,Sensor Fusion,Computer Vision*) pour l'analyse en temps réel des images issues de multiples caméras et capteurs associés à des systèmes de détection d'objets[58]. Les technologies employées par *Amazon* avaient ici pour but de simplifier l'expérience des utilisateurs dans les boutiques elles-mêmes mais pas de créer un continuum pour développer des services liés aux objets au-delà du point de vente. En plus d'équiper ses propres boutiques avec ces dispositifs, l'objectif d'*Amazon* est de diffuser cette technologie auprès de l'ensemble des grandes chaînes de distribution « physique ». Cependant, pour Devin Coldewey, l'un des premiers journalistes à avoir expérimenté le supermarché *Amazon Go* à Seattle, la question de l'acceptabilité sociale et politique de ces technologies se pose : *« Sur un plan philosophique, je suis évidemment troublé. Un supermarché dont vous sortez sans vous arrêter en caisse pourrait n'être que le masque de l'usage la plus controversé des technologies : la surveillance ubiquitaire des individus… »*[59].

> **“ Un supermarché dont vous sortez sans vous arrêter en caisse pourrait n'être que le masque de l'usage la plus controversé des technologies : la surveillance ubiquitaire des individus…**
>
> **Devin Coldewey**

57. *Biodegradable microsensors: the link between food products and the Internet of Things?* (ETH Zürich, septembre 2017) www.youtube.com/watch?v=S9ZiXGnadno

58. *How the Amazon Go Store's AI Works* (Medium, Towards Data Science 7 juin 2019) towardsdatascience.com/how-the-amazon-go-store-works-a-deep-dive-3fde9d9939e9

59. *Inside Amazon's surveillance-powered no-checkout convenience store* (TechCrunch, 22 janvier 2018) techcrunch.com/2018/01/21/inside-amazons-surveillance-powered-no-checkout-convenience-store

2.3 Vers un « *Droit au Silence des Puces* »

De nouvelles fonctionnalités devront être prévues dès la conception de ces objets pour que les « citoyens-usagers » puissent maîtriser les flux de données échangées par leurs objets connectés. Ainsi, la désactivation temporaire ou définitive des objets connectés devra être possible et ce d'autant plus que ces échanges d'informations seront possibles sans que les usagers en soient informés. Ainsi, dans son rapport sur les liens entre administrations et Internet des objets, la *Banque mondiale* préconise que les législations mises en place à l'avenir prennent en compte ces nouvelles dimensions technologiques liées à la protection des données personnelles :

> Pour garantir la sécurité et la confidentialité des données, il est important d'établir des normes réglementaires tournées vers l'avenir. La plupart des solutions actuelles à ces problèmes reposent sur des processus de calcul et de mémoire de haut niveau qui ont tendance à être limités dans les dispositifs de l'Internet des objets. Une prise en charge matérielle importante, telle que le chiffrement, l'authentification et l'attestation, et une prise en charge logicielle, telle que les architectures auto-réparatrices en temps réel, sont nécessaires pour les futurs dispositifs de l'Internet des objets. Il est essentiel de veiller à ce que seuls les utilisateurs autorisés pourront accéder aux données et à ce que les systèmes soient développés en suivant des processus et des normes et qu'ils soient contrôlés afin de s'assurer que des acteurs malveillants ne pourront pas exploiter ces technologies pour accéder aux données ou les endommager, en particulier lorsque les systèmes de l'Internet des objets se répercuteront sur le monde physique[60].

Or, s'il est relativement simple de désactiver un objet électronique élaboré, comme un smartphone, il en va tout autrement lorsqu'il s'agit d'une puce *RFID* utilisée pour « taguer » un objet industriel ou une

60. *Internet of Things The New Government To Business Platform a Review of Opportunities, Practices, and Challenges* (World Bank Group 3 novembre 2017) http://documents1.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf

denrée alimentaire. Ainsi, le principe du «*Droit au Silence des Puces*» a été élaboré en 2006[61] dans le but de permettre aux usagers de maîtriser les informations issues des puces *RFID*. Il implique en particulier que dès leur conception soient inclus des dispositifs de désactivation/réactivation associé à des systèmes de chiffrement dans le cas d'objets porteurs de données sensibles, en particulier pour les données médicales ou les données relatives à la sécurité des personnes.

Le droit au silence des puces a été officiellement évoqué en mai 2008 lors de la première réunion ministérielle européenne sur l'Internet des Objets[62], puis repris par la Commission européenne[63, 64] et le Parlement européen[65]. Ce droit est également a été évoqué par le Conseil d'État dans son rapport de 2014 « *Le numérique et les droits fondamentaux »*[66] comme l'une des pistes de réflexion pour l'avenir de l'Internet des objets. Cependant, il n'a pas encore fait l'objet de mise en œuvre législative en Europe. Parmi les réserves émises par les industriels figurent des inquiétudes sur la modification de l'équilibre économique que ces dispositifs pourraient engendrer. Cependant, les conflits autour de la dissémination non contrôlée des données personnelles rendent désormais plus probable la perspective d'une législation de ce type[67]. Si les fabricants de puces *RFID* étaient légalement contraints d'intégrer de nouveaux dispositifs de sécurité ainsi que des mécanismes de désactivation/réactivation, cela entraînera nécessairement un surcoût. Se posera donc ici la question d'un arbitrage entre le développement de nouvelles filières industrielles et la nécessaire protection des données personnelles des citoyens européens. Or, la progression des risques liés à la sécurité des objets connectés et la prise en compte par les usagers de nouveaux risques sur leurs données personnelles pourraient modifier les conditions de cet arbitrage. Cela d'autant plus qu'à terme les objets connectés via des puces *RFID* pourraient surpasser en nombre l'ensemble des autres types d'objets connectés.

61. Dans le texte *Architecture et Gouvernance de l'Internet* (Bernard Benhamou, Revue Esprit mai 2006).www.netgouvernance.org/ArchitectureEsprit.pdf (version anglaise www.netgouvernance.org/esprit-eng.pdf voir aussi *« Les Mutations Économiques, Sociales et Politique de l'Internet des Objets »* (Bernard Benhamou, Cahiers de la Documentation Française, janvier 2013). www.netgouvernance.org/IOT 20Cahiers 20DOC 20FRANCAISE.PDF

62. *« Internet des objets, Internet du futur »* conférence ministérielle européenne organisée dans le cadre de la *Présidence Française de l'Union Européenne* (Nice 2008).

63. E*urope prepares for the internet revolution* (European Action Plan, 18 juin 2009) europa.eu/rapid/press-release_IP-09-952_en.htm

64. *Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification* (12 mai 2009) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=6496

65. *Motion For A European Parliament Resolution On The Internet Of Things* (Committee on Industry, Research and Energy, Rapporteur: Maria Badia i Cutchet, 10 mai 2010) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2010-0154+0+DOC+PDF+V0//EN

66. *Le numérique et les droits fondamentaux* (Étude annuelle du Conseil d'État, septembre 2014) www.vie-publique.fr/sites/default/files/rapport/pdf/144000541.pdf

67. *The "silence of the chips" concept : towards an ethics (-by-design) for IoT*, Caroline Rizza & Laura Draetta. International Review of Information Ethics. vol. 22. 10.29173/irie125 (2015) www.researchgate.net/publication/282029896_The_silence_of_the_chips_concept_towards_an_ethics_-by-design_for_IoT/citation/download

2.4 Des objets et capteurs autonomes en énergie

Un autre enjeu majeur pour le déploiement de l'Internet des objets sera lié à l'autonomie énergétique des capteurs. Cette autonomie représente un enjeu stratégique tant d'un point de vue environnemental qu'industriel pour les fabricants d'objets connectés. En effet, si les puces *RFID* les plus simples ne disposent pas de source d'énergie interne, tous les capteurs actifs nécessitent des batteries qui constituent une limitation importante en termes de durée de vie mais aussi en termes de coût lors de leur remplacement. Ainsi, de nombreux industriels européens établissent des programmes de recherche sur le principe de la récolte d'énergie ambiante (*energy harvesting)*. Cela permet aux capteurs de se recharger à partir des variations physiques de leur environnement. Cette « moisson » d'énergie peut utiliser les vibrations de l'objet, les variations thermiques, lumineuses ou encore l'énergie issue d'autres ondes électromagnétiques :

> Pour tirer plus encore les tarifs vers le bas, le laboratoire R&D de l'entreprise *Sigfox* essaie de résoudre l'une des principales problématiques du secteur : le changement de batterie qui, même s'il n'a lieu qu'une fois tous les dix ans en moyenne pour les appareils fonctionnant avec le réseau *Sigfox*, reste coûteux. Les chercheurs de l'entreprise travaillent sur des technologies d'« *energy harvesting* ». Les appareils dotés de ce type d'équipements sont capables de capter de l'énergie dans leur environnement immédiat et donc (si les recherches aboutissent) de devenir 100% autonomes. *Sigfox* a par ailleurs annoncé pour 2020 des modules de connectivité radio commercialisés à 0,2 dollar, puis, à terme, à 0.02 dollar[68].

Dans un domaine voisin, le constructeur automobile *Peugeot* a expérimenté à Paris l'usage de panneaux de capteurs piézoélectriques qui transforment en électricité les vibrations issues du bruit de la circulation urbaine afin de recharger des véhicules électriques[69]. Un autre

68. *Sigfox : abonnement, couverture, concurrents...* (Journal du Net 9 octobre 2020) www.journaldunet.fr/web-tech/dictionnaire-de-l-iot/1195953-sigfox-abonnement-couverture-concurrents-20200704/

69. *New Peugeot 208 - Recycle the Noise, Silence the City* (Peugeot, 12 novembre 2019) www.youtube.com/watch?v=6_lVGiokmNM

exemple d'*energy harvesting* dans les objets du quotidien est celui des microturbines présentes dans les pommeaux de douche de la société *Hydrao*[70]. Ses capteurs sont alimentés par le flux d'eau et ils permettent d'informer l'usager sur le volume d'eau utilisé.

70. *Un pommeau anti-douche froide pour l'environnement* (Électricité de France, 2017) www.edf.fr/edf/accueil-magazine/un-pommeau-anti-douche-froide-pour-l-environnement

3

INTERNET DES OBJETS ET RECONFIGURATION DU PAYSAGE INDUSTRIEL

Les technologies de l'Internet ont permis à des sociétés comme les *GAFAM (Google, Amazon, Facebook, Apple, Microsoft)* ou encore les *NATU (Netflix, Airbnb, Tesla, Uber*) ou leurs équivalents chinois *BATX (Baidu, Alibaba, Tencent, Xiaomi)* d'investir des secteurs qui leur étaient initialement étrangers. Ces sociétés sont désormais sur le point de devenir des acteurs majeurs de la finance, des transports, de la santé, des médias ou encore du tourisme… Les technologies et les services de l'Internet des objets, par leur capacité à intégrer des informations sur les processus industriels ainsi que sur les individus et leur environnement, pourraient constituer un nouveau levier pour décloisonner des filières industrielles et à terme accélérer la reconfiguration de segments entiers de l'économie des pays développés.

Un exemple de cette intervention des objets connectés dans le champ industriel est lié aux nouveaux objets connectés liés à la maîtrise de l'énergie. En effet, l'optimisation par les usagers de la consommation d'énergie est devenue en l'espace de quelques années l'un des secteurs clés pour l'Internet des objets. Le marché mondial des thermostats connectés représente selon le rapport de *Allied Market Research*, 1,36 milliard de dollars en 2018 et devrait atteindre 8,78 milliards de dollars d'ici à 2026[71]. Parmi eux, les thermostats intelligents de la

71. *Smart Thermostat Market to Reach $8.78 Billion, Globally, by 2026 at 26.0% CAGR, Says Allied Market Research* (Bloomberg, 11 décembre 2019) www.bloomberg.com/press-releases/2019-12-11/smart-thermostat-market-to-reach-8-78-billion-globally-by-2026-at-26-0-cagr-says-allied-market-research

société *Nest (*filiale de *Google)* se sont déjà vendus à plus 11 millions d'exemplaires dans le monde[72]. Grâce à un ensemble de capteurs ainsi qu'à un logiciel qui analyse les habitudes de l'usager, ils ajustent automatiquement la température de la maison pour lui permettre de faire des économies d'énergie. Ces thermostats représentent ainsi des outils permettant d'améliorer la gestion de la consommation à l'échelle d'un quartier ou même d'une ville. Ils permettent ainsi de lisser la consommation et ainsi de diminuer le « pic » de consommation entre 18 et 20 heures. En effet, ce sont les dépenses nécessaires à soutenir la charge de ces pics de consommation électrique qui génèrent les plus importantes dépenses d'infrastructure pour les fournisseurs et distributeurs d'énergie. Plusieurs fournisseurs d'énergie aux États-Unis (comme la société texane *Reliant*) ont décidé d'offrir ces thermostats connectés à leurs abonnés[73]. Parce qu'ils permettent à la fois d'acquérir une connaissance plus fine des habitudes des usagers et un contrôle de leur consommation, ces thermostats connectés initialement perçus comme des produits *B2C* (*Business to Consumer*) sont devenus l'un des leviers de l'optimisation des activités de la production et de la distribution d'énergie.

3.1 Rapprochement entre automobile et santé connectée

Les automobiles figurent déjà parmi les objets connectés les plus richement dotés en capteurs (radar, sonar, caméras, accéléromètres, thermomètres, détecteurs d'humidité, etc.). Ces capteurs sont désormais coordonnés par une informatique embarquée de plus en plus puissante dont les fonctions sont souvent gérées par d'autres sociétés que les constructeurs automobiles eux-mêmes. Ce qui faisait dire à Dieter Zetsche, le PDG de *Mercedes-Benz,* qu'une voiture serait bientôt « *un smartphone avec quatre roues autour… »*[74]. À titre d'exemple, le volume d'information généré par les capteurs embarqués dans la

72. *Nest says it has sold over 11 million devices since 2011* (CNET 7 février 2018) www.cnet.com/news/nest-says-it-has-sold-over-11-million-devices-since-2011/

73. *In the world of Texas electricity, free is not always free* (Dallas Morning News, 12 octobre 2013) www.dallasnews.com/news/watchdog/2013/10/13/in-the-world-of-texas-electricity-free-is-not-always-free/

74. *Detroit Motor Show: Car firms take on the tech giants* (BBC News, 13 janvier 2015) www.bbc.com/news/business-30786709

voiture connectée *Ford Fusion* représentait déjà en 2012, 25 gigaoctets de données par heure de conduite[75]. Désormais, avec le développement des voitures sans pilotes, ce sont des téraoctets de données qui seront traitées par les capteurs des véhicules[76]. Si, dans leur majorité, ces capteurs sont dédiés à l'analyse des paramètres de fonctionnement du véhicule, d'autres sont spécifiquement destinés à analyser les paramètres physiologiques du conducteur ou son style de conduite. Ces capteurs pourraient au-delà de l'évaluation du niveau de vigilance, devenir une source d'information précieuse, notamment sur l'état de santé du conducteur. L'analyse de la conduite par des dispositifs connectés a d'ailleurs donné lieu à des expérimentations par des groupes d'assurance afin de moduler les primes (principe du « *Pay How You Drive* »). Il est à noter que jusqu'ici ces expérimentations ont souvent été jugées trop intrusives par les assurés potentiels[77].

Depuis plusieurs années, des constructeurs automobiles expérimentent l'intégration de capteurs connectés pour recueillir les paramètres physiologiques du conducteur d'un véhicule. La société *Ford* a ainsi envisagé d'intégrer des capteurs pour le suivi des pathologies cardio-respiratoires ou encore les troubles de la vigilance[78]. L'autre versant des technologies de prévention et de suivi des pathologies est lié aux utilisations non médicales de ces données. En se rapprochant ainsi de chacune des réactions intimes de leurs usagers, les objets connectés peuvent aussi donner naissance à des toutes nouvelles formes de manipulations basées sur l'analyse biologique et comportementale. Ce que l'historien Yuval Harari résumait en ces termes :

> Il est important de se rappeler que colère, joie, ennui et amour sont aussi des phénomènes biologiques comme la fièvre ou la toux. La technologie qui identifie la toux pourrait également identifier les rires. Si entreprises et gouvernements commencent à collecter nos données biométriques en masse, ils pourraient

75. *Ford Issues Predictions for Next Wave of Automotive Electronics Innovation* (Washington Times, 27 décembre 2012) www.washingtontimes.com/news/2012/dec/27/ford-predicts-next-auto-electronics-innovation/

76. *Les nouveaux défis de la cartographie routière pour les voitures autonomes* (Le Monde, 10 mars 2017) www.lemonde.fr/pixels/article/2017/03/12/les-nouveaux-defis-de-la-cartographie-routiere-pour-les-voitures-autonomes_5093246_4408996.html

77. *Assurances auto : êtes-vous prêt à tout dévoiler pour payer moins cher ?* (L'Express, 2 février 2016) votreargent.lexpress.fr/high-tech/assurances-auto-etes-vous-pret-a-tout-devoiler-pour-payer-moins-cher_1759408.html

78. *3 Ways Ford Cars Could Monitor Your Health. Ford is experimenting with car features that could help drivers with diabetes, heart problems, and more* (IEEE Spectrum, 19 mai 2017) spectrum.ieee.org/the-human-os/biomedical/diagnostics/3-ways-ford-cars-could-monitor-your-health

mieux nous connaître que nous ne nous connaissons nous-mêmes, et ils pourraient non seulement prédire nos sentiments mais aussi les manipuler et nous vendre tout ce qu'ils veulent, qu'il s'agisse d'un produit ou d'un politicien… La surveillance biométrique ferait ressembler le piratage de données de *Cambridge Analytica* à des outils de l'âge de pierre[79]…

3.2 De l'automobile individuelle… au « robotaxi » partagé ?

Dans le domaine industriel, les technologies de l'Internet des objets associées aux systèmes d'intelligence artificielle pourraient induire d'autres modifications radicales dans les modèles économiques existants. Ces nouvelles formes de « rationalisation » économiques constituent le fil rouge des transformations industrielles du secteur automobile. Ainsi, le développement des voitures sans pilotes pourrait à terme correspondre à la diminution du nombre d'automobiles vendues et pour certains experts elle pourrait même signer la fin de la propriété individuelle des véhicules[80]. Ainsi, les transports utilitaires seraient assurés par des voitures autonomes et partagées et la propriété individuelle des véhicules pourrait être réservée à des segments de voitures « loisirs ». Ainsi, pour Andreas Tschiesner, le responsable du secteur automobile chez *McKinsey,* les flottes de voitures autonomes qu'il nomme « robotaxis » pourraient modifier la structure des revenus des constructeurs (cf. évolution de la structure des revenus des constructeurs automobiles (source *McKinsey* via *Financial Times*[81])). Les constructeurs se transformeraient alors en fournisseurs de services de transports : « *En moyenne, les constructeurs automobiles gagnent 2000 dollars sur la vente d'un véhicule. Sur la durée de vie du véhicule, cela ne représente que 0,01 dollar par kilomètre, alors que pour les « robotaxis », le potentiel de gain est de 20 à 25 cents par kilomètre, cela constitue un levier considérable pour*

79. *Yuval Noah Harari: the world after coronavirus* (Financial Times 20 mars 2020) www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75?segmentid=acee4131-99c2-09d3-a635-873e61754ec6

80. *Could Self-Driving Cars Spell the End of Ownership?* (Wall Street Journal, 1 décembre 2015) www.wsj.com/articles/could-self-driving-cars-spell-the-end-of-ownership-1448986572

81. *Race to build a million-mile car becomes a reality* (Financial Times, 13 janvier 2018) www.ft.com/content/1255be4c-f680-11e7-88f7-5465a6ce1a00

accroître les gains des constructeurs… »[82]. L'intérêt des constructeurs correspondrait alors à augmenter le nombre de trajets effectués durant la vie d'un véhicule et plus à favoriser le renouvellement rapide de leurs véhicules.

Pour les constructeurs de véhicules (et de véhicules autonomes), au-delà des fonctions de transports une nouvelle source de services à valeur ajoutée sera liée aux services de loisirs et d'information à bord des véhicules *(in-car infotainment)*. Ainsi, les groupes de communications et les sociétés de production cinématographiques[83] investissent déjà pour développer de nouveaux formats pour les films, les jeux et les contenus d'information spécifiquement conçus pour les véhicules autonomes. Pour le cabinet *Allied Market Research*, le marché de l'information et des loisirs à bord des véhicules pourrait s'élever à 21 milliards de dollars en 2026[84].

3.3 Internet des objets et urbanisme : de nouveaux enjeux politiques

La mise en œuvre des flottes de voitures sans pilote pourrait aussi avoir des conséquences sur l'organisation des zones urbaines et périurbaines. Ainsi, en permettant de repousser les zones de parking à la périphérie des villes (pour la recharge et la maintenance des véhicules), ces technologies pourraient modifier la part de zones constructibles au sein des espaces urbains. Mais la conception des algorithmes qui assureront le fonctionnement de ces flottes pourraient générer de nouvelles formes de discriminations géographiques pour les utilisateurs et créer des défis nouveaux pour les régulateurs de ces technologies. Ainsi, dans son enquête sur la voiture sans pilote, *The Economist* établit un parallèle entre ces nouvelles formes de discriminations algorithmiques et celles plus anciennes basées sur l'architecture des villes :

82. *Robotaxis: can automakers catch up with Google in driverless cars?* (Financial Times 31 janvier 2019) www.ft.com/content/dc111194-2313-11e9-b329-c7e6ceb5ffdf

83. *Why Hollywood Could Make Billions From Self-Driving Cars* (Hollywood Reporter 28 août 2017) www.hollywoodreporter.com/behind-screen/why-driving-cars-could-be-hollywoods-next-big-thing-1031554

84. *In-Car Infotainment Market by Installation Type and Component Global Opportunity Analysis and Industry Forecast, 2019–2026* (Allied Market Research, janvier 2020) www.alliedmarketresearch.com/in-car-infotainment-market

> Les voitures autonomes enregistreront tout ce qui se passe dans et autour d'elles. Lorsqu'un crime sera commis, la police demandera aux voitures voisines ce qu'elles ont « vu ». (.....) Si, pour des raisons de sécurité, les conducteurs humains devaient être progressivement interdits, la liberté de mouvement des passagers pourrait s'en trouver limitée. En effet, l'absence de desserte de certaines destinations, pourrait créer de nouvelles formes de discriminations. Si tout cela semble peu plausible, rappelez-vous que l'architecte Robert Moses avait conçu la voie reliant New York à Long Island, avec des ponts trop bas pour favoriser l'accès des riches blancs en voiture, tout en discriminant les noirs pauvres dans les bus. En Chine déjà, le système de « crédit social » qui note les citoyens en fonction de leur comportement, limite déjà les voyages en train et en avion à ceux qui dévient du « droit chemin »[85]...

Contrairement aux modifications architecturales de nos villes, les discriminations créées en modifiant les technologies ou les services des objets connectés pourraient dans un premier temps être invisibles pour les citoyens.

“ Rendre visibles par les citoyens les risques de dérives des technologies déployées dans l'espace urbain constituera aussi un objectif stratégique pour les responsables publics...

De nouvelles questions seront liées à l'usage qui sera fait des données recueillies par les objets et véhicules connectés. Ainsi, le *Washington Post* évoquait le mode « *sentinelle* » des voitures connectées *Tesla* qui permet à la police américaine de recueillir les images des caméras en cas d'accidents ou d'infractions qui surviennent à proximité du véhicule[86]. L'automobile connectée devenant alors l'œil des autorités dans le cadre d'enquêtes de police.

Rendre visibles par les citoyens les risques de dérives des technologies déployées dans l'espace urbain constituera aussi un objectif stratégique pour les responsables publics. Ce travail pourra prendre là encore la

85. *Self-driving cars offer huge benefits - but have a dark side* (The Economist, 1 mars 2018) www.economist.com/leaders/2018/03/01/self-driving-cars-offer-huge-benefits-but-have-a-dark-side

86. *My car was in a hit-and-run. Then I learned it recorded the whole thing* (Washington Post, 27 février 2020) www.washingtonpost.com/technology/2020/02/27/tesla-sentry-mode/

forme de mesures d'éducation, de sensibilisation et de régulation de ces technologies. Des débats et des consultations démocratiques devront aussi être mis en place afin que les citoyens puissent être associés en amont à l'élaboration de ces technologies.

3.4 Des risques de déclassement 4.0 ?

Les risques sociaux engendrés par la combinaison des technologies d'intelligence artificielle et de l'Internet des objets deviennent désormais des éléments de décision importants pour l'ensemble des acteurs industriels impliqués. En effet, pour les employés des secteurs visés par les transformations, la synergie entre Internet des objets et intelligence artificielle pourrait induire des transformations de leur cœur de métier voire leur suppression. C'est par exemple le cas, dans le domaine des transports avec l'arrivée des véhicules autonomes. Ainsi pour John Samuelsen, le président du syndicat américain des travailleurs du transport (TWU) qui fédère près de 150 000 travailleurs qui, en majorité, sont chargés du transport de passagers, ces technologies représentent des risques sociaux importants :

> « *Les véhicules autonomes sont une très mauvaise idée pour le transport*. » En septembre 2018, Samuelsen s'est rendu à Columbus pour mener personnellement une manifestation contre les expérimentations de navettes autonomes de la ville. L'impact de la technologie des véhicules autonomes sur le travail de ses membres est une préoccupation majeure pour Samuelsen. Les promoteurs des véhicules autonomes affirment que les véhicules de transport en commun sans conducteur auront besoin de travailleurs pour collecter les tarifs, répondre aux questions et résoudre les problèmes de sécurité, comme le harcèlement des passagers. Mais Samuelsen déclare que cette affirmation passe à côté de l'essentiel : «*Même si les emplois de chauffeur de bus étaient*

> *remplacés par des préposés, ils ne gagneraient jamais un salaire équivalent*». Il affirme que les techniciens des transports autonomes « *vont prendre la richesse des quartiers ouvriers d'Amérique pour l'amener à Wall Street et à la Silicon Valley…* »[87].

Pour Kai-Fu Lee, les conséquences éthiques et sociales de l'introduction de ces technologies commencent déjà à avoir un impact sur les décideurs et en particulier sur les élus : « *Ces casse-tête moraux pourraient bien inciter les élus américains – toujours influencés par les groupes d'intérêt et la menace de publicité négative – à freiner le processus. Les premiers signes sont là : en 2017, grâce à leurs efforts de lobbying auprès du Congrès américain, des syndicats de chauffeurs routiers ont réussi à exclure les poids lourds de la législation visant à accélérer la généralisation des véhicules autonomes* »[88].

3.5 Villes intelligentes : le contre-exemple de Google à Toronto

Pour les acteurs industriels de l'Internet des objets, les technologies et les services des villes intelligentes constituent parmi les plus importants débouchés en termes de marchés. Les technologies de l'Internet des objets participent en effet à la mise en œuvre de l'ensemble des politiques publiques à l'échelle locale ; depuis l'organisation des transports, le contrôle des grands réseaux d'infrastructures, la sécurité sanitaire, la maîtrise de l'énergie ou encore le contrôle environnemental. La gouvernance des projets de villes intelligentes est désormais un enjeu stratégique et politique pour les acteurs publics comme pour les citoyens.

Cependant, ces projets peuvent aussi donner lieu à des dérives lorsque les acteurs publics ne sont pas en mesure de contrôler les orientations stratégiques des sociétés à qui ils concèdent ces marchés de villes intelligentes. Cela a été le cas avec la ville de Toronto lorsqu'elle a confié

87. *A Move for Driverless Mass Transit Hits Speed Bumps* (Wired, 18 août 2020) www.wired.com/story/driverless-mass-transit-hits-speed-bumps/

88. *AI Superpowers: China, Silicon Valley, and the New World Order* (Kai-Fu Lee, HMH Books 2018)

à une filiale de Google *(Sidewalk Labs)* le soin d'organiser les fonctions et les services de ville intelligente du quartier *Waterfront*. Les observateurs ont progressivement noté d'étranges et dérangeantes similarités entre le projet de ville intelligente de *Google* et les orientations du « *Crédit social* » chinois : notation des « bons » comportements et sanctions pour les autres. En particulier pour les citoyens qui refusent la « transparence » et ne communiquent pas leurs informations personnelles. Le journal canadien *Globe* & *Mail* a ainsi obtenu les documents préparatoires à ce projet qui décrivaient comment la filiale de Google comptait *« percevoir ses propres taxes, suivre et prédire les mouvements des personnes et contrôler certains services publics. [...] Cette expérience serait en partie basée sur la quantité de données que les usagers accepteront de partager, et qui pourraient finalement servir à récompenser les gens pour « bon comportement... »*[89]. Il est à noter que c'est l'intervention des citoyens de Toronto, relayée par une intense campagne de presse[90], qui a remis en question l'existence même de cette initiative. Ainsi, en mai 2020, la filiale de *Google* annonçait qu'elle abandonnait définitivement son projet *Waterfront* à Toronto[91].

“ Les observateurs ont progressivement noté d'étranges et dérangeantes similarités entre le projet de ville intelligente de *Google* et les orientations du « *Crédit social* » chinois...

3.6 Les enjeux de l'acceptabilité sociale de l'Internet des objets

L'acceptabilité sociale des innovations technologiques de l'Internet des objets est devenue un facteur crucial pour l'ensemble des acteurs industriels. En effet, la « rétribution » que constitue l'échange de données personnelles en contrepartie d'un service « gratuit » semble de moins en moins satisfaisante pour les citoyens. À mesure que les citoyens sont informés des risques de dérives liées au piratage de leurs

89. *Sidewalk Labs document reveals company's early vision for data collection, tax powers, criminal justice* (Globe & Mail, 30 octobre 2019) www.theglobeandmail.com/business/article-sidewalk-labs-document-reveals-companys-early-plans-for-data/

90. *Google wants to run cities without being elected. Don't let it* (The Guardian, 24 octobre 2017) www.theguardian.com/commentisfree/2017/oct/24/google-alphabet-sidewalk-labs-toronto

91. *Why we're no longer pursuing the Quayside project - and what's next for Sidewalk Labs* (Daniel L. Doctoroff, Medium, 7 mai 2020) medium.com/sidewalk-talk/why-were-no-longer-pursuing-the-quayside-project-and-what-s-next-for-sidewalk-labs-9a61de3fee3a

données ou des risques de surveillance généralisée, de nouvelles réticences se font jour. On note ainsi une grande variabilité des réponses des usagers face aux sollicitations des plateformes de l'Internet pour obtenir leurs données personnelles. Comme l'enquête de la banque *Morgan Stanley* le notait, ce degré d'acceptation varie en fonction du pays et des origines culturelles des personnes interrogées :

> Les limites de la tolérance du public à l'égard de ces pratiques d'incitation et de « maternage » ne sont pas encore claires. «*Il y a certainement un moment où l'on passe de l'utile à l'effrayant*», déclare John Hocking responsable de la branche assurance de *Morgan Stanley*. Il a réalisé des enquêtes pour demander aux gens quelle réduction de prix ils souhaiteraient obtenir pour accepter de partager leurs données. Les personnes interrogées en Asie étaient les plus disposées à confier leurs données contre une réduction de prix. Les Occidentaux étaient moins enthousiastes, et les Allemands étaient les plus méfiants de tous...[92]

Si les opinions publiques deviennent désormais critiques vis-à-vis des risques sociaux et politiques de l'Internet des objets, cette exigence de lucidité pourrait amener les concepteurs des prochaines générations de technologies à intégrer dès l'amont ces préoccupations plutôt que de risquer des scandales à répétition comme ceux auxquels on a pu assister ces dernières années depuis les révélations d'Edward Snowden et plus récemment avec le scandale *Cambridge Analytica*. Pour *The Economist,* en aidant à « déminer » en amont les principaux risques liés à l'Internet des objets, cette vigilance accrue pourrait paradoxalement assurer aux technologies de l'Internet des objets une plus grande pérennité :

> Les Big Tech sont désormais accusés de tous les maux, depuis la toxicomanie des enfants jusqu'à l'incitation au terrorisme, ils

92. The Internet of Things (The Economist Technology Quarterly, septembre 2019)

ont perdu leur lustre utopique. Cette désillusion s'étend aux prédictions les plus sombres concernant l'Internet des objets. En un sens, c'est précieux, car plus les problèmes peuvent être prévus, plus ils peuvent être évités facilement. Mais si le techno-optimisme qui a imprégné les années 1990 et 2000 apparaît aujourd'hui comme naïf, le techno-pessimisme qui est à la mode aujourd'hui est peut-être tout aussi exagéré. Tout comme l'internet d'origine, l'Internet des objets promet des bénéfices considérables. Contrairement à l'internet d'origine, l'Internet des objets arrivera à maturité à une époque devenue sceptique quant à l'avenir d'un monde connecté et numérisé. S'il doit se battre pour conquérir la confiance de ses utilisateurs, sur le long terme cela ne sera que mieux pour l'Internet des objets[93].

93. Ibid.

4

LES NOUVEAUX ENJEUX DE LA RÉGULATION DE L'INTERNET DES OBJETS

4.1 États et Internet des objets : synergie ou « ubérisation » ?

Les technologies de l'Internet ont progressivement épousé les formes et les contours des États à mesure que leurs fonctions essentielles nécessitaient l'usage du réseau. En ce sens, les instruments fondamentaux de la souveraineté sont déjà indiscernables des outils de la puissance technologique. L'Internet des objets, dont les technologies participeront à un nombre croissant d'activités dans le secteur public, pourrait accélérer encore ce phénomène. Le défaut de maîtrise des technologies de l'Internet des objets par les acteurs publics pourrait encore augmenter leur situation de dépendance vis-à-vis des acteurs numériques.

> **“Les instruments fondamentaux de la souveraineté sont déjà indiscernables des outils de la puissance technologique…**

Déjà en 2011, Eric Schmidt alors patron de *Google* évoquait lors de son audition devant la commission antitrust du Sénat américain les propos d'Andy Grove l'ancien PDG d'Intel : « *Les entreprises de haute technologie fonctionnent 3 fois plus vite que les entreprises traditionnelles.*

Et le gouvernement fonctionne trois fois moins vite que les entreprises traditionnelles. Nous avons donc un écart d'un facteur 9 avec les gouvernements… »[94]. Plus tard, en 2013, Eric Schmidt confirmait dans son livre *The New Digital Age*[95], que pour lui les États étaient devenus trop lents et inefficaces pour faire face à la rapidité des évolutions technologiques.

Désormais, au-delà de l'ubérisation de secteurs économiques entiers, ce sont les fonctions régaliennes des États qui peuvent être « privatisées » par l'introduction des technologies d'intelligence artificielle et de Big Data. Cette logique d'analyse Big Data a permis à *Palantir*, la société fondée par Peter Thiel et financée à son origine par *In-Q-Tel* le fonds d'investissement de la CIA, d'équiper la quasi-totalité des services de renseignement américains en particulier pour la lutte anti-terroriste. En France, la récente reconduction du contrat passé par la *DGSI* avec la société *Palantir*[96], a souligné les risques de dépendance politique liés à notre dépendance technologique. Et cela d'autant plus que la société *Palantir* a été associée au scandale *Cambridge Analytica*[97] et que son fondateur, proche de Donald Trump, a été membre de son comité de transition à la présidence des États-Unis.

Il est à noter, que lorsque les États ont perçu des menaces sur leurs prérogatives régaliennes « traditionnelles », ils ont fait preuve d'une réactivité incomparable à celle qu'ils déploient dans le domaine de la régulation de la concurrence et en particulier des lois antitrust. Ainsi, lorsque *Facebook* a annoncé son projet de cryptomonnaie « *Libra* », les autorités européennes et américaines ont immédiatement fait part de leur volonté de réguler voire d'interdire cette initiative[98]. En plus de constituer un nouveau canal de collecte des données personnelles, cette monnaie aurait pu à terme concurrencer les monnaies souveraines, faciliter le blanchiment ou rendre intraçable le financement du terrorisme. Ainsi, en l'espace de quelques semaines, les principaux partenaires du projet (*Visa, MasterCard, eBay, PayPal*) ont renoncé à coopérer avec *Facebook* de crainte de s'aliéner leurs

94. *Google's Eric Schmidt Expounds on His Senate Testimony* (Washington Post, 30 Sep 2011) www.washingtonpost.com/national/on-leadership/googles-eric-schmidt-expounds-on-his-senate-testimony/2011/09/30/gIQAPyVgCL_story.html

95. *The New Digital Age: Transforming Nations, Businesses, and Our Lives* par Eric Schmidt et Jared Cohen (Ed. John Murray 2014)

96. *La société américaine Palantir, proche de la CIA, est toujours indispensable aux espions français* (Le Monde, 29 novembre 2019) www.lemonde.fr/economie/article/2019/11/29/l-americain-palantir-est-toujours-indispensable-aux-espions-francais_6021016_3234.html

97. *Palantir, l'embarrassant poisson-pilote du big data* (Le Monde, 9 octobre 2018) www.lemonde.fr/pixels/article/2018/10/09/palantir-l-embarrassant-poisson-pilote-du-big-data_5366568_4408996.html

98. *Facebook Unveils Cryptocurrency Libra in Bid to Reshape Finance* (Wall Street Journal, 18 juin 2019) www.wsj.com/articles/facebook-unveils-crypto-wallet-based-on-currency-libra-11560850141

interlocuteurs gouvernementaux. *Facebook* qui, après le scandale *Cambridge Analytica,* voyait en *Libra* un moyen de diversifier ses activités dans un secteur stratégique a ainsi été contraint de réduire ses ambitions. À l'inverse, lorsque l'Union européenne a infligé en mars 2019 une amende de 1,49 milliard d'euros contre *Google* pour abus de position dominante, cette sanction est intervenue après de nombreuses années d'enquête (certains des faits reprochés à *Google* remontaient à 2006). De plus, ces sanctions économiques n'ont jusqu'ici démontré qu'un impact limité sur l'activité de la société.

Il conviendra de veiller à ce que les technologies utilisées par la France (et plus largement par les États européens) soient maîtrisées et qu'elles concourent bien à l'intérêt général. Il conviendrait de créer à cet effet une fonction de coordinateur des technologies de l'État à l'instar du « *Chief Technology Officer* » *(CTO)* de l'administration fédérale mise en place aux États-Unis. Ce coordinateur national aurait en particulier pour fonction de veiller à ce que l'ensemble des technologies mises en place par l'État soient à la fois maîtrisées par les agents de l'État, qu'elles soient durables et qu'elles ne pourront donner lieu à des utilisations contraires à l'intérêt des citoyens. Afin que ce coordinateur des technologies de l'État puisse exercer pleinement sa mission interministérielle, il serait souhaitable que cette fonction soit directement rattachée au Premier ministre et qu'il dispose en propre d'une équipe d'experts afin de pouvoir analyser les dossiers qu'il aura à traiter à la fois sous l'angle technologique, économique, industriel et social.

4.2 Santé et Internet des objets : vers des solutions liberticides ?

Avant même la pandémie de *Covid-19*, de nombreux scientifiques avaient évoqué la possibilité d'intégrer des réseaux de capteurs et des systèmes d'intelligence artificielle pour effectuer la détection

précoce des épidémies. Désormais, l'urgence de la pandémie rend plus probable encore le déploiement de technologies de l'Internet des objets pour aider à maîtriser les menaces biologiques. Qu'il s'agisse d'objets connectés *wearables* (casques, bagues, lunettes ou bracelets dotés de capteurs), des drones pour l'imagerie thermique ou encore de réseaux de capteurs urbains[99]. Les technologies de l'Internet des objets qui peuvent être mises à contribution dans ce domaine se diversifient à mesure que se développent de nouvelles méthodes d'analyses basées sur l'intelligence artificielle. Ces algorithmes peuvent en effet révéler (ou déduire) des éléments sur l'état de santé d'une personne à partir d'informations en apparence anodines. Ainsi, lorsque l'on analyse dans la durée les déplacements d'une personne, on peut anticiper la survenue possible de troubles cardiaques ou circulatoires. *Facebook* a ainsi développé des brevets portant sur l'analyse en continu des déplacements de ses utilisateurs[100]. Plusieurs sociétés travaillent aussi à la détection des signes précoces liés à l'infection de *Covid-19* par l'analyse du rythme cardiaque et de l'activité des porteurs de montres connectées[101]. Récemment, des équipes de recherche du *MIT*[102] et de l'*École Polytechnique Fédérale de Lausanne (EPFL)*[103] ont annoncé qu'elles développaient des algorithmes d'intelligence artificielle qui permettent la détection des personnes porteuses du coronavirus à partir de l'analyse du son d'une toux forcée via le micro des smartphones. Ces systèmes de détection précoce du *Covid-19* conçus à partir de l'analyse de plusieurs dizaines de milliers d'enregistrements, permettraient de découvrir des variations sonores inaudibles pour l'oreille humaine chez les personnes atteintes par le virus y compris pour des personnes asymptomatiques.

Dans un autre registre, en Chine, plusieurs entreprises expérimentent déjà des casques dotés de capteurs cérébraux qui analysent les ondes cérébrales de leurs employés afin de détecter le stress, la colère ou l'endormissement[104]. Récemment, *Amazon* a lancé une nouvelle génération

99. *Internet of Things for Current COVID-19 and Future Pandemics : An Exploratory Study by* M. Nasajpour, S. Pouriyeh, M. Parizi, M. Dorodchi, M. Valero, H. Arabnia Dept of Information Technology and Dept of Software Engineering and Game Development, Kennesaw State University, Department of Computer Science, University of North Carolina and University of Georgia (article submitted on 22 juillet 2020) arxiv.org/pdf/2007.11147.pdf

100. *What 7 Creepy Patents Reveal about Facebook* (New York Times, 21 Juin 2018) nytimes.com/interactive/2018/06/21/opinion/sunday/facebook-patents-privacy.html

101. *Could You Have Covid-19? Soon Your Smartwatch or Smart Ring Might Tell You* (Wall Street Journal, 28 juillet 2020) www.wsj.com/articles/could-you-have-covid-19-soon-your-smartwatch-or-smart-ring-might-tell-you-11595949072

102. *Artificial intelligence model detects asymptomatic Covid-19 infections through cellphone-recorded coughs Results might provide a convenient screening tool for people who may not suspect they are infected.* (MIT News Office 29 octobre 2020) news.mit.edu/2020/covid-19-cough-cellphone-detection-1029

103. *Des applis mobiles pour dépister le covid par la toux* (Le Temps, 10 nov 2020) www.letemps.ch/sciences/applis-mobiles-depister-covid-toux

104. *En Chine, des capteurs cérébraux pour surveiller les émotions des employés* (Slate, 1er Mai 2018) www.slate.fr/story/161173/en-chine-des-capteurs-cerebraux-pour-surveiller-les-emotions-des-employes

de bracelets *Halo* dotés de capteurs dédiés à l'analyse de l'état émotionnel et des paramètres physiologiques de leurs porteurs[105]. Plus récemment encore, la nouvelle version de l'*Apple Watch* devrait permettre la détection du niveau de stress et la prévention des crises de panique. Cette fonction correspondra à l'analyse combinée de la saturation en oxygène du sang, la fréquence cardiaque et respiratoire ainsi que d'autres paramètres comme les mouvements ou la localisation de l'utilisateur[106].

Là encore, ce sont les mesures prises pour assurer la sécurité des données recueillies par ces capteurs qui détermineront si ces capteurs s'inscrivent dans une trajectoire de prévention, de contrôle ou de manipulation des individus. En effet, comme le notent plusieurs auteurs, la limite entre prévention des conduites à risque et conditionnement des utilisateurs via les objets connectés reste délicate à fixer. Cette tendance au contrôle des populations pourrait en effet marquer le passage de l'ingénierie sociale… au contrôle social assisté par l'Internet des objets.

À l'extrême, pour le cabinet d'étude *Frost* & *Sullivan*, la réponse la plus « efficiente » en termes de lutte contre les pandémies consisterait à établir un réseau mondial de capteurs. Ce réseau de capteurs permettrait de détecter de manière précoce les menaces biologiques où qu'elles apparaissent dans le monde. Cependant, comme le soulignent les auteurs, cette proposition qui correspondrait à l'une des plus importantes opportunités de marchés technologiques jamais conçus pour l'Internet des objets, se heurterait nécessairement à l'opposition des opinions publiques du fait de son caractère liberticide :

> La solution la plus simple serait de permettre aux entreprises, aux villes et aux gouvernements de créer collectivement un vaste réseau mondial de capteurs pour détecter les virus. Cependant, cela nécessiterait une planification et une mise en œuvre à l'échelle mondiale qui s'attaquerait aux fondements mêmes

105. *Amazon Amazon Announces Halo, a Fitness Band and App that Scans Your Body and Voice* (The Verge, 27 août 2020) www.theverge.com/2020/8/27/21402493/amazon-halo-band-health-fitness-body-scan-tone-emotion-activity-sleep

106. *Apple Watch may soon be able to detect panic attacks before they happen* (SlashGear, 10 mai 2020) www.slashgear.com/apple-watch-may-soon-be-able-to-detect-panic-attacks-before-they-happen-10619926

> de la démocratie et exigerait des gouvernements qu'ils placent les besoins de la planète devant les besoins de leurs citoyens. La solution la plus logique est souvent la plus difficile à mettre en œuvre. Le degré de planification nécessaire pour mettre en œuvre cette solution en ferait l'une des réalisations les plus importantes de l'histoire de l'humanité [...] et à long terme cela représente le « *Saint Graal* » des opportunités de marché pour l'Internet des objets[107].

Ainsi, la fascination pour la « techno-efficience » de certains acteurs technologiques de l'Internet des objets rappelle le « *solutionnisme technologique* » évoqué par Evgeny Morozov dans son ouvrage « *Pour tout résoudre cliquez ici* »[108]. Cette fascination est encore plus présente lorsqu'il est question de l'Internet des objets dans le domaine de la santé. Cette tendance n'est pas uniquement le fait de régimes autoritaires, mais bien d'acteurs économiques ou de gouvernements qui évaluent le rapport bénéfice/risque de ces technologies et considèrent que démocratie et protection des libertés peuvent devenir des variables d'ajustement...

4.3 Assurance santé et Internet des objets : du traitement à la prévention

La captation et le traitement des données de santé sont ainsi devenus des enjeux stratégiques pour les acteurs des technologies. Les dispositifs de santé connectée et en particulier les technologies du suivi et de la prévention des pathologies deviennent le nouveau terrain d'expansion pour les industriels des technologies. En effet, grâce à de nouvelles générations d'objets médicaux connectés capables de suivre en continu les activités et les paramètres physiologiques des usagers, il devient possible de mettre en place à moindre coût des systèmes de prévention et de suivi personnalisés. Ces objets connectés qui accompagneront les usagers au quotidien devraient

107. *The Next Generation of IoT – Addressing the Coronavirus and Preventing Future Outbreaks* (Frost & Sullivan, 31 janvier 2020) ww2.frost.com/frost-perspectives/the-next-generation-of-iot-addressing-the-coronavirus-and-preventing-future-outbreaks/

108. *Pour tout résoudre cliquez ici - l'aberration du solutionnisme technologique* (Evgeny Morozov, Ed. Fyp 2014)

permettre le diagnostic précoce de pathologies chroniques (cancer, diabète, asthme, maladies cardio-vasculaires…). Ils devraient aussi permettre de modifier les comportements de leurs utilisateurs pour maîtriser les facteurs de risques comme la sédentarité ou l'obésité.

D'autres secteurs clés des économies européennes pourraient ainsi être transformés par l'arrivée de nouvelles générations de services de l'Internet des objets ; ceux de la santé et de l'assurance. Les acteurs technologiques pourraient en effet prendre pied dans le secteur prudentiel (banques et assurances) et déplacer le centre de gravité de l'économie de la santé vers la prévention. Voir sur ce point le rapport 2015 de *Goldman Sachs*[109] sur la santé connectée qui estime à 305 milliards de dollars les économies qui seront induites aux États-Unis par l'introduction des technologies de l'Internet des objets dans le domaine de la santé. Parmi ces économies, 200 milliards de dollars seraient liés à l'amélioration de la prévention et la gestion des pathologies chroniques, en particulier les maladies cardio-vasculaires, l'asthme et le diabète. Ces économies représenteraient aux États-Unis près de 10 % du total des dépenses de santé (soit 3600 milliards de dollars en 2018)[110].

Cette même dynamique de prévention des risques, était déjà présente dans la proposition de loi *HR1313* introduite en 2017 au Congrès américain. L'objectif affiché de cette proposition de loi était, grâce à des tests génétiques réalisé à grande échelle en entreprise, de développer des mesures de prévention et de détection précoce des maladies. Cette loi prévoyait de déployer ces tests génétiques dans les entreprises américaines et d'imposer des pénalités de 4 000 à 5 000 dollars par an à l'encontre des employés qui refuseraient de se soumettre à ce « screening génétique »[111].

L'un des enjeux pour la puissance publique en France et en Europe sera de veiller à ce que les évolutions de l'Internet des objets ne remettent pas en cause notre modèle social au profit d'une logique de

109. *The Digital Revolution comes to US Healthcare* (Goldman Sachs Equity Research 2015) www.anderson.ucla.edu/Documents/areas/adm/acis/library/DigitalRevolutionGS.pdf

110. *National Health Expenditures 2018* (U.S. Centers for Medicare & Medicaid Services 2019) www.cms.gov/files/document/highlights.pdf

111. *Employees who decline genetic testing could face penalties under proposed bill* (Washington Post, 11 mars 2017) www.washingtonpost.com/news/to-your-health/wp/2017/03/11/employees-who-decline-genetic-testing-could-face-penalities-under-proposed-bill/

contrôle systématisé des individus. Et ce d'autant plus que seront bientôt intégrées à ces plateformes des données issues de la génomique. Désormais, la protection de notre modèle de protection sociale relève de la souveraineté numérique. La mise en place d'une logique d'hyper-individualisation de la couverture santé irait à l'encontre de notre modèle social fondé sur la solidarité et la mutualisation des risques au niveau de la société tout entière. Or, les objets connectés dédiés à la santé permettent déjà aux grandes plateformes de compléter leurs informations sur les utilisateurs pour affiner leurs profils. Cela permet d'effectuer, comme jamais auparavant, une évaluation précise du risque santé pour chaque individu. Ainsi, comme le précise M. Demurger, directeur général de la *MAIF* : *« C'est un renversement complet du monde de l'assurance. Traditionnellement, les assureurs avaient très peu de données sur leurs clients mais un grand nombre de clients. Grâce au big data, nous pouvons désormais récolter un grand nombre de données comportementales sur une seule personne »* [112].

Ainsi, le secteur de l'assurance santé devient l'une des cibles prioritaires des grands acteurs des technologies. Plutôt que devenir directement des acteurs du soin, secteur qui nécessite en effet des investissements importants et aléatoires sur le long terme, les grandes plateformes de l'Internet peuvent désormais utiliser les données accumulées sur leurs usagers pour fournir des services de prévention des pathologies. Grâce à des capteurs connectés associés à des systèmes d'intelligence artificielle, ces données leur permettront de modéliser de manière précise les risques liés à la santé de chaque individu et ainsi optimiser les profits de leurs services d'assurances. Ainsi, *Google* (via *Alphabet*) vient d'annoncer qu'elle se lançait dans le secteur de l'assurance santé avec *Coefficient* sa nouvelle division : *« Alphabet passe une étape supplémentaire dans le domaine de la santé en se lançant dans l'assurance. Verily, sa division dédiée qui développe et commercialise des objets connectés dans ce secteur, lance une nouvelle filiale, baptisée Coefficient Insurance Company.*

112. *Santé : faut-il faire payer les assurés en fonction de leur mode de vie ?* (Le Monde, 6 septembre 2016) www.lemonde.fr/economie/article/2016/09/06/assurance-votre-vie-privee-vaut-bien-une-ristourne_4993378_3234.html

Cette dernière va s'appuyer sur le big data et des outils analytiques pour proposer des assurances de santé à des entreprises »[113].

Dans ce domaine, la création par le ministère de la Santé d'une plateforme de données de santé (*Health Data Hub*) conçue pour devenir un guichet unique d'accès à l'ensemble des données de santé préfigure les évolutions de la santé connectée. En effet, cette plateforme vise à développer de nouveaux services d'intelligence artificielle appliquée à la santé. Cependant, comme l'ont fait remarquer des professionnels de santé ainsi que des spécialistes de l'informatique médicale, l'hébergement de ce dispositif par la société *Microsoft*[114] constituait à la fois un risque en termes de souveraineté sur des données sensibles et une opportunité manquée pour développer des savoir-faire essentiels dans l'écosystème français de la santé connectée[115]. Face aux controverses liées aux choix de la société *Microsoft*, le gouvernement a récemment annoncé qu'il comptait désormais rapatrier l'hébergement vers des sociétés françaises ou européennes[116]. Dans le même temps, la *CNIL* a pris acte de la décision de la Cour de justice de l'Union européenne qui avait annulé le *Privacy Shield* permettant à des sociétés américaines de transférer les données personnelles des Européens aux États-Unis. La CNIL a ainsi estimé que *« Le changement de la solution d'hébergement du Health Data Hub et des autres entrepôts de santé hébergés par les sociétés soumises au droit étasunien devrait intervenir dans un délai aussi bref que possible »*[117]. Cet avis de la *CNIL* correspond à une reconnaissance de fait des principes de localisation des données (*data localisation /data residency*) en particulier pour les données sensibles. S'il devait être codifié au sein d'une directive européenne, ce principe constituerait une rupture profonde avec les principes sur lesquels ont été fondés les activités et les modèles économiques des principaux acteurs de l'Internet.

113. *Verily (Alphabet) se lance dans l'assurance avec sa nouvelle division, Coefficient* (L'Usine Digitale, 25 août 2020) www.usine-digitale.fr/article/verily-alphabet-se-lance-dans-l-assurance-avec-sa-nouvelle-division-coefficient.N996864

114. *« L'exploitation de données de santé sur une plate-forme de Microsoft expose à des risques multiples »* (tribune parue dans Le Monde du 10 décembre 2019) www.lemonde.fr/idees/article/2019/12/10/l-exploitation-de-donnees-de-sante-sur-une-plate-forme-de-microsoft-expose-a-des-risques-multiples_6022274_3232.html

115. *Health Data Hub : « Le choix de Microsoft, un contresens industriel ! » (interview Bernard Benhamou* Le Point, 18 Juin 2020) www.lepoint.fr/technologie/health-data-hub-le-choix-de-microsoft-et-un-contresens-industriel-10-06-2020-2379394_58.php

116. *Microsoft doit se retirer du Health Data Hub, d'après la Cnil* (L'Usine Digitale 9 octobre 2020) www.usine-digitale.fr/article/microsoft-doit-se-retirer-du-health-data-hub-d-apres-la-cnil.N1014634

117. *La Cnil réclame l'arrêt de l'hébergement des données de santé des Français par Microsoft* (L'Obs, 9 octobre 2020) www.nouvelobs.com/high-tech/20201009.OBS34527/la-cnil-reclame-l-arret-de-l-hebergement-des-donnees-de-sante-des-francais-par-microsoft.html

4.4 Data brokers : un modèle économique « toxique » ?

La collecte en masse des données personnelles constitue désormais un sujet politique pour l'ensemble des régulateurs européens. Ainsi, une activité moins connue, celle des data brokers ou « *courtiers en données* », commence à être examinée par les régulateurs tant aux États-Unis qu'en Europe où leurs activités pourraient être jugées contraires au règlement général sur la protection des données. En effet ces data brokers agrègent des données personnelles issues de nombreuses sources différentes et consolident des profils d'utilisateurs qui pour les importants d'entre eux se comptent en centaines de millions. Ces profils peuvent compter dans certains cas jusqu'à plusieurs *dizaines de milliers de paramètres par individus*. Ces profils sont ensuite revendus à des banques, des assureurs, des chaînes de distribution, à des gouvernements ou mêmes à d'autres data brokers pour consolider leurs bases de profils. Il est à noter que c'est à l'issue du scandale *Cambridge Analytica* que la société *Facebook* a annoncé qu'elle renonçait à faire appel aux data brokers pour compléter ses offres publicitaires[118].

> **« La Commission européenne prévoit qu'en 2020 le marché des données en Europe pourrait être estimé à 106,8 milliards d'euros…**

Les data brokers dont les activités sont quasiment inconnues du grand public occupent une place stratégique dans l'économie des grandes plateformes de l'Internet. La Commission européenne prévoit ainsi qu'en 2020 le marché des données en Europe pourrait être estimé à 106,8 milliards d'euros[119]. Les objets connectés constituent désormais l'une des sources majeures pour la collecte des données des data brokers. Ainsi, l'analyse des données de géolocalisation des personnes peut à elle seule aider à constituer des profils, médicaux, religieux, sportifs ou encore politiques des individus.

118. *Facebook ends data broker partnerships in blow to targeted ads* (VentureBeat, 28 mars 2018) venturebeat.com/2018/03/28/facebook-ends-data-broker-partnerships-in-blow-to-targeted-ads/

119. *Data brokers: regulators try to rein in the 'privacy deathstars'* (Financial Times, 9 janvier 2019) www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521

La récente annulation de l'accord transatlantique *Privacy Shield*, après l'annulation de son prédécesseur le *Safe Harbor* en 2015, rend plus incertaine encore la pérennité du modèle économique des data brokers. En effet, du fait même de leur modèle économique, ces sociétés constituent un facteur de risque de diffusion incontrôlée des informations qu'elles peuvent détenir sur les utilisateurs de l'Internet.

4.4.1 Une impossible régulation des Data brokers ?

Le *RGPD* a commencé à contraindre les data brokers à intégrer une dimension éthique dans leurs activités. Ainsi, John Mitchison, le responsable de la politique et de la conformité à la *Data* & *Marketing Association* (l'organisme professionnel des entreprises des données) évoque l'impact qu'a eu le *RGPD* sur l'organisation des activités des data brokers en Europe :

> Lorsque le *RGPD* est entré en vigueur, les acteurs de ce secteur ont été forcés de regarder la législation et ont compris que les technologies qu'ils utilisaient étaient juste à la frontière et à la limite de la [loi] existante. L'une des choses les plus radicales que j'ai constatées est que toutes ces entreprises ont drastiquement réduit le nombre d'entreprises tierces dont elles acceptent des données. Il faut maintenant des preuves que les données ont été collectées de manière appropriée, ils ont ainsi éliminé de nombreux fournisseurs qui ne respectaient pas ces normes.[120]

Dans son rapport sur les data brokers, rédigé avant le scandale *Cambridge Analytica*, la *FTC (Federal Trade Commission)* américaine s'inquiétait déjà de l'étendue des informations que ces sociétés détiennent sur les individus ainsi que sur leurs capacités considérables de « déduction » sur les comportements des individus :

120. *Data brokers: regulators try to rein in the 'privacy deathstars'* (Financial Times, 9 janvier 2019) www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521

> Les courtiers en données combinent et analysent les données sur les consommateurs pour en tirer des conclusions sur eux, y compris des conclusions potentiellement sensibles : Les courtiers en données déduisent les intérêts des consommateurs à partir des données qu'ils collectent. Ils utilisent ces intérêts, ainsi que d'autres informations, pour classer les consommateurs par catégories. Certaines catégories peuvent sembler anodines comme « propriétaire de chien », « passionné de « sports d'hivers » ou « répond aux courriers ». Les catégories potentiellement sensibles comprennent celles qui se concentrent principalement sur l'ethnicité et les niveaux de revenus, comme « *Urban Scramble* » et « *Mobile Mixers* », qui comprennent toutes deux une forte proportion de Latinos et d'Afro-Américains à faibles revenus[121].

4.4.2 Une plus grande transparence et une meilleure visibilité pour les data brokers

Les data brokers bénéficient jusqu'ici de l'opacité dans laquelle ils effectuent leur travail d'agrégation des profils d'utilisateurs. Ainsi, au-delà du consentement des usagers pour la transmission de leurs données personnelles, il serait désormais utile que soient affichées l'ensemble des structures auxquelles seront transmises les informations collectées. Ainsi la *FTC* proposait que soit créé un dispositif centralisé pour permettre aux usagers de choisir ou non de transmettre leurs données personnelles :

> Étant donné l'état d'invisibilité actuelle des data brokers, une question persiste : si un mécanisme centralisé d'accès et d'effacement devait être mis à la disposition des consommateurs, comment pourraient-ils en être informés ? Une façon pour la loi d'accroître la visibilité du secteur des data brokers et de leurs outils d'accès et d'effacement serait d'exiger que les sources qui entrent en contact avec les consommateurs les informent

121. *Data Brokers: A Call for Transparency and Accountability* (Federal Trade Commission report, mai 2014) www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

> de manière visible qu'ils partagent leurs données avec les data brokers et leur donnent la possibilité de refuser de partager leurs informations avec ces mêmes data brokers.[122]

Des dispositions de ce type ont depuis été mises en œuvre en Europe dans le cadre du *RGPD*, cependant, comme le fait remarquer Antoine Dubus, chercheur à *l'Institut Mines-Télécom*, cette démarche de transparence ne suffit pas à réduire les risques pour les utilisateurs :

> Contrairement à ce que l'on pourrait penser de prime abord, nos premiers résultats font apparaître un risque d'intensification de collecte et de vente de données personnelles par les data brokers, lié à l'application des nouvelles obligations définies par le *RGPD*. En effet, le respect des obligations légales augmente leur coût de collecte des données personnelles. Dès lors, les data brokers vont chercher à optimiser leur bénéfice soit en reportant leur activité de collecte sur des données plus rentables, soit sur d'autres consommateurs initialement non ciblés. Nos résultats suggèrent également que les entreprises achetant les services des data brokers font face à un dilemme du prisonnier. Dans le cas des courtiers en données, ce principe se caractérise de la façon suivante : les entreprises augmenteraient leurs profits si aucune d'entre elles n'avait recours aux services d'un data broker. Toutefois, une entreprise n'a pas intérêt à être la seule à ne pas traiter avec les data brokers car ses concurrents se trouveraient alors en situation de position dominante. Notre analyse économique suggère donc que les autorités de protection pourraient aider les entreprises à sortir de ce dilemme du prisonnier en proposant par exemple des marques de confiance, certifiant qu'un organisme ne recourt pas à des services basés sur l'utilisation des données personnelles relatives à ses clients à leur insu. Cela contribuerait à réduire le nombre de données personnelles collectées par les data brokers[123].

122. *Ibid*.

123. *Les effets du RGPD sur la collecte et la monétisation des données personnelles* (Chaire Valeurs et Politiques des Informations Personnelles - Institut Mines-Télécom, 10 mai 2019) cvpip.wp.imt.fr/2019/05/10/les-effets-du-rgpd-sur-la-collecte-et-la-monetisation-des-donnees-personnelles/

4.4.3 Régulation européenne des données : les perspectives du *Data Governance Act*

Au-delà du règlement général sur la protection des données (*RGPD*), les nouvelles activités liées au marché européen des données nécessitaient que soient mises en œuvre de nouvelles formes d'encadrement des acteurs de ce secteur. Ainsi, en lançant le *Data Governance Act*[123], la Commission européenne a souhaité mettre un terme aux incertitudes juridiques et technologiques qui prévalaient dans le domaine du commerce des données. Il s'agissait d'établir un contrôle sur l'activité des data brokers en particulier pour les données industrielles issues de l'Internet des objets, les données personnelles et aussi les données issues du secteur public.

En effet, les data brokers du fait de l'absence de régulations spécifiques ont contribué à la dissémination des données personnelles ainsi qu'au développement d'utilisations non souhaitées de ces données. Du fait de leur modèle économique ces sociétés ont aussi participé à la concentration des données autour des seules grandes plateformes de l'Internet. Ainsi, comme l'a noté la vice-présidente exécutive de la Commission, Margrethe Vestager, lors du lancement du Data Governance Act : *« Il s'agit d'un modèle alternatif à la gestion des données par les big tech…»*[124].

Les nouveaux acteurs européens de ce partage ou « *intermédiaires de données* » devront en effet fonctionner strictement comme des intermédiaires neutres dont l'activité consistera à relier détenteurs et utilisateurs des données. Des limites nouvelles étant imposées aux acteurs de ce partage des données. Ainsi, pour éviter la revente et la consolidation des données entre data brokers, le *Data Governance Act* prévoit l'impossibilité de revente des données à d'autres intermédiaires de données :

123. *Regulation of the European Parliament and of the Council on European Data Governance* (Data Governance Act, 25 Nov 2020) ec.europa.eu/newsroom/dae/document.cfm?doc_id=71222

124. Speech by Executive Vice-President Vestager at the Press Conference on the Data Governance Act and the Action Plan on Intellectual Property (25 novembre 2020) ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_2210

> La neutralité des prestataires de services de partage de données à l'égard des données échangées entre les détenteurs et les utilisateurs de données est fondamentale pour instaurer la confiance et accroître le contrôle des détenteurs et des utilisateurs de données. Il est donc nécessaire que les prestataires de services de partage de données agissent uniquement en tant qu'intermédiaires dans les transactions, et qu'ils n'utilisent les données échangées à aucune autre fin. Dès lors, une séparation structurelle entre le service de partage de données et tout autre service fourni sera également nécessaire, afin d'éviter les conflits d'intérêts. Cela signifie que le service de partage de données devrait être fourni par une entité juridique distincte des autres activités du prestataire[125].

De plus, pour limiter les risques liés à l'utilisation des données issues du secteur public, les conditions de réutilisation de ces données seront fixées par contrat et ne pourront plus excéder une durée de trois ans. Le *Data Governance Act* prévoit ainsi la création de nouveaux espaces européens communs des données (ou *European Data Spaces*) dans les domaines de la santé, des transports, de l'industrie manufacturière, des services financiers, de l'énergie, du développement durable, de l'agriculture, des administrations publiques, ou encore des compétences…

4.4.4 L'Internet des objets dotera les data brokers de capacités encore plus « intrusives »

L'Internet des objets, par la multiplication des sources d'information et aussi par la possibilité de recueillir des informations sur les plus infimes actions de leurs utilisateurs donne aux data brokers des instruments nouveaux pour consolider les profils qu'ils rassemblent sur les utilisateurs.

125. *Regulation of the European Parliament and of the Council on European Data Governance* (Data Governance Act, 25 novembre 2020) ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_2210

Ainsi, la minimisation et l'agrégation des données issues des objets connectés pourraient être insuffisantes pour garantir une protection suffisante de la vie privée des usagers. En effet l'usage de système d'intelligence artificielle permet déjà, via l'analyse de données en apparence anodines, de déduire des schémas de comportement associés à des données sensibles[126]. C'est par exemple le cas du détecteur de fumée *Nest Protect* qui possède un capteur de présence qui déclenche l'allumage d'une veilleuse lors de passages nocturnes sous le détecteur. Les informations issues de cette fonction « annexe » pourraient avoir des conséquences importantes sur le profil de l'utilisateur. En effet l'heure et le nombre de passages sous ce capteur pourraient être révélateurs de troubles du comportement ou de pathologies. Ces données une fois soumises à des algorithmes d'analyse du risque, pourraient ainsi modifier le profil assurantiel de leurs utilisateurs.

D'autres formes de déductions concernant les données sensibles peuvent être issues de l'analyse des informations issues des compteurs électriques intelligents. Ainsi, en analysant les schémas de consommation énergétique, il devient possible d'effectuer un profilage ethnique ou religieux des usagers. En effet, l'absence ou la diminution de consommation électrique à des périodes précises permettent de déduire si l'utilisateur modifie sa consommation lors du mois du ramadan ou le vendredi soir et le samedi pour les personnes qui observent le shabbat.

4.4.5 Des risques de sécurité inhérents aux activités des data brokers

Plus récemment, aux États-Unis, c'est la *NSA (National Security Agency)* qui s'est inquiétée de la dissémination incontrôlée des données de géolocalisation des agents du gouvernement américain. En effet, cette diffusion permettait via les data brokers de retracer les déplacements

126. Données sensibles (Définition de la CNIL) : données relatives à l'origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques ou biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie (ou l'orientation) sexuelle. www.cnil.fr/fr/definition/donnee-sensibleinfluence-machine/

des personnes et ainsi de connaître leurs activités. Cela constituait une vulnérabilité à la fois pour les agents du gouvernement en particulier pour leurs militaires et les agents du renseignement :

> La NSA a publié de nouvelles directives à l'intention des personnels militaires et des services de renseignement, les avertissant sur les risques liés à la géolocalisation des téléphones portables par le biais d'applications, de réseaux sans fil et des technologies Bluetooth. L'avertissement détaillé de l'une des principales agences de renseignement du pays est une reconnaissance du fait que la pratique de la Silicon Valley consistant à collecter et à vendre des informations de géolocalisation de téléphones portables à des fins de publicité et de marketing représente un risque de sécurité nationale sérieux pour de nombreuses personnes au sein du secteur public.[127]

À l'issue du scandale *Cambridge Analytica*, certains chercheurs établissent même un parallèle entre les risques sécuritaires issus de la dissémination des armes, et les risques sociaux et politiques issus de la dissémination des données sensibles sur les individus qui, à leur tour, peuvent devenir des armes[128]. Dans un premier temps, les régulateurs ont conçu des régulations « en aval » de la captation de la donnée. Pensant que ces régulations suffiraient à limiter les risques de dérives issues de l'Internet et dans un second temps de l'Internet des objets. Ainsi, pour l'enseignante à *Harvard* Shoshana Zuboff, les activités des data brokers contribuent à la transformation de nos sociétés vers ce qu'elle nomme le « *Capitalisme de surveillance* » :

> Dans cette nouvelle phase de développement du capitalisme, la matière première est la nature humaine qui est à l'origine d'une nouvelle dynamique de marché, dans laquelle les prévisions de notre comportement sont mises au jour puis vendues. Les impératifs économiques de ce nouveau capitalisme produisent des

127. *NSA Warns Cellphone Location Data Could Pose National-Security Threat* (The Wall Street Journal, août 4, 2020) www.wsj.com/articles/nsa-warns-cellphone-location-data-could-pose-national-security-threat-11596563156

128. *Weaponizing the Digital Influence Machine : The Political Perils of Online Ad Tech* (Data & Society Report, 17 octobre 2018) datasociety.net/library/weaponizing-the-digital-

> asymétries extrêmes des connaissances et du pouvoir qui découlent de ces connaissances. Cela représente un territoire inédit qui aura de profondes conséquences sur la société du XXIe siècle[129].

Désormais, pour que ces technologies soient en mesure de se développer sans remettre en cause les principes et valeurs des Européens, il conviendra d'établir des mécanismes de limitation des activités de collecte, de stockage ainsi que de circulation des données issues des objets connectés.

4.5 Internet des objets et « *surplus comportemental* »

Les grandes plateformes de l'Internet ont en effet découvert que l'analyse des activités de leurs usagers leur permettait d'obtenir des informations précieuses sur leur personnalité, leurs convictions, leurs habitudes et leur histoire personnelle. Ces informations, une fois rassemblées et analysées, constituaient un levier puissant pour influencer les comportements de consommation des utilisateurs de ces plateformes et même modeler certaines de leurs convictions. Ce principe a été inventé par *Google* dans les premières années de développement de son moteur de recherche et il a été décrit par Shoshana Zuboff. Il correspond à l'analyse de ce qu'elle nomme le « *surplus comportemental* » (*behavioral surplus*). En effet, *Google* a décidé très tôt d'analyser la totalité des requêtes des utilisateurs et pas seulement de celles qui étaient utiles à l'amélioration des résultats du moteur de recherche. Ce surcroît d'informations a permis à *Google* d'analyser massivement les comportements et les centres d'intérêt de plusieurs milliards d'utilisateurs. Ces informations lui ont non seulement permis d'améliorer l'efficacité des démarches publicitaires mais aussi d'agir dans la durée sur le comportement des usagers. En effet, en analysant les réactions des utilisateurs, il devenait possible de les soumettre à des messages ciblés en fonction de leur état d'humeur,

129. *Twenty years of surveillance marketing - Shoshana Zuboff* (Wired Magazine 21 nov 2018) www.wired.com/beyond-the-beyond/2018/11/twenty-years-surveillance-marketing/

de leur localisation, de leur situation familiale ou professionnelle ou encore de leurs convictions religieuses ou politiques.

Avec l'Internet des objets c'est une deuxième phase de ce *surplus comportemental* qui se mettra en place et permettra, au-delà des interactions informationnelles de rassembler les données sur le comportement quotidien des usagers. En effet, les profils déjà assemblés sur les usagers de l'Internet par les plateformes dédiées au micro-ciblage publicitaire permettent d'accroître considérablement l'efficacité des démarches des annonceurs. En connectant des objets jusqu'ici « inanimés » et en permettant à ces objets de « parler » de leurs utilisateurs, ces technologies rendent visibles des comportements et des réactions qui échappaient jusqu'ici aux data brokers. Ce que rappelle Shoshana Zuboff : *« Le directeur de la recherche de Gartner, le cabinet de recherche et de conseil aux entreprises, le souligne sans ambiguïté lorsqu'il évoque la maîtrise de l'Internet des objets comme un élément clé dans la transformation des modèles économiques de « niveaux de performance garantis » en « résultats garantis »... »*[130].

4.6 De nouvelles architectures pour protéger la vie privée ?

Face à la constitution de ces gigantesques agrégateurs de données, un enjeu juridique et technologique majeur correspondra au fait d'assurer aux usagers de l'Internet une meilleure maîtrise de leurs données. Ainsi, afin de garantir l'interopérabilité et la portabilité entre les différentes plateformes qui traitent les données issues des objets connectés, de nouvelles architectures technologiques et juridiques devront être mises en place. Ainsi Lalana Kagal du laboratoire d'Informatique et d'intelligence artificielle au MIT prévoit que les changements dans les régulations concernant les données personnelles devraient avoir pour objectifs d'inciter

130. *The Age of Surveillance Capitalism.* Shoshana Zuboff (Public Affairs 2019)

ces entreprises à revoir l'architecture de leurs applications : « *Les réglementations en matière de protection de la vie privée pourraient devenir tellement restrictives que les entreprises pourraient être obligées de passer à un modèle plus décentralisé. Elles pourraient se rendre compte que le stockage et la collecte de toutes ces informations personnelles ne valent plus la peine… »*[131]

> **“ Les réglementations en matière de protection de la vie privée pourraient devenir tellement restrictives que les entreprises pourraient être obligées de passer à un modèle plus décentralisé. Elles pourraient se rendre compte que le stockage et la collecte de toutes ces informations personnelles ne valent plus la peine…**
>
> **Lalana Kagal**

De nombreux acteurs « historiques » de l'Internet ont aussi souhaité proposer de nouvelles architectures technologiques pour aider les usagers à mieux contrôler leurs données personnelles sur Internet. C'est le cas de l'inventeur du Web, Tim Berners-Lee, avec son projet *Solid*[132]. Ce projet né après le scandale *Cambridge Analytica* repose sur le principe de la « séparation structurelle » entre les données introduites par les utilisateurs et les applications qui devront les traiter. En effet pour Tim Berners-Lee : *« Il y a une nécessité très forte, aujourd'hui, de séparer les applications des données, Ces programmes peuvent accéder et traiter vos photos, vos informations, vos contacts, etc., il n'y a pas de problème à cela. Mais vous devez avoir un contrôle permanent et total sur vos informations. C'est vous qui devez autoriser tel ou tel service à y accéder. »*[133]

Dans un domaine voisin, l'auteur Cory Doctorow dans sa tribune pour l'*Electronic Frontier Foundation* évoquait la nécessité de créer de nouveaux intermédiaires informationnels qui pourraient intervenir en lieu et place des usagers lors de la collecte et l'utilisation de leurs données personnelles. Sa proposition aurait pour but de décloisonner les silos informationnels des grandes plateformes et garantir leur interopérabilité. Elle aurait aussi pour but d'éviter que les données ne continuent à

131. *A plan to redesign the internet could make apps that no one controls* Will Douglas Heaven (MIT Technology Review, 1er juillet 2020) www.technologyreview.com/2020/07/01/1004725/redesign-internet-apps-no-one-controls-data-privacy-innovation-cloud/

132. *Ibid.*

133. *Les solutions de Tim Berners-Lee pour sauver le web* (Le Temps, 12 mars 2019) www.letemps.ch/economie/solutions-tim-bernerslee-sauver-web

être utilisées et diffusées hors de tout contrôle. Pour Cory Doctorow, les acteurs qui interviendraient au nom des utilisateurs devraient être régis par des nouvelles règles : *« Les données partagées devront être réduites au minimum à ce qui est réellement nécessaire pour réaliser l'interopérabilité. Et les entreprises qui collectent des données via ces nouvelles interfaces interopérables ne devraient pas être autorisées à monétiser ces données de quelque manière que ce soit, y compris en les utilisant pour effectuer le profilage des utilisateurs à des fins publicitaires. »*[134]

4.7 Quelle régulation pour les technologies de l'Internet des objets ?

Un autre instrument de régulation des plateformes sera lié à l'analyse des algorithmes qui traitent les données personnelles. En effet, la transparence vis-à-vis du « *Code* » de ces algorithmes pourrait bientôt devenir un impératif pour les sociétés démocratiques. Cette régulation pourrait s'appliquer en particulier à la conception des algorithmes des objets connectés qui auront une influence sur la sécurité des personnes. C'est par exemple le cas pour les algorithmes qui assureront le fonctionnement des véhicules autonomes. Ainsi, le *Media Lab* du *MIT (Massachusetts Institute of Technology)* a mis en place le projet *Moral Machine* pour analyser les choix éthiques et moraux des utilisateurs en cas d'accidents impliquant des voitures autonomes. Ce projet a permis de réaliser une enquête internationale auprès de personnes issues de 233 pays et territoires. L'analyse de cette enquête a permis de connaître les points de consensus mais aussi les divergences dans les choix éthiques des utilisateurs en fonction de leurs pays d'origine (cf. schéma *MIT Moral Machine*[135]).

Comme le préconise Lawrence Lessig[136], le juriste spécialiste de la régulation de l'Internet, le « *Code* » des algorithmes cruciaux pour la vie des citoyens devra être sous le contrôle des citoyens et plus

134. *A Legislative Path to an Interoperable Internet* (Bennett Cyphers and Cory Doctorow, Electronic Frontier Foundation, 28 juillet 2020) www.eff.org/deeplinks/2020/07/legislative-path-interoperable-internet

135. *The Moral Machine Experiment* (E. Awad, S. Dsouza, R. Kim, J. Schulz, J. Henrich, A. Shariff, J-F. Bonnefon & I. Rahwan - Nature, 24 octobre 2018) www.americaninno.com/wp-content/uploads/2017/05/The-MM-Experiment.pdf

136. *Code and other Laws of Cyberespace,* Lawrence Lessig (Basic Books, 1999)

conçu de manière opaque par des sociétés en dehors de tout contrôle démocratique. Ainsi, l'universitaire Frank Pasquale dans son ouvrage *The Black Box Society* réclame la transparence pour ces algorithmes qui ont un impact majeur sur nos sociétés : « *Exiger la transparence de la part des industriels des technologies n'est que la première étape. Pour qu'une société soit lisible par ses citoyens, elle doit s'assurer que les décisions cruciales de ses plus importantes entreprises sont justes, non-discriminatoires et aussi qu'elles sont contestables. Les acteurs de la Silicon Valley et de Wall Street doivent accepter autant de responsabilité qu'ils en imposent aux autres…* »[137]. Ce besoin de régulation sera d'autant plus important pour l'Internet des objets que de nouvelles générations d'objets connectés seront présentes dans l'environnement des utilisateurs sans qu'ils en aient forcément conscience. Ainsi, qu'il s'agisse des objets du contrôle environnemental, des transports autonomes ou des capteurs des villes intelligentes, les technologies qui permettront de recueillir et traiter ces informations devront être sous le contrôle des citoyens. Mais les régulations qui imposeront à ces plateformes une plus grande transparence et une interopérabilité avec leurs concurrents, se heurtent encore à la rapidité d'évolution des acteurs technologiques. Plutôt que de rendre public le code de ces algorithmes cruciaux pour les acteurs économiques et pour le fonctionnement démocratique de nos sociétés, Frank Pasquale propose de créer des mécanismes d'audit par des experts du code de ces algorithmes (on parle dans ce cas de « *transparence qualifiée* »). En Europe déjà le principe de la transparence des algorithmes cruciaux apparaît déjà comme une nécessité pour les régulateurs. Ainsi, Margrethe Vestager a souhaité que soient intégrées dans

> **“Nous ne pouvons pas laisser les décisions qui affectent l'avenir de notre démocratie être prises dans le secret de quelques conseils d'administration…**
>
> **Margrethe Vestager**

137. *The Black Box Society* par Frank Pasquale (Harvard University Press 2015)

la nouvelle directive sur les services numériques (*Digital Services Act*[138]) des mesures pour assurer la transparence des algorithmes des grandes plateformes. En effet, pour la vice-présidente de la Commission européenne : « Nous ne pouvons pas laisser les décisions qui affectent l'avenir de notre démocratie être prises dans le secret de quelques conseils d'administration… »[139].

Parallèlement à la régulation des plateformes existantes, les acteurs industriels européens devront aussi être en mesure de développer des technologies qui respecteront les principes et valeurs des citoyens. Les acteurs industriels européens pourraient ainsi être à l'origine d'alternatives aux plateformes existantes qui ne seraient pas basées sur l'extraction de données des utilisateurs à des fins publicitaires. Étrangement, à l'issue de l'affaire Snowden et plus récemment du scandale *Cambridge Analytica*, l'Europe dispose d'une fenêtre d'opportunité pour un rebond industriel qui serait basé sur des technologies plus protectrices des libertés et des individus. En effet, les risques d'une crise de confiance systémique sont tels que les modèles économiques centrés sur les données personnelles et le micro-profilage (ou micro-targeting) apparaissent désormais comme risqués pour les investisseurs. Cela, en raison des incertitudes qui pèsent désormais sur les évolutions du cadre juridique des grandes plateformes et donc sur leurs modèles économiques.

4.8 Radicalisation algorithmique… et manipulations électorales

Les algorithmes des grandes plateformes peuvent déjà avoir une influence déterminante sur la formation des opinions publiques. Ainsi en favorisant l'exposition de leurs usagers à des contenus plus « clivants » ou « polarisants », ces plateformes exercent un rôle politique majeur. La sociologue Zeynep Tüfekçi décrit ainsi une « convergence

138. Regulation of the European Parliament and of The Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (15 décembre 2020) https://ec.europa.eu/info/sites/info/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf

139. *Algorithms and democracy* (Margrethe Vestager at AlgorithmWatch Online Policy Dialogue, 30 octobre 2020) https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/algorithms-and-democracy-algorithmwatch-online-policy-dialogue-30-october-2020_en

d'intérêts toxique » entre *YouTube* et les mouvements politiques les plus radicaux en ces termes : *« Les concepteurs des algorithmes de recommandation de YouTube se sont rendu compte que si vous incitez les gens à penser que vous allez leur montrer quelque chose de plus radical, de plus « hardcore », ils resteront plus longtemps, pendant que Google leur montrera des publicités »*. Et de conclure que : *« Compte tenu de son milliard d'utilisateurs, YouTube est peut-être l'un des plus puissants instruments de radicalisation du XXIe siècle… »*[140].

> **Compte tenu de son milliard d'utilisateurs, YouTube est peut-être l'un des plus puissants instruments de radicalisation du XXIe siècle…**
>
> **Zeynep Tüfekçi**

La connaissance intime des individus que permettent les réseaux sociaux peut déjà avoir des conséquences sur le fonctionnement même des démocraties. Ainsi, comme l'a démontré le scandale *Cambridge Analytica*, des manipulations électorales portant sur un nombre restreint de personnes peuvent avoir des conséquences politiques majeures sur des scrutins essentiels. Les messages hyper-ciblés qui furent envoyés en fonction des profils politiques et émotionnels des électeurs pourraient avoir fait basculer l'élection présidentielle américaine de 2016 qui s'est jouée à 107 000 voix dans 3 États (Pennsylvanie, Wisconsin, Michigan). Ces votes ne représentaient alors que 0,09 % des suffrages exprimés lors de cette élection[141]. En effet, comme le notent les chercheurs du think tank *Data* & *Society,* les campagnes basées sur le micro-ciblage des électeurs ne peuvent faire évoluer des pans entiers de l'électorat mais se révèlent assez efficaces pour influencer la frange d'indécis qui peut faire basculer une élection en cas de scrutin serré :

> Le ciblage des publicités politiques sera rarement, voire jamais, efficace pour changer les croyances profondes des individus. L'objectif de ces campagnes sera plutôt d'amplifier les ressentiments et les angoisses existantes, d'augmenter les résonances émotionnelles de certains sujets ou de faire passer au premier

140. *YouTube, the Great Radicalizer* Zeynep Tufekci (Op-Ed New York Times, 10 mars 2018) www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html

141. *How Trump won the presidency with razor-thin margins in swing states (*Washington Post 11 novembre 2016) www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/

> plan certaines préoccupations au détriment d'autres, [...] et d'influencer subtilement les décisions concernant des comportements ordinaires (comme le fait d'aller voter ou d'assister à une réunion politique). Dans le cas d'élections serrées, si ces tactiques offrent des avantages même minimes, les groupes qui s'engagent dans ces manœuvres peuvent en retirer d'importants bénéfices[142].

D'autres mécanismes qui combinent les données issues des réseaux sociaux et la puissance de traitement des systèmes d'intelligence artificielle sont désormais utilisés pour subvertir le fonctionnement électoral lui-même. Ainsi, pour la juge à la Cour suprême américaine Elena Kagan, les redécoupages électoraux assistés par intelligence artificielle (*gerrymandering)* pourraient saper les fondements même de la démocratie. Ces manipulations électorales permettraient en effet de rendre certaines circonscriptions « ingagnables » ou au contraire « imperdables ». Pour Elena Kagan : *« À mesure que le temps passe, les manipulations liées aux redécoupages électoraux ne feront que s'aggraver. Ce qui était possible avec un papier et un stylo deviendra insignifiant face à ce qui deviendra possible avec le développement de l'intelligence artificielle. À mesure que les données deviendront plus précises et que s'amélioreront les techniques d'analyse, quelque part en chemin, le peuple aura perdu sa souveraineté...*[143] ».

142. *Weaponizing the Digital Influence Machine : The Political Perils of Online Ad Tech* (Data & Society Report, 17 octobre 2018) datasociety.net/library/weaponizing-the-digital-influence-machine/

143. *Supreme Court Justice Elena Kagan warns AI-powered gerrymandering could undermine US democracy* (Business Insider, 28 juin 2019) www.businessinsider.com/justice-elena-kagan-warns-ai-powered-gerrymandering-may-hurt-democracy-2019-6

5
GÉOPOLITIQUE DE L'INTERNET DES OBJETS

5.1 Le conflit sino-américain sur la *5G*

Les technologies de l'Internet des objets peuvent ainsi être à l'origine de tensions internationales en raison de leur caractère stratégique pour les États. Le conflit entre les autorités américaines et la société *Huawei* sur les technologies *5G* a constitué dans ce domaine un signal d'alarme pour l'ensemble des gouvernements européens. Au-delà des enjeux liés à la concurrence industrielle sino-américaine, la sécurité des infrastructures de l'Internet des objets est devenue un enjeu de sécurité nationale pour chaque pays de l'Union. En France, l'*ANSSI (Agence nationale de la sécurité des systèmes d'information)* a ainsi imposé, pour les opérateurs télécoms qui en étaient déjà équipés, une date butoir de 8 ans pour l'utilisation des équipements de la société *Huawei*[144].

Cette crise a aussi révélé des changements dans la dynamique transatlantique en matière de technologies. Ainsi, le ministre américain de la justice William Barr a déclaré que, pour faire pièce à la société *Huawei*, il devenait nécessaire pour les « *États-Unis et des compagnies alliées* » d'envisager une prise de participation majoritaire au sein des deux équipementiers européens *Nokia* et *Ericsson*[145]. En effet, ces deux sociétés possèdent parmi les plus importants portefeuilles de brevets dans le domaine de la *5G* (cf. tableau *IPlytics*[146]). Les industries européennes étant alors perçues par les autorités américaines comme

144. *5G : L'Anssi affirme qu'il n'y aura pas de «bannissement total» de Huawei* (L'Usine Digitale, 6 juillet 2020) www.usine-digitale.fr/article/5g-l-anssi-affirme-qu-il-n-y-aura-pas-de-bannissement-total-de-huawei.N982976

145. *Barr urges US stakes in Nokia and Ericsson to stall Huawei* (Financial Times, 6 février 2020) www.ft.com/content/1aa61918-48fc-11ea-aeb3-955839e06441

146. *Who is leading the 5G patent race? A patent landscape analysis on declared 5G patents and 5G standards contributions* (IPlytics – novembre 2019) www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf

des « proies » pour renforcer la puissance des industriels américains dans leur conflit avec le chinois *Huawei*.

Le conflit sino-américain sur les technologies pourrait avoir d'autres conséquences géopolitiques majeures. En effet, l'embargo mis en place par les autorités américaines concerne plusieurs sociétés américaines mais aussi le fabricant de processeurs taïwanais *TSMC*. Or, cette société produit 90 % des puces commercialisées dans les smartphones de la société *Huawei.* Selon certains observateurs, la dépendance de l'une des sociétés chinoises majeures vis-à-vis de la « province renégate » pourrait constituer le prétexte que cherchent les autorités chinoises pour déclencher une invasion de Taïwan. Ainsi, le *South China Morning Post*, quotidien de Hong Kong et filiale du groupe *Alibaba*, évoquait récemment la possibilité d'une action militaire chinoise contre Taïwan qui prendrait appui sur la nécessité pour la Chine de sécuriser son approvisionnement dans le domaine des technologies stratégiques.[147]

5.2 Internet "*By and for* China" ?

À plusieurs reprises déjà par le passé, le gouvernement chinois a souhaité revenir sur l'architecture des protocoles fondamentaux de l'Internet (*TCP/IP*). Ces projets avaient pour but d'établir un niveau de contrôle plus élevé sur le réseau et ses utilisateurs. Ainsi, en 2004, une proposition de protocole *IPv9* avait été soutenue par les autorités chinoises pour permettre de centraliser les processus de contrôle et de censure du réseau[148]. Cette proposition avait été rapidement abandonnée face à l'hostilité de l'ensemble des acteurs industriels et technologiques qui percevait un risque accru de « *balkanisation* » de l'Internet. Cette fragmentation de l'Internet que certains nomment aujourd'hui « *splinternet* » pourrait se produire si l'Internet était fragmenté pour des raisons politiques ou technologiques[149]. Dans

147. *As US targets China's Huawei, a perfect storm is brewing over Taiwan* (South China Morning Post, 8 août 2020) www.scmp.com/comment/letters/article/3096204/us-targets-chinas-huawei-perfect-storm-brewing-over-taiwan

148. *The Strange Case of China's IPv9* (Telecom Asia, 4 février 2008) www.telecomasia.net/content/strange-case-chinas-ipv9-0
Architecture et Gouvernance de l'Internet (Bernard Benhamou, Revue Esprit, mai 2006) www.netgouvernance.org/ArchitectureEsprit.pdf

149. *Tech leaders have long predicted a 'splinternet' future where the web is divided between the US and China. Trump might make it a reality* (Business Insider, 6 août 2020) www.businessinsider.fr/us/splinternet-us-china-internet-trump-pompeo-firewall-2020-8

son ouvrage sur la fragmentation de l'Internet, l'universitaire Milton Mueller évoque ainsi les risques de stagnation technologique et économique issus de cette fragmentation. Il revient sur la définition de la souveraineté formulée par le politologue Robert Jackson qui par extension pourrait s'appliquer à la souveraineté numérique :

> La souveraineté est un concept fondamental de la politique et du droit qui ne peut être correctement compris que comme, en même temps, une idée d'autorité supérieure de l'État et une idée d'indépendance politique et juridique d'États géographiquement séparés. L'indépendance, la suprématie et la territorialité sont interdépendantes : un monde fondé sur la souveraineté des États est un monde de juridictions territoriales s'excluant mutuellement ; un monde sans chevauchement des juridictions. Il en résulte que pour être « suprême », l'autorité doit également être limitée géographiquement. C'est la combinaison du pouvoir suprême, de la légitimité et de l'exclusivité sur un territoire donné qui définit un souverain[150].

5.3 Une architecture de contrôle pour l'Internet des objets chinois

Dans un premier temps, les autorités chinoises ont pris le risque de la fragmentation technologique de l'Internet. Cependant, le fait de créer une norme Internet incompatible avec le reste du monde s'est révélé être un risque trop grand pour le développement des entreprises et donc de l'économie chinoise. Désormais, la stratégie de la Chine pour redéfinir l'architecture de l'Internet est plutôt de convaincre le reste du monde d'adopter ses propres normes technologiques. Les autorités chinoises s'appuient pour cela sur les recherches effectuées par la société *Huawei.* Celle-ci a en effet développé un « nouveau protocole IP » qui a pour objectif de répondre à des impératifs de contrôle vertical

150. Robert Jackson cité par Milton Mueller dans *Will the Internet Fragment?* (Digital Futures Ed. Wiley 2017)

(top/down) de l'Internet des objets. En effet, malgré la mise en place par les autorités chinoise du *Great Firewall of China*, les protocoles fondamentaux de l'Internet permettent encore à des usagers d'échapper à certaines mesures de contrôle et de censure mises en place par le gouvernement chinois[151]. Pour les autorités chinoises, l'architecture actuelle basée sur *TCP/IP* est « inadaptée » aux évolutions prévisibles de l'Internet. Comme souvent par le passé, lorsque des gouvernements ou des entreprises ont souhaité promouvoir des technologies alternatives à l'Internet, les arguments utilisés s'appuyaient sur la nécessité d'améliorer la qualité de service du réseau. Les exemples mis en avant correspondent à des applications très exigeantes en bande passante (ici, il est question de projection holographique) ou encore des applications critiques en temps réel nécessitant une très faible latence comme la téléchirurgie[152].

Ce protocole *New IP* vise à « recentraliser » le contrôle du réseau en partant du constat que l'architecture décentralisée de l'Internet serait à l'origine de ses lacunes supposées[153]. Cette proposition, si elle devait être adoptée, posséderait en effet un double avantage pour ses concepteurs : elle placerait les acteurs technologiques chinois en position d'arbitre des normes et standards de l'Internet des objets et elle leur permettrait d'intégrer nativement des fonctions de contrôle et de censure[154] pour faciliter le contrôle politique de la population chinoise et pourrait devenir une norme internationale. L'objectif des autorités chinoises étant à terme d'exporter cette technologie de contrôle au-delà de leurs frontières. En effet, comme le note le *Financial Times* : *« Le gouvernement chinois considère la conception de l'infrastructure et des normes de l'Internet comme un élément central de sa politique étrangère numérique, et ses outils de censure comme une démonstration de faisabilité pour un Internet plus efficace, qu'il sera en mesure d'exporter »*[155].

Un exemple récent de la volonté chinoise de combiner actions diplomatiques et exportation des technologies de surveillance est venu

151. *China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI* (ZDnet, 8 août 2020) www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/

152. *China's controversial mission to reinvent the internet* (Financial Times, 27 mars 2020) www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f

153. *Architecture et Gouvernance de l'Internet* (Bernard Benhamou revue Esprit, mai 2006) www.netgouvernance.org/ArchitectureEsprit.pdf

154. *China's "New IP" proposal to replace TCP/IP has a built in "shut up command" for censorship* (Privacy News Online, 3 avril 2020) www.privateinternetaccess.com/blog/chinas-new-ip-proposal-to-replace-tcp-ip-has-a-built-in-shut-up-command-for-censorship

155. *Inside China's controversial mission to reinvent the internet* (Financial Times, 27 mars 2020) www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f

en réponse à l'interdiction de *Huawei* et *TikTok* aux États-Unis. La contre-offensive diplomatique chinoise vise en effet à fédérer une alliance internationale pour contrecarrer l'extension du *Clean Network*[156] mis en place par le département d'État pour bloquer les technologies chinoises aux États-Unis. Ainsi pour le *Wall Street Journal* :

> L'initiative chinoise exhorte les pays à s'opposer à la « *surveillance de masse contre d'autres États* » et appellerait les entreprises technologiques à ne pas installer « de portes dérobées dans leurs produits et services pour obtenir illégalement les données des utilisateurs, contrôler ou manipuler les systèmes et appareils des utilisateurs. Elle exhorterait également les gouvernements à respecter la souveraineté des autres pays dans la manière dont ils traitent les données - conformément à la vision de Pékin sur la « *cyber-souveraineté* », selon laquelle les pays doivent exercent un contrôle total sur leurs propres segments de l'Internet[157].

5.4 Le *Crédit Social* Chinois, nouveau produit d'exportation ?

Un autre « produit » que la Chine a développé à partir de la combinaison des technologies de l'Internet des objets, de la reconnaissance faciale et des algorithmes d'intelligence artificielle est le *Crédit social*. Ce dispositif orwellien élaboré par certaines des plus puissantes sociétés chinoises comme *Alibaba,* permet d'attribuer une note à l'ensemble des citoyens chinois. Cette note permet d'évaluer le « comportement » social, financier et politique de chaque citoyen chinois (cf. infographie *Bertelsmann Foundation* 2019[158]). Une note de *Crédit social* trop basse empêche d'accéder à des libertés aussi fondamentales que se déplacer en train ou en avion, accéder à certains services publics ou encore obtenir un crédit. Selon le journal gouvernemental *Global Times* le gouvernement chinois a déjà empêché 17,5 millions de personnes

156. *The Clean Network* (U.S. Department of State, août 2020) www.state.gov/the-clean-network

157. *China to Launch Initiative to Set Global Data-Security Rules* (Wall Street Journal, Chun Han Wong, 7 septembre 2020) www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974

158. *China's Social Credit System* (Bertelsmann Foundation 2019) https://www.bertelsmann-stiftung.de/fileadmin/files/aam/Asia-Book_A_03_China_Social_Credit_System.pdf

de prendre l'avion et 5,5 millions de personnes de voyager en train à grande vitesse[159]. Pour Hou Yunchun, l'ancien directeur adjoint du centre de recherche sur le développement du Conseil d'État, le but du *Crédit Social* est simplement de « *mettre les personnes discréditées en faillite...* »[160].

Désormais, au-delà de la surveillance de sa population, la Chine pourrait exporter le principe du *Crédit social* au-delà de ses frontières. Il s'agit pour les autorités chinoises d'imposer ce principe de notation à l'ensemble de leurs interlocuteurs économiques étrangers. Ainsi, Tara Francis Chan, du journal britannique *The Independent* évoque l'initiative du gouvernement chinois prise pour noter le comportement politique des entreprises étrangères en particulier dans le domaine des transports :

> Un nouveau rapport du *Strategic Policy Institute* australien mentionne que le système du *Crédit social* [...] a été utilisé avec succès pour menacer des dizaines de compagnies aériennes étrangères afin qu'elles adoptent la position politique du Parti communiste chinois sur Taïwan. Les transporteurs ont été informés que s'ils ne s'y conformaient pas, cette infraction serait inscrite sur leurs dossiers de *Crédit social*. Plus tôt cette année, les entreprises étrangères ont été obligées d'obtenir un « code de crédit social unifié » à 18 chiffres, qui aidera les autorités chinoises à enregistrer les infractions au crédit et servira à déclencher des sanctions[161].

Plus récemment, lors de la pandémie de *Covid-19*, le gouvernement chinois a mis en place avec la société *Alibaba* une application de traçage qui permet de géolocaliser en temps réel l'ensemble des citoyens chinois dans les zones touchées par la pandémie. Cette application peut aussi interdire à certaines personnes l'accès à des lieux publics en fonction de leur exposition supposée au virus[162].

159. *China bars millions from travel for 'social credit' offenses* (Associated Press, 23 février 2019) apnews.com/article/9d-43f4b74260411797043ddd391c13d8

160. *China blacklists millions of people from booking flights as 'social credit' system introduced* (The Independent, 22 novembre 2018) www.independent.co.uk/news/world/asia/china-social-credit-system-flight-booking-blacklisted-beijing-points-a8646316.html

161. *It looks like China is extending its Black Mirror-like 'social credit system' to overseas companies* (Business Insider, 3 juillet 2018) www.businessinsider.fr/us/china-social-credit-system-controlling-foreign-companies-2018-6

162. *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flag* (New York Times, 1 mars 2020) www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

Les instruments dont disposent les régimes autoritaires pour effectuer leur surveillance de masse n'ont jamais été aussi intrusifs ou précis que ceux dont ils bénéficient désormais avec l'apport combiné des terminaux mobiles, des réseaux sociaux et de l'intelligence artificielle. À ces informations sur le comportement des individus s'ajoutent désormais les informations issues des technologies de génomique. Au-delà du *Crédit social*, les autorités chinoises souhaitent utiliser le « *Génome social* » comme nouvel outil de surveillance de masse. Ainsi, grâce aux équipements de séquençage *ADN* de la société américaine *Thermo Fisher Scientific*, les autorités chinoises renforcent leur système de surveillance de masse en particulier auprès des minorités ethniques (Tibétains, Hui en Mongolie ou Ouïgours au Xinjiang)[163]. La police chinoise recueille des échantillons de sang d'hommes et de garçons dans l'ensemble du pays afin d'établir progressivement la cartographie génétique de ses 700 millions d'hommes[164].

163. *U.S. DNA firm Thermo Fisher reportedly still helping China tamp unrest, crime* (Biometric Update, 19 juin 2020) www.biometricupdate.com/202006/u-s-dna-firm-thermo-fisher-reportedly-still-helping-china-tamp-unrest-crime

164. *China Is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment* (New York Times, 17 juin 2020) www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html

6
POLITIQUE INDUSTRIELLE ET INTERNET DES OBJETS

À l'heure de l'Internet des objets, la souveraineté numérique ne peut se concevoir sous une forme uniquement défensive mais bien comme la synergie entre mesures de régulation et élaboration de dispositifs de politique industrielle. En effet, comme l'a démontré le succès du programme allemand *Industrie 4.0*, seul le développement d'alternatives technologiques européennes constituera une solution durable aux défis technologiques et politiques que posent les technologies extra-européennes en termes de souveraineté numérique.

L'État américain exerce depuis l'origine son action de politique industrielle en appuyant des technologies (et des industries) en fonction de leur caractère stratégique. De nombreuses technologies de l'Internet (et l'Internet lui-même) ont d'abord été développées dans un environnement ou avec le soutien de crédits militaires. Cette importance de l'action de l'État américain dans le développement des technologies de l'Internet est telle que l'économiste Mariana Mazzucato évoquait les technologies clés de l'iPhone en ces termes : *« Il n'y en a pas une seule qui n'ait pas été financée par l'État fédéral américain. Cela inclut les technologies des réseaux sans fil, l'Internet, le GPS, l'écran tactile, et plus récemment l'assistant personnel à commande vocale Siri...*[173] *».* Le schéma d'intervention de l'État était alors le suivant : après financement

165. *Tech's Enduring Great-Man Myth* (MIT Technology Review, 4 août 2015) www.technologyreview.com/s/539861/techs-enduring-great-man-myth/

public des recherches fondamentales sur les technologies stratégiques, le relais était pris par la commande publique (via l'instrument du *Small Business Act)* pour accompagner les premières phases de développement d'applications civiles et faire émerger les technologies les plus prometteuses qui à leur tour pouvaient être financées par des fonds privés.

6.1 Vers un *Small Business Act* français et européen

Développer les technologies nécessaires pour assurer la souveraineté numérique des pays de l'Union européenne nécessitera aussi d'orienter la commande publique vers les *PME* innovantes. En effet, le levier de la commande publique est l'un des instruments les plus puissants pour aider les entreprises à orienter leurs activités en fonction d'une demande solvable et ainsi faire évoluer leurs offres et leur permettre d'étendre leurs activités. Cette croissance des *PME* innovantes passera aussi par la mise en place d'un *Small Business Act* en France et en Europe pour réserver une part significative de l'ensemble des commandes publiques à des *PME* innovantes. Il s'agira aussi (et dans le même temps) d'être en mesure de bloquer des interventions extérieures de rachats potentiellement hostiles autour de technologies stratégiques.

Une stratégie défensive fondée uniquement sur le droit ne suffira pas à protéger notre souveraineté numérique et à enrayer la dynamique actuelle de dépendance vis-à-vis des industriels extra-européens. En effet, seul le soutien aux entreprises capables de développer un écosystème industriel indépendant des filières américaines et chinoises permettra d'éviter d'être soumis aux dérives auxquelles nous assistons de la part de ces entreprises.

Les entreprises qui développent les technologies liées aux infrastructures critiques de l'Internet des objets devront à l'avenir être considé-

rées en France (et plus largement en Europe) comme des « *opérateurs d'importance vitale* ». Le rachat, ou la prise de participation majoritaire, de ces entreprises par des entités extra-européennes devra faire l'objet d'un examen préalable afin de déterminer si les risques liés à la sécurité nationale des pays de l'Union européenne peuvent être de nature à remettre en cause ces rachats.

6.2 Développer en France et en Europe les normes et standards de l'Internet des objets

Les pays de l'Union européenne doivent désormais être en mesure de participer à l'élaboration des normes et standards sur lesquels fonctionneront ces objets connectés. Ainsi, les évolutions de l'Internet des objets dans les secteurs clés de la santé, l'énergie, l'environnement et les transports pourraient donner à l'Europe l'occasion de faire valoir ses principes dans le domaine de la protection des données personnelles et plus largement de la protection des libertés. C'est le propos que tenait le vice-chancelier allemand Sigmar Gabriel, en rappelant le caractère crucial de ces normes et standards dans le programme allemand *Industrie 4.0* et plus largement en termes de souveraineté numérique[166]. Dans son ouvrage *Pax Technica*, Philip N. Howard le directeur de l'*Oxford Internet Institute* évoque l'importance que prendra l'élaboration des normes et standards de l'Internet des objets dans les années à venir et ce tant du point de vue industriel que politique :

> Au niveau international, nous devons nous engager activement dans le processus d'établissement de normes technologiques mondiales, encourager l'ouverture et l'interopérabilité, et assouplir les réglementations trop restrictives en matière de propriété intellectuelle. Et maintenant, nous devons nous préoccuper de la structure de l'actionnariat des opérateurs mobiles, en particulier dans les pays où le gouvernement possède directement ces

166. *Sigmar Gabriel : Nous devons continuer de penser à l'avenir en matière de numérisation* (Ministère fédéral de l'Économie et de l'Énergie, BMWi 2016) www.bmwi.de/Redaktion/FR/Pressemitteilungen/2016/20160525-gabriel-bei-digitalisierung-jetzt-schon-weiter-in-die-zukunft-denken.html

> sociétés. Les experts des médias avaient l'habitude de s'élever contre la propriété croisée des journaux, des stations de radio ou des chaînes de télévision. Lorsque les sociétés d'infrastructure produisent également du contenu, la neutralité du réseau - l'idée que toutes les données sur l'internet doivent être traitées de la même manière - est en danger[167].

Pour permettre à la France et l'Europe de participer à l'élaboration des normes et standards de l'Internet des objets, il convient d'assurer une coordination de haut niveau entre l'ensemble des entreprises et organisations chargées d'élaborer ces normes et standards en France et en Europe. Dans le même temps, il conviendrait de renforcer les investissements dans les technologies de l'Internet des objets ainsi que la présence française et européenne dans les instances internationales de normalisation et de standardisation de l'Internet des objets.

6.3 Le programme allemand *Industrie 4.0*

La production industrielle est devenue l'un des secteurs qui a connu la plus forte croissance dans son utilisation des technologies de l'Internet des objets. En effet, comme le précise l'*AIOTI* (*Alliance internationale des industriels pour l'innovation dans l'Internet des objets*), ces technologies sont amenées à avoir un rôle crucial dans l'optimisation de l'ensemble des processus industriels :

> La convergence des technologies cloud et de l'Internet des objets facilitera le développement des usines du futur et la réalisation de fabrication numérique. Ces futures usines comprendront de nombreux dispositifs, des objets intelligents physiques et virtuels, interconnectés tant en interne qu'en externe, pour permettre la configuration et la surveillance dynamiques des capacités opérationnelles de l'usine, ou des réseaux d'usines, le contrôle de

167. *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up,* Philip N. Howard (Yale University Press, 2015)

> la qualité et l'amélioration de l'efficacité. En outre, les processus traditionnels et fragmentés de conception, de production et de relation avec le client seront remplacés par une gestion en boucle fermée de la conception de « bout en bout » et de suivi du client, où les cycles seront plus courts et les produits seront conçus en fonction des exigences du client (fabrication basée sur le client)[168].

Ainsi, de nombreux pays ont souhaité développer l'usage des technologies de l'Internet des objets auprès de leurs entreprises. Cela a été le cas du gouvernement allemand qui a perçu le risque que son appareil productif soit progressivement rendu obsolète par l'arrivée d'acteurs qui utiliseraient les technologies de l'Internet des objets pour obtenir des gains de productivité importants ainsi qu'un canal de relation privilégiée avec leurs clients. La particularité du programme *Industrie 4.0* est qu'il représente un exemple de politique industrielle *ad hoc*. En effet, il s'agissait pour les autorités allemandes de développer les technologies et les savoir-faire de l'Internet des objets spécifiquement utiles au renforcement du potentiel industriel allemand. Pour ses promoteurs, ce programme visait à permettre aux industriels d'économiser sur les processus industriels existants et de créer de nouveaux services à haute valeur ajoutée pour l'entreprise. Il s'agit ainsi de permettre de passer de l'*Internet des objets…* à l'*Internet des services*. Pour Dorothée Kohler et Jean-Daniel Weisz dans leur ouvrage sur le programme allemand *Industrie 4.0* :

> L'objectif premier de l'*Industrie 4.0* ne correspond pas à davantage d'automatisation, mais à plus d'intelligence dans la mise en réseau des machines entre elles et des machines avec les hommes. Il répond au besoin de personnalisation croissante des produits et à la peur de voir des géants de l'internet comme Google capter l'exclusivité de la relation avec le client, monopoliser l'accès à ses données d'usage et drainer une part croissante de la marge au sein de la chaîne de création de valeur[169].

168. *Report on Smart manufacturing - The Alliance for the Internet of Things Innovation* (AIOTI WG11 2015) aioti.eu/wp-content/uploads/2017/03/AIOTIWG11Report2015-Smart-manufacturing.pdf

169. *Industrie 4.0* par Dorothée Kohler et Jean-Daniel Weisz (La Documentation française, 2017)

L'une des missions essentielles du programme *Industrie 4.0* mis en place par le gouvernement allemand aura été de rendre possible les changements dans la structure même du tissu économique des sociétés en Allemagne en développant auprès des industriels *« L'aptitude à accepter la vulnérabilité de modèles d'affaires ayant démontré leur robustesse depuis plus de cent ans… »*[170]. Pour les concepteurs de ce programme, il était nécessaire de sensibiliser l'ensemble des acteurs industriels allemands à ces technologies afin de faire évoluer leurs pratiques et promouvoir l'usage de la donnée industrielle comme vecteur de modèles économiques nouveaux : *« Cela peut même conduire à développer des modèles d'affaires où l'on vend la valeur d'usage des machines et non plus la machine elle-même »*[171].

Une autre originalité de cette démarche est qu'elle a donné lieu à un large consensus politique, social et industriel. Ainsi dans leur entretien avec les responsables de l'*Institut Fraunhofer* chargés de ce programme, les Dr Olaf Sauer et Thomas Usländer précisent :

> La nouveauté avec *l'Industrie 4.0,* c'est que pour la première fois depuis longtemps le sujet de la production et de la création de valeur s'affirme au sein de l'agenda politique (cf. le contrat de coalition). *L'Industrie 4.0* conduit à ce que les ministères, les chercheurs, les fédérations professionnelles et les entreprises tirent tous dans le même sens. Une discussion est en cours au sein de la société sur les bénéfices et les conséquences de l'Industrie 4.0. […] *L'Industrie 4.0* se présente comme la construction d'un nouvel imaginaire industriel destiné à chasser la peur face aux menaces sur le leadership industriel allemand, à accepter les incertitudes, à miser sur des alliances stratégiques pour déjouer le pouvoir intrusif des géants de l'internet, à saisir les opportunités de croissance, à miser sur un leadership collectif. Enfin, elle cherche à faire rêver à une révolution technologique non seulement une population d'ingénieurs et d'informaticiens, mais aussi une société entière[172].

170. *Ibid.*

171. *Ibid.*

172. *Ibid.*

Afin d'étudier l'impact de ces mesures, le cabinet d'étude *Staufen AG* a conçu le *German Industry 4.0 Index*[173], qui a permis de suivre l'adoption des technologies de l'Internet des objets par les entreprises allemandes depuis le lancement du programme *Industrie 4.0*. Les entreprises interrogées appartenaient au secteur de l'ingénierie industrielle, de l'automobile et de l'électrotechnique. Sur l'ensemble des entreprises allemandes étudiées, la part de celles qui n'envisageaient pas d'utiliser les technologies de l'*Industrie 4.0* a diminué de moitié en 5 ans. À l'inverse la part des entreprises qui ont développé des projets opérationnels basés sur ces technologies est passée de 31 à 48 % durant la même période.

Les autres pays de l'Union européenne, s'ils possèdent des paysages industriels différents (et donc des nécessités de politique industrielle différentes) pourraient s'inspirer des leçons du volontarisme politique tel qu'il a été appliqué au renouveau industriel allemand dans le cadre du programme *Industrie 4.0*. D'autres programmes de politiques industriels pourraient ainsi être conçus pour épouser les contours spécifiques des paysages industriels français et européens. Il s'agit ainsi de prendre appui sur les forces et les spécificités industrielles de chaque pays afin de mettre en œuvre avec ces technologies leurs orientations de politique générale (sécurité sanitaire, politique, environnementales, transports, transition énergétique…).

6.4 Vers un « moment antitrust » pour l'Internet des Objets ?

Désormais tant aux États-Unis qu'en Europe, les responsables politiques évoquent des mesures antitrust qui pourraient être prises contre les grandes plateformes. Les sanctions économiques prises jusqu'ici n'ont pas montré d'efficacité réelle tant sur le comportement fiscal qu'en matière de respect de lois sur la concurrence. Face à des

173. *German Industry 4.0 Index 2019* (Staufen AG and Staufen Digital Neonex GmbH Studies 2019) www.staufen.ag/fileadmin/HQ/02-Company/05-Media/2-Studies/STAUFEN.-Study-Industry-4-0-index-2019-en_.pdf

sociétés qui ont acquis des valorisations inédites jusqu'alors les sanctions récemment imposées par la commission européenne à *Google* ou même à *Apple* en Irlande ne remettent pas en cause durablement leurs modèles économiques. Il est à noter qu'*Apple* a connu un quasi-doublement de sa capitalisation boursière durant la pandémie pour atteindre une valorisation de 2000 milliards de dollars.

Pour la première fois, les capitalisations cumulées des entreprises technologiques américaines représentent plus que celles des 600 plus importantes sociétés cotées en Europe (*Stoxx 600 Index*)[174].

Ainsi, dans un changement de doctrine important, le commissaire européen Thierry Breton a évoqué récemment auprès du *Financial Times*[175] qu'il envisageait des sanctions inédites contre les acteurs américains qui abuseraient de leur position dominante ou refuseraient d'appliquer les directives ou règlements européens. Ces mesures pourraient aller jusqu'à l'exclusion du marché européen ou le démantèlement de ces sociétés. Propos que Thierry Breton a précisé dans son discours au Parlement européen auprès de la commission du marché intérieur et de la protection des consommateurs :

> De la même manière que la crise financière de 2008 avait mis en exergue le rôle et le caractère systémique de quelques grandes banques, cette crise a révélé le rôle et le caractère systémique de certaines plateformes qui se comportent souvent comme si elles étaient trop grandes pour se soucier des préoccupations légitimes sur leur rôle : « *too big to care* ». Comme pour les banques, nous devons donc avoir les outils réglementaires adéquats pour superviser et contrôler ces acteurs qui ne sont plus de simples hébergeurs, mais des fournisseurs de services diversifiés et intégrés verticalement[176].

174. *Une combinaison des capitalisations boursières des valeurs technologiques de l'indice S&P 500, d'Amazon, de Facebook et d'Alphabet, société mère de Google, a dépassé pour la première fois celle de l'indice de référence européen Stoxx 600. Bloomberg.*
Christophe Barraud, Top 5 Charts of the Day, 31 août 2020
www.christophe-barraud.com/top-5-charts-of-the-day-31-aout-2020

175. *EU seeks new powers to penalise tech giants* (Financial Times, 20 septembre 2020)
www.ft.com/content/7738fdd8-e0c3-4090-8cc9-7d4b53ff3afb

176. *Discours du Commissaire Breton lors de l'échange de vues avec le Comité IMCO au Parlement européen* (28 septembre 2020)
ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/discours-du-commissaire-breton-lors-de-lechange-de-vues-avec-le-comite-imco-au-parlement-europeen_en

Plus récemment, aux États-Unis, la majorité démocrate à la Chambre des représentants a justifié la nécessité de mettre en œuvre des mesures antitrust à l'encontre des grandes sociétés technologiques comme *Apple, Google, Amazo*n ou *Facebook* en des termes explicites :

> Bien que ces 4 sociétés diffèrent de manière importante, l'étude de leurs pratiques commerciales a révélé des problèmes communs. Premièrement, chacune de ces plateformes sert désormais de contrôleur d'accès pour un canal de distribution stratégique. En contrôlant l'accès aux marchés, ces géants peuvent choisir les gagnants et les perdants dans l'ensemble de notre économie. Non seulement ils exercent un pouvoir énorme, mais ils en abusent également en exigeant des frais exorbitants, en imposant des clauses contractuelles léonines et en collectant des données précieuses sur les personnes et les entreprises qui dépendent de ces plateformes. Deuxièmement, chaque plateforme utilise sa position de passage obligé pour maintenir son pouvoir de marché. En contrôlant les infrastructures de l'ère numérique, ils ont surveillé les autres entreprises pour identifier des rivaux potentiels et ont finalement racheté, copié ou éliminé leurs menaces concurrentielles. Et, enfin, ces entreprises ont abusé de leur rôle d'intermédiaires pour consolider et étendre leur domination. Ces plateformes déjà dominantes ont utilisé leur pouvoir pour devenir encore plus dominantes, par le biais de la cooptation de leurs propres produits, de la pratique de prix d'éviction ou encore de comportements d'exclusion[177].

Au moment où l'Internet des objets devient un enjeu politique et économique majeur, la régulation des acteurs qui déploient ces solutions technologiques apparaît encore plus nécessaire.

Ainsi, l'ensemble des régulateurs européens reconnaissent la nécessité de promouvoir de nouvelles formes de compétition et d'éviter une

177. *Investigation of Competition in Digital Markets* (House Judiciary Committee's Antitrust Subcommittee, 6 octobre 2020) judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf

concentration préjudiciable tant aux acteurs économiques qu'aux citoyens. La commission européenne vient ainsi de lancer une enquête sur la compétition dans le secteur de l'Internet des objets. La commissaire européenne à la concurrence Margrethe Vestager, a déclaré lors du lancement de cette enquête :

> L'Internet des objets grand public devrait se développer de manière significative dans les années à venir et se banaliser dans la vie quotidienne des consommateurs européens. [...] Les possibilités semblent infinies. Mais l'accès à de grandes quantités de données utilisateur semble être la clé pour succès dans ce secteur, nous devons donc nous assurer que les acteurs du marché n'utilisent pas leur contrôle sur ces données pour fausser la concurrence, ou fermer ces marchés pour des concurrents. Cette enquête sectorielle nous aidera à mieux comprendre la nature et les effets probables des problèmes de concurrence dans ce secteur[178].

Là encore, c'est le contrôle sur les données issues des objets connectés qui constituera le pivot de l'action antitrust en Europe. En effet, comme c'est le cas pour les grandes plateformes de l'Internet, l'absence d'interopérabilité entre les différentes catégories d'objets connectés se traduit par la volonté de créer des environnements propriétaires et « clos » pour les objets conçus par chacune de ces plateformes. C'est cette fermeture qui s'est avérée propice aux abus de position dominante. Cependant, comme le rappelle Shoshana Zuboff, s'il apparaît nécessaire de faire évoluer les législations antitrust dans le domaine des technologies, ce sont bien les législations encadrant la collecte et le traitement des données qui devront évoluer pour instaurer/restaurer la confiance dans les technologies de l'Internet des objets[179].

178. *Antitrust: Commission launches sector inquiry into the consumer Internet of Things (IoT)* (Press release 16 juillet 2020) ec.europa.eu/commission/presscorner/detail/en/IP_20_1326

179. *« La régulation des Gafa sous le prisme de l'antitrust doit être un début pas une fin »* (Le Figaro, 15 octobre 2020) www.lefigaro.fr/secteur/high-tech/shoshana-zuboff-la-regulation-des-gafa-sous-le-prisme-de-l-antitrust-doit-etre-un-debut-pas-une-fin-20201014

6.5 Un climat d'incertitude réglementaire inédit

En plus des menaces d'actions antitrust, les acteurs américains et chinois des technologies sont désormais au cœur de tensions internationales qui pourraient avoir des conséquences imprévisibles sur le développement de ces sociétés. Ainsi, dans le prolongement du conflit sino-américain sur la *5G*, deux géants de l'Internet chinois, le réseau social de partage vidéo *TikTok* (*ByteDance)* et l'agrégateur de services de messageries et de paiement sur mobile *WeChat* (*Tencent*) devaient être interdits sur le territoire américain à partir du 12 novembre 2020[180]. Ainsi pour Matt Perault, professeur au *Center on Science and Technology Policy* de l'université *Duke*, on assiste pour la première fois à une inversion de la prise en compte des risques entre les entreprises américaines et chinoises : « *Pour réduire le risque réglementaire, les entreprises chinoises opérant aux États-Unis sont désormais contraintes d'adopter des stratégies similaires à celles que les entreprises américaines ont depuis longtemps adoptées en Chine. Ces stratégies consistent notamment à céder des actifs, à se limiter à des participations minoritaires dans de nouveaux investissements et à ajuster l'endroit où elles stockent les données des clients »*[181].

Désormais, les tensions nées de l'affrontement sino-américain sur les technologies créent un climat d'incertitude industrielle inédit. Ces tensions sont aussi liées aux changements prévisibles des régulations sur le recueil et la localisation des données personnelles. L'ensemble des acteurs technologiques anticipent déjà des modifications importantes des cadres législatifs européens et américains dans ces domaines. Ainsi, la société *Palantir,* dans les documents préalables à son introduction en Bourse, avertissait les investisseurs qu'elle pourrait être contrainte de modifier fondamentalement ses activités en raison des évolutions du cadre juridique sur la protection des données :

180. *TikTok: Trump questions Oracle deal if ByteDance keeps stake* (The Guardian, 17 septembre 2020) www.theguardian.com/technology/2020/sep/17/tiktok-trump-questions-oracle-deal-if-bytedance-keeps-stake

181. *Trump's Attacks on TikTok and WeChat Could Further Fracture the Internet* (New York Times, 17 août 2020) www.nytimes.com/2020/08/17/technology/trump-tiktok-wechat-ban.html

> La nature évolutive de ces lois, a déclaré *Palantir*, « pourrait se traduire par des coûts, des dommages ou une responsabilité » pour l'entreprise si elle ne parvient pas à mettre en œuvre et à suivre les contrôles programmatiques appropriés, ou si elle subit des violations malveillantes (ou par inadvertance) des exigences de confidentialité et de protection des données. Outre les amendes, poursuites et autres procédures qui pourraient survenir en cas de non-conformité, la société a déclaré que des lois nouvelles ou modifiées pourraient obliger *Palantir* à modifier ou « changer fondamentalement » ses activités[182].

Ces mises en garde intervenaient après l'annulation du *Privacy Shield* l'accord transatlantique sur le traitement des données personnelles des Européens aux États-Unis. À terme, il apparaît désormais probable que des régulations seront conçues afin de mieux contrôler la circulation et le traitement des données personnelles. En Europe de nouvelles régulations pourraient en effet imposer que les données personnelles des Européens (en particulier leurs données sensibles comme les données de santé) soient exclusivement traitées sur le territoire de l'Union européenne.

6.6 Annulation du Privacy Shield : quelles conséquences pour l'Internet des objets ?

En effet, le principe qui prévaut jusqu'ici auprès de la Commission européenne pour les données « non personnelles » était celui du *Free Data Flow*[183]. Ce principe pourrait lui aussi être remis en cause pour favoriser le traitement des données en Europe par des acteurs industriels européens. Récemment, Thierry Breton a ainsi évoqué pour la première fois la nécessité de mettre en œuvre les principes de *Data Localisation*/*Data Residency* pour les données des Européens :

182. *Palantir warns investors of complex, inconsistent global privacy law risk* (Yahoo Finance, 26 août 2020) finance.yahoo.com/news/palantir-s1-warns-of-complex-inconsistent-global-privacy-law-risk-125635667.html

183. *Free flow of non-personal data* (European Commission - Shaping Europe's digital future, 24 février 2020) ec.europa.eu/digital-single-market/en/free-flow-non-personal-data

> Ce qui fait le succès de l'Internet, c'est son caractère mondial. En ce qui nous concerne nous, Européens, nos données, c'est ce que nous avons de plus précieux en matière industrielle», a déclaré le commissaire européen au marché intérieur. «J'ai toujours dit que je souhaitais que les données des Européens soient traitées, stockées et processées en Europe. J'ai l'impression que Donald Trump dit la même chose. Les Chinois et les Russes le font, on le fera aussi[184].

Cette déclaration intervenait après la décision de la *CJUE* (*Cour de Justice de l'Union Européenne*) du 16 juillet 2020 qui a jugé le que la transmission de données personnelles depuis l'Union Européenne vers les États-Unis, n'offrait pas une protection suffisante au vu des risques d'interceptions de ces données par les autorités américaines[185]. Face à cette nouvelle annulation d'un accord transatlantique, l'Union européenne peut tenter de renégocier un accord, au risque de le voir à son tour invalidé pour les mêmes motifs. L'autre option consisterait à établir les bases d'un nouveau modèle de circulation des données réaffirmant que les Européens doivent pouvoir disposer de leurs données, à la fois dans les outils et les usages, en ayant recours à des entités localisées et gouvernées depuis l'Europe.

Depuis l'annulation du *Safe Harbor* en 2015, les *GAFAM* étaient déjà dans l'anticipation de la chute du *Privacy Shield* en créant plusieurs data centers en Europe dans la perspective d'un durcissement des régulations sur la localisation des données[186]. Cependant, ces précautions pourraient s'avérer insuffisantes du fait des lois comme le *Patriot Act* de 2001 et surtout le *Cloud Act* de 2018 qui ajoute l'extraterritorialité et permet aux autorités américaines d'obtenir des données stockées par des sociétés américaines en dehors des États-Unis. Plus récemment encore, la *Cour de justice de l'Union européenne* a aussi déclaré que la surveillance de masse « *généralisée et indifférenciée* » via les données collectées par les opérateurs télécoms

184. *Thierry Breton: « Je souhaite que les données des Européens soient traitées et stockées en Europe »* (BFMTV, 25 août 2020) www.bfmtv.com/economie/thierry-breton-je-souhaite-que-les-donnees-des-europeens-soient-traitees-et-stockees-en-europe_AD-202008250281.html

185. *The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield* (CJUE, 16 juillet 2020) curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf
The Fight for Digital Sovereignty : What It Is, and Why It Matters, Especially for the EU (Luciano Floridi, Springer Nature, 12 août 2020) link.springer.com/article/10.1007/s13347-020-00423-6#Fn5

186. *U.S. Tech Giants Are Investing Billions to Keep Data in Europe* (New York Times, 3 octobre 2016) www.nytimes.com/2016/10/04/technology/us-europe-cloud-computing-amazon-microsoft-google.html

(données de géolocalisation ou métadonnées de connexion) était incompatible avec le droit européen[187].

L'une des options désormais envisagées par les États européens est non seulement que les données des Européens soient traitées sur le territoire de l'Union, mais aussi que le quartier général des sociétés chargées du traitement de ces données soit lui-même localisé en Europe. Ainsi les projets de clouds européens souverains prendraient une importance particulière si cette option de « *Data Residency* » était retenue par l'Union européenne. C'est ce que notent les responsables du *Conseil européen des relations internationales* à propos du projet *Gaia-X* :

> Le projet Gaia-X est motivé par la notion de « souveraineté des données » ou, plus précisément, de « gouvernance des données », et vise à exercer un plus grand contrôle européen sur les flux et le stockage des données. Cela reflète le fait que non seulement de plus en plus de processus métier fonctionneront sur des services basés sur le cloud, mais que les principaux fournisseurs de cloud sont des entreprises basées aux États-Unis et donc soumis aux juridictions américaines. Cela rend l'Europe vulnérable car elle ne peut pas influer sur la manière dont ces données sont gérées et gouvernées[188].

Le projet *Gaia-X*, incarne une nouvelle stratégie européenne fondée sur l'interopérabilité entre différents acteurs économiques du cloud en Europe. Sa réussite dépendra aussi de deux facteurs déterminants en matière de souveraineté numérique : la vigilance vis-à-vis des choix technologiques opérés dans le cadre de cette initiative et la mise en place d'une politique cohérente quant à l'usage des clouds souverains et non-souverains dans l'espace public européen.

187. Arrêts dans l'affaire C-623/17 Privacy International et dans les affaires jointes C-511/18 La Quadrature du Net e.a. et C-512/18, French Data Network e.a., ainsi que C-520/18 Ordre des barreaux francophones et germanophone e.a. (Cour de justice de l'Union européenne, communiqué de presse n° 123/20 - 6 octobre 2020) curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123fr.pdf
Voir aussi : *La justice de l'UE s'oppose à la collecte massive des données de connexions Internet et téléphoniques par les États* (Le Monde, 6 octobre 2020) www.lemonde.fr/pixels/article/2020/10/06/la-justice-de-l-ue-s-oppose-a-la-collecte-massive-des-donnees-de-connexions-internet-et-telephoniques-par-les-etats_6054906_4408996.html

188. *Europe's Digital Sovereignty : From Rulemaker to Superpower in the Age of Us-China Rivalry* Carla Hobbs (ed.) Alicia Richart, *Broadband : Europe's silent digital ally* (European Council on Foreign Relations, juillet 2020) www.ecfr.eu/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf

7

UNE « TROISIÈME VOIE » EUROPÉENNE POUR L'INTERNET DES OBJETS

À elles seules, les mesures d'encadrement juridique et les actions antitrust ne réussiront pas à limiter les risques de dérives issues des technologies de l'Internet des objets. En effet, pour que l'Internet des objets ne remette pas durablement en cause les principes et valeurs qui ont fondé l'Europe, l'Union doit aussi bâtir sa propre stratégie industrielle. Ce que Charles Michel, le président du Conseil européen, résumait en ces termes : « *Le progrès technologique est inutile s'il ne sert pas à améliorer pas la vie des gens. Entre le modèle américain « business avant tout » et l'autoritarisme de l'État chinois, il y a de la place pour un modèle attractif qui serait centré sur l'humain, « une voie européenne » qui pourrait permettre d'établir des normes mondiales dans la révolution numérique »*[189].

> **“Entre le modèle américain « business avant tout » et l'autoritarisme de l'État chinois, il y a de la place pour un modèle attractif centré sur l'humain, « une voie européenne » qui pourrait établir des normes mondiales dans la révolution numérique...**
>
> **Charles Michel**

Le règlement général sur la protection des données (*RGPD*) est déjà devenu une référence internationale au-delà même des frontières de l'Union européenne. Depuis sa mise en œuvre, certains États

189. *"Europe's way" to set global standards in the digital revolution.* Charles Michel (Financial Times - ETNO 26 septembre 2020) www.consilium.europa.eu/en/press/press-releases/2020/09/29/the-digital-in-a-fractious-world-europe-s-way-speech-by-president-charles-michel-at-the-ft-etno-forum/

américains comme la Californie se sont inspirés des travaux européens pour encadrer la collecte et le traitement des données personnelles. C'est aussi le cas en Amérique du Sud pour l'Argentine, le Pérou et le Brésil ainsi que dans plusieurs pays en Afrique et en Asie[190]. Étrangement, même la Chine reconnaît désormais s'inspirer du *RGPD* lorsqu'elle met en place sa première loi sur la cybersécurité et la protection des données personnelles[191].

Comme le *RGPD* a aidé à développer la confiance sur Internet, une filière européenne de l'Internet des objets qui s'appuiera sur une régulation protectrice des données et de la sécurité des usagers pourrait devenir une référence au-delà des frontières de l'Union européenne. Cette alternative aux technologies actuellement conçues aux États-Unis ou en Chine porte désormais le nom de « *troisième voie* », pour l'Internet des objets européen. Ainsi, pour devenir les architectes d'un Internet des objets qui conjuguera les valeurs et les principes des Européens, il conviendra de s'appuyer sur des acteurs industriels européens qui seront à même d'élaborer les normes et standards des prochaines générations de technologies de l'Internet des objets.

7.1 Confiance et sécurité « marques de fabrique » de l'Internet des objets européen

À l'issue du scandale *Cambridge Analytica*, Tom Wheeler, l'ancien patron de la puissante *FCC (Federal Communications Commission)* américaine, déclarait *: « Dans le domaine de la protection de la vie privée, le Nouveau Monde doit apprendre de l'Ancien. L'économie de l'Internet a fait de nos données personnelles une matière première. Le gouvernement américain se doit de rendre le contrôle de ces données à leurs créateurs légitimes*[192] *».* Cet hommage à la vision européenne sur la protection des données montre à quel point la confiance est devenue un facteur crucial pour le développement de ces technologies auprès des citoyens. Si, dans le passé, la protection

190. *The impact of the GDPR outside the EU* (Lexology, septembre 2019) www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f

191. *China unveils first law on personal data protection* (Global Times, 13 octobre 2020) www.globaltimes.cn/content/1203363.shtml

192. *Can Europe Lead on Privacy?* (New York Times, 1 avril 2018) www.nytimes.com/2018/04/01/opinion/europe-privacy-protections.html

des données personnelles était perçue par les entreprises comme une contrainte, elle pourrait devenir pour l'Internet des objets un important facteur de différenciation et un avantage concurrentiel majeur pour les sociétés qui développeront une démarche éthique dans ces domaines. Ainsi, dans leur ouvrage « *Age of Context : Mobile, Sensors, Data and the Future of Privacy* », Scoble et Israel évoquaient en 2013 déjà le caractère crucial de la politique de protection des données pour les entreprises sur Internet *: « À l'heure où les données sont le plus souvent « contextualisées », ce sont les entreprises les plus dignes de confiance qui seront en mesure de se développer. Celles qui seront jugées défaillantes en termes de transparence vont rapidement se retrouver à court de clients. Transparence et fiabilité seront les facteurs de différenciation par lequel les clients effectueront un nombre de plus en plus important de leurs choix. »*[193].

> **“ Transparence et fiabilité seront les facteurs de différenciation par lequel les clients effectueront un nombre de plus en plus important de leurs choix...**
>
> **Robert Scoble et Shel Israel**

Plus récemment, la protection de la vie privée est ainsi devenue un argument commercial pour les fabricants d'objets connectés. Ainsi, *Apple* considère qu'à la différence de son rival *Google* dont le modèle économique est essentiellement lié à la publicité, le développement de ses activités de constructeurs d'objets connectés passe par l'affirmation de son désintérêt pour les données personnelles de ses utilisateurs. Cependant, en plus des applications hébergées sur l'*App Store*, les services développés en propre par *Apple* (*Apple Pay, Apple Music, Apple TV)* prennent une part de plus en plus importante dans les revenus de la société[194]. Or, ces services permettent à *Apple* d'agréger des informations sur les goûts et les activités de ses clients au-delà même des informations issues du fonctionnement usuel des terminaux connectés. Ainsi, une enquête menée en 2019 par le *Washington Post* a montré qu'en moyenne en l'espace d'une semaine, 5400 « traqueurs »

193. *«Age of Context : Mobile, Sensors, Data and the Future of Privacy»*, R. Scoble et S. Israel (Brewster Press 2013)

194. *Apple's Services Revenue Reaches All-Time High* (Statista, mai 2020) www.statista.com/chart/14629/apple-services-revenue/

d'applications transmettaient les données personnelles à l'insu des utilisateurs d'*iPhone*[195]. Ce qui tendait à contredire l'affirmation publicitaire : *« Ce qui se passe sur votre iPhone reste sur votre iPhone… ».*

7.2 Quelles régulations pour la sécurité et la durabilité de l'Internet des objets ?

Pour les régulateurs, il ne s'agit plus uniquement de veiller à sécuriser les dispositifs connectés mais aussi d'envisager les nouveaux usages malveillants qui pourraient être faits à partir des informations recueillies par les objets connectés. On peut ainsi différencier plusieurs « strates » de préoccupations de la part des régulateurs en matière de sécurité de l'Internet des objets.

Le premier niveau de protection concerne la lutte contre la prise de contrôle malveillante des objets connectés. C'est le point le plus consensuel, puisqu'il est question d'éviter que les objets ne se retournent contre leurs utilisateurs lors de piratages (qu'il s'agisse de fuites de données ou de prise de contrôle à distance d'un objet connecté). La loi californienne et la loi britannique prennent en compte en priorité cet aspect de la sécurité des objets connectés. C'est aussi le cas pour le mandat confié à *l'ENISA*, l'agence de cyber-sécurité européenne, pour élaborer un cadre de certification pour les objets connectés en Europe dans le cadre du *Cybersecurity Act*[196].

7.3 Répondre aux nouvelles formes d'attaques basées sur l'Internet des objets

Cependant, avec l'essor des objets connectés dans nos sociétés, nous assistons aussi à la naissance de nouvelles formes d'attaques contre les personnes qui prennent appui sur des objets connectés. Ainsi, Nellie Bowles, dans son enquête pour le *New York Times,* décrivait

195. *It's the middle of the night. Do you know who your iPhone is talking to*? (Washington Post, 28 mai 2019) www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking

196. *Cybersecurity Act: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013* eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN

ces nouvelles formes de violences domestiques souvent issues de personnes proches :

> Une femme allume son climatiseur, mais il s'éteint sans qu'elle y touche. Une autre dit que le code de la serrure numérique de sa porte change tous les jours sans qu'elle comprenne pourquoi. Une autre encore raconte à une ligne d'entraide qu'elle entendait toujours la sonnerie de sa porte, sans que personne ne soit là. Leurs histoires font partie d'un nouveau type de violence conjugale lié à l'essor des technologies des objets connectés. Les serrures, les enceintes connectées, les thermostats intelligents, les lumières et les caméras connectées vendus comme des équipements de pointe sont devenus des outils de harcèlement, de surveillance ou encore de vengeance[197].

Des mesures juridiques d'encadrement viseront à intégrer ces nouvelles formes d'intrusion et d'agression dans le champ des infractions reconnues par la justice. Les dimensions sociétales de la sécurité de l'Internet des objets commencent à peine à être étudiées par les acteurs industriels ainsi que par les régulateurs. Comme souvent lorsqu'il est question de sécurité sur Internet, des mesures qui devront être prises pourront s'articuler suivant 3 axes : sensibilisation aux risques, mesures technologiques et encadrement juridique des technologies.

La sensibilisation et l'éducation des usagers constitueront en effet des volets cruciaux de l'action publique en matière de sécurité de l'Internet des objets. En effet, à la différence des objets traditionnels, les objets connectés constituent des « *portes d'entrées* » à l'intérieur même du domicile ou plus généralement auprès de l'usager et doivent être reconnus comme telles par leurs usagers. Cette prise de conscience des risques inhérents aux objets connectés peut avoir des conséquences pour l'usager qui devra éviter des conduites à risque comme le fait de ne pas utiliser (ou renouveler) des codes de sécurité.

197. *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse* (Nellie Bowles, New York Times, 23 juin 2018) www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Des mesures technologiques doivent aussi permettre une meilleure sécurisation de ces objets connectés en introduisant par exemple des dispositifs de chiffrement pour les objets connectés qui n'en disposent pas. Les constructeurs et concepteurs de services de l'Internet des objets devront aussi concevoir des dispositifs ergonomiques qui prendront en compte la difficulté pour la plupart des usagers de sécuriser leur environnement familier comme s'il s'agissait d'un lieu de travail.

D'autres formes d'utilisation des données issues des objets connectés devront aussi être prises en compte dans le cadre de nouvelles formes de régulations. C'est le cas de la protection contre la dissémination incontrôlée des données issues des objets connectés à des fins de profilage publicitaire, mais aussi politiques. Certaines applications et en particulier certains jeux sur smartphone ainsi ont été conçus exclusivement pour recueillir des informations sur leurs usagers. C'était aussi le cas du quiz de personnalité utilisé par la société *Cambridge Analytica* qui a permis de moissonner les données de plusieurs dizaines de millions d'utilisateurs sur *Facebook*[198].

Ces risques ont aussi été mis en évidence avec des objets connectés qui transmettaient, à l'insu des utilisateurs, des informations sans lien avec leur fonction à des fins de monétisation. Ainsi, Shoshana Zuboff évoque la controverse née autour de l'aspirateur autonome *Roomba* :

> En juillet 2017, l'aspirateur autonome *Roomba* de la société *iRobot*, a fait les gros titres des journaux lorsque le PDG de la société, Colin Angle, a confié à *Reuters* sa stratégie commerciale basée sur l'acquisition de données de la maison intelligente. Cette stratégie incluait une nouvelle source de revenus issue de la vente de plans des pièces de la maison des clients captés grâce aux nouvelles capacités cartographiques de l'aspirateur. M. Angle indiqué qu'*iRobot* pourrait conclure un accord avec *Google*, *Amazon* ou *Apple* pour vendre ces plans dans les

198. *Cambridge Analytica : 87 millions de comptes Facebook concernés* (Le Monde, 4 avril 2018) www.lemonde.fr/pixels/article/2018/04/04/cambridge-analytica-87-millions-de-comptes-facebook-concernes_5280752_4408996.html

> 2 prochaines années. En prévision de cette entrée dans le marché de la surveillance, une caméra, de nouveaux capteurs et un logiciel ont déjà été ajoutés aux aspirateurs *Roomba* haut de gamme, créant la possibilité d'établir une carte combinée à la géolocalisation. Le marché boursier avait récompensé cette perspective de croissance pour *iRobot*, faisant passer l'action de 35 dollars l'année précédente à 102 dollars en juin 2017, ce qui correspondait à une capitalisation boursière de 2,5 milliards de dollars[199].

D'autres fabricants d'objets connectés ont déjà été accusés de recueillir ou de monétiser les données de leurs utilisateurs sans leur consentement. Ainsi, à plusieurs reprises, les constructeurs d'enceintes connectées ont été accusés de conserver des enregistrements issus de leurs utilisateurs[200]. Le plus étrange cas de captation non souhaitée d'enregistrements sonores d'un objet connecté concernait les jouets pour adultes de la société *Lovense*, enregistrements non autorisés que les responsables de la société ont par la suite décrits comme un « *bug mineur* » (sic)[201]...

7.4 Vers une *éthique by design* pour l'Internet des objets européen

Les formes que prendra l'Internet des objets en Europe pourraient avoir des conséquences politiques majeures sur les citoyens et l'ensemble des organisations. Ainsi, pour Shoshana Zuboff : *« Bien qu'il soit possible d'imaginer quelque chose comme « l'Internet des objets » sans le capitalisme de surveillance, il est impossible d'imaginer le capitalisme de surveillance sans quelque chose qui ressemblerait à « l'Internet des objets »»*[202].

Le fait d'introduire une dimension éthique, depuis la conception jusqu'au déploiement de ces technologies, pourrait devenir une autre marque de fabrique de l'Internet des objets européen. Ainsi, l'universitaire Scott

199. *The Age of Surveillance Capitalism* Shoshana Zuboff (Public Affairs, 2019)

200. *Smart talking: are our devices threatening our privacy?* (The Guardian, 26 mars 2019) www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy

201. *Sex toy company admits to recording users' remote sex sessions, calls it a 'minor bug'* (The Verge, 10 novembre 2017) www.theverge.com/2017/11/10/16634442/lovense-sex-toy-spy-surveillance

202. *The Age of Surveillance Capitalism* Shoshana Zuboff (Public Affairs, 2019)

J. Shackelford qui enseigne l'éthique d'entreprise à *l'Université d'Indiana,* prévoit que la cybersécurité et la protection des données deviendront pour les stratégies des entreprises des enjeux de même importance que les démarches liées au développement durable :

> Une autre option que certaines entreprises comme *Eli Lilly* explorent est de ne pas considérer la cybersécurité uniquement comme un coût pour l'entreprise, mais comme un avantage concurrentiel et une responsabilité sociale des entreprises. L'argument avancé est qu'il est dans l'intérêt à long terme des entreprises (ainsi que pour la sécurité nationale) d'adopter une vision large pour le secteur privé des pratiques de gestion des risques afin d'y intégrer des facteurs moins traditionnels, à la manière de ce que les entreprises ont fait en matière de développement durable[203].

« Bien qu'il soit possible d'imaginer quelque chose comme « l'Internet des objets » sans le capitalisme de surveillance, il est impossible d'imaginer le capitalisme de surveillance sans quelque chose qui ressemblerait à « l'Internet des objets »...

Shoshana Zuboff

Ces propos rejoignent ceux de Paul Nemitz, directeur au département de la justice de la Commission européenne, pour qui les questions liées à la protection des données pourraient, à l'instar du développement durable, donner naissance à un secteur industriel en tant que tel. Secteur dans lequel l'Union européenne pourrait occuper une place centrale à l'avenir : « *Le mouvement pour l'écologie, dont l'Europe a été l'initiatrice et qui a fini par engendrer des gains de compétitivité importants pour l'industrie européenne, s'est d'abord heurté (dans les années soixante-dix et quatre-vingt) à des résistances importantes. Il est très possible que nous soyons confrontés à un même mouvement qui partira d'Europe et qui prendra appui cette fois sur la protection des données personnelles* »[204].

203. *The Internet of Things : What Everyone Needs to Know* (Scott J. Shackelford, Oxford University Press 2020)

204. *Europe pivots between safety and privacy online* (Christian Science Monitor, 18 janvier 2015) www.csmonitor.com/World/Europe/2015/0118/Europe-pivots-between-safety-and-privacy-online

CONCLUSION

L'Internet des objets représente un enjeu politique, industriel et technologique majeur pour les acteurs européens. En effet, les technologies des objets connectés sont en mesure de transformer l'ensemble de nos économies mais aussi nos modes de vie et l'organisation de nos démocraties. L'Internet des objets pourrait aussi permettre à l'Europe de faire entrer en synergie les politiques environnementales et les politiques liées à la protection des données. En effet, les technologies de la maîtrise de l'énergie et du contrôle environnemental (que l'on nomme aussi *climate tech*[205]) reposent largement sur l'analyse d'informations issues des capteurs et des objets connectés. À mesure que ces technologies se diffuseront auprès des entreprises mais aussi dans l'espace public, la protection des données issues des objets connectés deviendra un élément clé pour leur acceptabilité et constituera un facteur de différenciation et de confiance pour les technologies européennes au-delà même des frontières de l'Union.

Les grandes plateformes de l'Internet commencent en effet à être confrontées aux limites sociales, politiques et industrielles de leurs modèles économiques « data centrés ». Leur appétit toujours plus grand pour l'accumulation des données personnelles les a en effet conduits à créer des technologies de plus en plus intrusives. À cela s'ajoutent les risques de polarisation des opinions publiques et de dérives autoritaires par le contrôle des données issues des objets connectés. De plus, la concentration des principaux acteurs des technologies et leurs abus de position dominante a conduit les

205. *The State of Climate Tech 2020* (Price Waterhouse Cooper, septembre 2020) www.pwc.com/gx/en/services/sustainability/assets/pwc-the-state-of-climate-tech-2020.pdf

gouvernements des pays développés (et l'ensemble des autres acteurs économiques) à s'élever contre le *statu quo* imposé par les grandes plateformes de l'Internet.

Pour les pays de l'Union européenne, développer un Internet des objets respectueux des données et des citoyens constitue un impératif en termes de souveraineté numérique. Cela représente aussi l'opportunité pour l'Europe de créer une alternative industrielle, politique et sociale aux technologies américaines ou chinoises. En ce sens, reprendre le contrôle de sa destinée technologique constituera pour l'Europe l'un des plus importants défis politiques et industriels de la décennie à venir.

À PROPOS DE L'ISN ET DE L'AFNIC

L'INSTITUT DE LA SOUVERAINETÉ NUMÉRIQUE (ISN)

www.souverainetenumerique.fr

L'*Institut de la Souveraineté Numérique (ISN)* est une association loi 1901 à but non lucratif qui a pour mission de fédérer les acteurs du numérique et, au-delà, les acteurs économiques afin de créer une synergie sur les enjeux liés à la souveraineté numérique européenne. *L'ISN* s'est engagé depuis sa fondation en 2015 à faire la pédagogie et mobiliser les citoyens, et leurs représentants, sur les enjeux de la souveraineté numérique. *L'ISN* considère qu'il est nécessaire de promouvoir la protection de notre cyberespace, au même titre que celle de notre espace terrestre, maritime et aérien. *L'ISN* propose des actions et des mesures technologiques, juridiques et politiques qui permettent de faire valoir la souveraineté numérique sur l'ensemble de nos ressources numériques et en particulier sur nos données. Enfin, *l'ISN* souhaite contribuer à la transformation numérique de l'État afin de permettre de garantir la protection de notre souveraineté et de préserver dans le même temps nos libertés individuelles et collectives.

L'ASSOCIATION FRANÇAISE POUR LE NOMMAGE INTERNET EN COOPÉRATION (AFNIC)

www.afnic.fr

L'*Afnic* est une association à but non lucratif est l'office d'enregistrement désigné par l'État pour la gestion des noms de domaine sous l'extension .fr. L'*Afnic* est un opérateur multi-registres au service des domaines de premier niveau correspondant au territoire national (.fr et ultramarins) et de plusieurs projets français de nouvelles extensions Internet. L'*Afnic* contribue au développement d'un Internet sûr et stable, ouvert aux innovations. L'*Afnic* exerce ses missions dans le respect de l'intérêt général, en associant à ses décisions toutes les parties prenantes (scientifiques, pouvoirs publics, représentants des acteurs privés de l'Internet en France). Premier opérateur en France des services de registre sur Internet, l'*Afnic* se fixe pour objectifs de développer la préférence pour le .fr en France, de contribuer au renforcement de la résilience d'Internet et de diffuser ses expertises auprès de la communauté Internet.

REMERCIEMENTS

Ce rapport a été réalisé par *l'Institut de la Souveraineté Numérique* en partenariat avec *l'Afnic*. Il a été coordonné par **Bernard Benhamou**, secrétaire général de l'ISN, qui a précédemment exercé les fonctions de délégué interministériel aux usages de l'Internet auprès du ministère de la Recherche et du ministère de l'Économie numérique. Bernard Benhamou a aussi coordonné la première conférence ministérielle européenne sur l'Internet des objets lors de la présidence française de l'Union européenne en 2008 après avoir été le conseiller de la délégation française au Sommet des Nations unies sur la Société de l'Information (*SMSI*).

Ce rapport a bénéficié de l'aide de **Pierre Bonis**, directeur général de *l'Afnic* et ses équipes et en particulier **Benoît Ampeau**, directeur des partenariats et de l'innovation et **Lucien Castex**, représentant pour les affaires publiques et le développement des partenariats.

L'ISN et l'AFNIC tiennent à remercier pour leur participation à l'élaboration de ce rapport :

Vincent Audebert
Expert IoT & Telecom
EDF Lab

Olivier Beaujard
Membre du conseil d'administration et président du groupe
de travail sur les affaires réglementaires
LoRa Alliance
Senior Director
Semtech

Paul-Emmanuel Brun
Innovation & IoT Program Leader
Airbus CyberSecurity

Francis Jutand
Directeur Général adjoint
Institut Mines Télécom

Rob van Kranenburg
Fondateur
Internet of Things Council

Sophie Le Pallec
Directrice des affaires publiques et réglementaires
GS1 France

Désirée Miloshevic
Fondatrice de Descon (IoT Ecology Hackathon)
Ancienne Conseillère spéciale du groupe consultatif de la présidence
Forum sur la Gouvernance de l'Internet (IGF) - Nations unies

Michael Nelson
Directeur des affaires internationales et des technologies
Carnegie Endowment for International Peace
Ancien conseiller pour les technologies d'Al Gore, vice-président des États-Unis

Javier Pallero
Directeur des affaires publiques
Access Now

Dr Françoise Roure
Présidente du groupe de travail sur les biotechnologies,
les nanotechnologies et les technologies convergentes (BNCT)
OCDE

Gérald Santucci
Ancien chef de l'unité Future Internet Enterprise Systems & IoT
Commission Européenne

Pierre-Jean Verrando
Directeur
Eurosmart

Achevé d'imprimer en Janvier 2021

Conception et mise en page : batphil@batphil.com

Impression : Imprimerie Compedit Beauregard