L’Internet des Objets Grand Public et la Captation de Données : Menaces Émergentes et Stratégies de Protection de la Vie Privée

7

Dahbia BEN HAMOU - Melek CAY - Victor CETOUT - Koffi DOGNINOUGAN - Yann HADJ-SAADI

Citations

« Le seul système véritablement sécurisé est un système éteint, enfermé dans un bloc de béton et scellé dans une pièce tapissée de plomb avec des gardes armés - et même dans ce cas, j'ai des doutes. »

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."

Gene Spafford, 1989[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**, 2015**[2]

[1] https://en.wikiquote.org/wiki/Gene_Spafford

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

Remerciements

Nous tenons à exprimer notre profonde gratitude à toutes les personnes qui ont contribué à la réalisation de ce mémoire.

Nous remercions tout particulièrement **Monsieur Laurent Barrat** pour son accompagnement précieux, ses conseils avisés et son soutien indéfectible tout au long de ce travail.

Nous tenons à remercier l'**École de Guerre Économique** et en particulier **Monsieur Christian Harbulot**, pour l'opportunité et l'encadrement offerts durant ce parcours.

Nous souhaitons également adresser nos remerciements à tous les experts du domaine qui ont généreusement accepté de nous accorder de leur temps et de partager leur expérience, rendant ainsi possible l'enrichissement de cette étude, en particulier :

- Monsieur **Fréderic CHARLES,** Directeur Stratégie & Innovation chez SUEZ Smart Solutions**.**
- Monsieur **Régis Chatellier**, Responsable d'études prospectives chez CNIL.
- Monsieur **Bernard BENHAMOU**, Secrétaire général de l'institut de la souveraineté numérique.
- Monsieur **Stéphane FERRER,** DPO-Conformité RGPD, Fondateur RGPD-SF
- Madame **Anne FAURE**, Cheffe de Projet Économie Numérique à France Stratégie
- Monsieur **Gérôme BILLOIS**, Associé et Directeur de la practice Cybersécurité, Wavestone.
- Monsieur **Richard Coffre**, Chef de projet transverse à l'Afnic, membre de l'ARCSI
- Monsieur **Fabrice BRU**, Directeur cybersécurité "Groupement Les Mousquetaires" et Administrateur du CESIN
- Monsieur **Julien FOURNIER**, Directeur de missions chez ITNOVEM

Notre reconnaissance va également à l'ensemble de **notre promotion**, pour sa solidarité, son soutien constant et sa bienveillance tout au long de cette aventure.

Enfin, nous remercions toutes les personnes qui nous ont soutenus de près ou de loin dans ce projet. Leur appui a été une source de motivation inestimable.

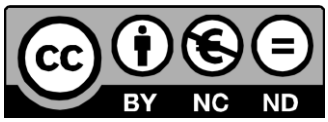


Table des matières

Citations 2

Remerciements 3

Table des illustrations 7

Glossaire 9

I. Introduction 11

II. L'IdO Grand public : Définition, Architecture et Vulnérabilité 14

II.1 Définition de l'Internet des Objets 15

II.2 Architecture fonctionnelle de l'internet des objets 16

II.2.1 La couche perception 17

II.2.2 La couche réseau 19

II.2.3 La couche traitement de la donnée 23

II.2.4 La couche applicative 24

II.2.5 La couche sécurité 25

II.3 Menaces et vulnérabilités 26

II.3.1 Les types d'attaques 26

II.3.2 Les vulnérabilités et scénarios d'attaques des IdO 28

II.3.3 Risques liés à l'utilisation des objets connectés grand public 30

II.4 Réponses aux défis de l'Internet des Objets 33

III. État du marché de l'IdO : Tendances actuelles et projections futures 36

III.1 Taille et croissance du marché des IdO 37

III.2 Moments clés de l'évolution de l'Internet des objets 39

III.3 Facteurs clés de croissances des IdO 39

III.3.1 Segmentation du marché de l'IdO par région 41

III.3.2 Segmentation du marché de l'IdO par application 42

III.3.3 Segmentation du marché de l'IdO par technologie 44

III.4 Les tendances émergentes 45

IV. Législation et réglementation de l'IdO : Cadres juridiques et enjeux 48

IV.1 Comprendre la réglementation des Objets Connectés 50

IV.2 Au Royaume Uni 52

IV.2.1 Loi sur la sécurité des produits et des infrastructures de télécommunications 52

IV.2.2 En Europe 53

IV.2.3 R*èglement* délégué (UE) 2022/30 complétant la Directive dite RED 53

IV.2.4 Règlement Général sur la Protection des Données (RGPD 95/46/CE) 54

IV.2.5 IV.3.3 La loi sur la cybersécurité de l'Union européenne 54

IV.3.4 La proposition de loi de l'Union Européenne sur la cyber-résilience 56

IV.3 Aux Etats-Unis d'Amérique 57

IV.3.1 Loi américaine sur l'amélioration de la cybersécurité des (IdO)..... 57
IV.3.2 Loi californienne sur la cybersécurité de l'IdO SB-327 58
IV.3.3 Marque de confiance en cybersécurité des États-Unis. 59
IV.3.4 Le CLOUD Act 60

IV.4 Perspectives et évolutions de la Réglementation des Objets (IdO) Grand Public 62

V. Manœuvres stratégiques autour de l'internet des objets : Chine, Etats-Unis, Israël et Inde 65

V.1 Les géants de l'IdO : Rivalités sino-américaines 65

V.1.1 Une stratégie libérale versus une stratégie d'Etat-Parti centralisée 65
V.1.2 V.1.2 La donnée, matière première du capitalisme et du communisme de surveillance de masse 69
V.1.3 Un cas d'école : Le crédit social chinois, mythe ou réalité 78

V.2 Stratégie d'Israël 80

V.2.1 Stratégie générale incluant les objets connectés et la captation de données 80
V.2.2 Relation entre les État -Unis et l'État d'Israël 85
V.2.3 V.2.3 Le Projet NIMBUS 86
V.2.4 Les points conclusifs 87

V.3 Stratégie de l'Inde 88

V.3.1 Dans l'univers du numérique 89
V.3.2 V.3.2 L'IdO de l'Inde 89
V.3.3 V.3.3 Cybersécurité et protection des données personnelles 91
V.3.4 Le RGPD Indien 92

VI. Stratégies pour un Internet des objets plus sûr : Recommandations et perspectives 95

VII. VII. Conclusion 108

VIII. Références bibliographiques 111

IX. AnnexeS 117

IX.1 Annexe 1 : Cas réels de cyberattaques et violations de la vie privée 117

IX.2 Annexe 2 : Sélection de partenariats sino-européens dans le domaine de l'IdO (Traduit De L'anglais) 119

IX.3 Annexe 3 : Impact du dispositif de contrôle sur la destination des données (Divers chemins et différents acteurs). 120

IX.4 Annexe 4 : Exemples de labels de confiance IdO – Japon et Singapour. 124

Table des illustrations

Figure 1 : Objets connectés d'une maison intelligente 14
Figure 2 : Architecture de l'Internet des Objets 15
Figure 3 : – Modèle de référence de l'IdO par l'UIT 16
Figure 4 : Architecture topologique d'un lampadaire intelligent 17
Figure 5 : COMPOSANTE SOFTWARE D'UN OBJET CONNECTE 18
Figure 6 : ARCHITECTURE FONCTIONNELLE D'UN RFID..... 19
Figure 7 : Architecture d'un réseau LoRa 19
Figure 8 : ARCHITECTURE D'UN RESEAU LPWAN 20
Figure 9 : COMPARATIF DES RESEAUX IDO 21
Figure 10 : Comparaison des réseaux LPWAN Cellulaires 23
Figure 11 : Fonctionnement d'un CoAP 24
Figure 12 : Protocole de messageries au niveau des IdO 25
Figure 13 : Analyse des Vulnérabilités dans les Foyers Intelligents 28
Figure 14: IdO les plus populaires dans une maison intelligente 29
Figure 15 : Appareils IdO les plus vulnérables en 2022 30
Figure 16 : malwares IdO selon Zscaler, janv-juin 2023 31
Figure 17 : Nombre et prévision des dispositifs (IdO) dans le monde 37
Figure 18 : CA annuel de IdO dans le monde de 2020 à 2030 en milliards $ 38
Figure 19 : Nombre (IdO) en millions par région de 2020 à 2030 42
Figure 20 : Différentes connectivités des IdO 44
Figure 21 : Couverture des IdO Sidewalk aux USA 45
Figure 22 : Illustration des objets Connectés (IdO) Grand Public 48
Figure 23 : Réglementations Mondiales des Objets Connectés 51
Figure 24 : Logo CE 53
Figure 25 : Nombre de partenaires et d'accords de coopération de la Chine (2002-21) 68
Figure 25: Capture d'écran de l'application WeChat 79
Figure 26: TVL PARTNERS 2015 82
Figure 27: Part des investisseurs étrangers sur les 5 dernières années 83
Figure 28: ABITBOL ASSOCIES 84
Figure 29 : Tendances IdO 2020 en Inde 91
Figure 30 : Projet de label de cybersécurité de l'UE..... 101
Figure 31: Label finlandais de sécurité de l'information dédié à l'IdO 102
Figure 32 : Projet de label IT en Allemagne 103

Mots-clés : Internet des objets, Ubiquité, données personnelles, vie privée, collecte massive de données, menaces, ciblage marketing, influence opinion publique, surveillance grande échelle, sécurité, cybersécurité, stratégie

EXECUTIVE SUMMARY :

Internet-connected devices, now ubiquitous in our daily lives, provide undeniable convenience but also carry hidden risks. A lack of awareness, insufficient regulation, and a certain carelessness expose our personal data and privacy to numerous threats. This information can be exploited by data brokers for marketing purposes or fall into the hands of cybercriminals for malicious use. Additionally, some governments may access this data to influence public opinion or conduct large-scale surveillance programs. Given this massive data collection, the issue of privacy and security becomes critical, requiring greater vigilance and stricter laws to protect users. We have studied all the publications on this topic in France, as well as the strategies of the main providers of consumer IoT and the biggest data predators. We drew inspiration from them to propose strategic recommendations aimed at creating a safer and more privacy-respecting consumer IoT ecosystem.

Keywords : Internet of Things, Ubiquity, personal data, privacy, massmassive data collection, threats, marketing targeting, public opinion influence, large-scale surveillance, security, cybersecurity, strategy

Glossaire

Acronyme	Définition
ADEME	Agence de l'Environnement et de la Maîtrise de l'Énergie
AFNIC	Association Française pour le Nommage Internet en Coopération
AFP	Agence France Presse
AIE	Agence Internationale de l'Energie
ANCC	Autorité Nationale de Certification de Cybersécurité
ANSSI	Agence nationale de la sécurité des systèmes d'information
ARCEP	Autorité de Régulation des Communications Electroniques, des Postes
BATX	Baidu, Alibaba,Tencent, Xiaomi
BLE	Luetooth Basse Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik (office fédéral allemand pour la sécurité de l'information)
CCDS	Connected Consumer Device Security Council
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Electrotechnique
CEPD	Comité Européen de la Protection des Données
CERT-in	Indian, Computer Emergency Response Team
CIA	Central Intelligence Agency
CISPE	Cloud Infrastructure Services Providers in Europe
CLOUD	Dans le cloud act,
CLS	Cybersecurity Labelling Scheme
CNIL	Commission nationale de l'informatique et des libertés
CNUCED	Conférence des Nations Unies sur le Commerce et le Développement
CoAP	Constrained Application Protocol
DDoS	Distributed Denial of Service
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes
DoS	Denial of Service
DPDPA	Digital Personal Data Protection Act
DPO	Protection Des Données
DSL	Data Security Law
ECCG	European Cybersecurity Certification Group

ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute (Institut européen des normes de télécommunications)
EU	European Union
FCC	Federal Communications Commission
GAFAM	Google, Apple, Facebook, Amazon et Microsoft
GPS	Global Positioning System
IA	Intelligence Artificielle

IdO (IoT)	Internet des objets (Internet of Things)
IEEE	Institute of Electrical and Electronics Engineers
IFRI	Institut Français des Relations Internationales
LAN	Local Area Network
LPWAN	Low Power Wide Area Network
M2M	Machine to Machine
MQTT	Message Queuing Telemetry Transport
NASSCOM	National Association of Software and Service Companies
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCDE	Organisation de coopération et de développement économiques
OPSS	Office for Product Safety and Standards
OWASP	Open Web Application Security Project
PAN	Personal Area Network
PCC	Parti Communiste Chinois
PIB	Produit Interieur Brut
PIPL	Personal Information Protection Law
PSTI	Telecommunications Infrastructure
R&D	Recherche & Développement
RFID	Radio frequency identification
RGPD	Règlement général sur la protection des données
SCS	Système de Crédit Social
UNAF	Union nationale des associations familiales
WAN	Wide Area Network

Le Monde de l'IdO
Numéro 2024.20/09/2024

FUITE DE DONNÉES PERSONNELLES ET MÉDICALES DE 65 MILLIONS DE FRANÇAIS !

Botnet IdO massif

Paris, 20 sept. 2024 (AFP) – Les données personnelles et médicales de 65 millions de Français ont été révélées sur le DarkWeb, marquant ainsi la plus importante fuite de données de l'histoire du pays. Ce contexte explique le message d'alerte envoyé récemment par l'assurance maladie à tous les assurés, qui mentionnait une suspicion de fuite de données et rappelait à la vigilance.

Bien que cette attaque n'ait pas été revendiquée, plusieurs faisceaux d'indices suggèrent l'implication d'acteurs étatiques hostiles. Les premiers éléments d'enquête révèlent que cette attaque a été minutieusement préparée et de longue date.

Complicités internes soupçonnées

D'après nos informations, le mode opératoire serait très sophistiqué et s'appuierait sur une combinaison d'attaque en déni de service (DDoS) par le biais d'un botnet d'objets connectés grand public vulnérables, suivie d'une opération de phishing ayant aboutie à la récupération de plusieurs données d'authentification qui a permis une latéralisation de plusieurs mois et enfin une exfiltration des données sur plusieurs semaines afin de ne pas éveiller les soupçons et échapper aux dispositifs de surveillance et de détection.

Les enquêteurs nous ont indiqué qu'une telle attaque n'aurait pas été possible avec autant d'impact sans des complicités internes.

Le communiqué officiel du ministère de la santé et de l'assurance maladie se veut plus rassurant malgré la gravité de la situation et indique que très peu d'informations médicales auraient été compromises, et que seules des informations personnelles auraient été exposées.

www.afp.fr 9

Comme vous l'aurez deviné, heureusement, cette dépêche est bien fictive... pour l'instant…

Ce scénario est délibérément provocateur et les spécialistes en cybersécurité ne manqueront pas de dénoncer son invraisemblance. Bien que techniquement complexe, une telle attaque reste théoriquement possible et à la portée d'un acteur étatique hostile.

Pourtant, des attaques similaires à grande échelle ont déjà eu lieu ; l'une en 2015 dont a été victime Anthem[1], l'une des plus grandes compagnies d'assurance santé aux Etats-Unis, ayant permis d'exfiltrer les données de 78,8 millions d'assurés ; l'autre en 2018 dont a été victime SingHealth[2], la plus grande base de données de santé de Singapour, et qui a abouti au vol des données de 1,5 millions de patients, y compris celles du premier ministre.

Le scénario de la dépêche fictive illustre le tremplin que pourraient constituer les dispositifs vulnérables de l'internet des objets (IdO) et l'effet de diversion auquel ils contribuent pour détourner l'attention et la vigilance du vrai objectif visé par l'attaque.

Ces dernières années, plusieurs rapports ont été produit et traitant de l'internet des objets dans toute sa diversité et sa spécificité et notamment les menaces et les risques auxquels il nous expose, par sa prolifération rapide et la surface d'attaque immense qu'il offre. Néanmoins, depuis 2022, ce sujet semble avoir été complètement éclipsé par des sujets plus « à la mode » come l'intelligence artificielle (IA) et la Blockchain, pour ne citer que ces deux technologies.

Pourtant l'IdO est partout et a investi tous les pans de l'économie et de la société. A travers notre mémoire, nous nous sommes fixés comme ambition de remettre en lumière cet écosystème et d'évaluer les risques et les menaces qu'il fait peser sur nos données personnelles et notre vie privée.

Dans un souci d'efficacité et de clarté, nous avons choisi de nous focaliser sur l'IdO grand public, notamment en lien avec la domotique, le bien-être, les dispositifs de géolocalisation et les jouets numériques.

Avant d'aborder la réglementation régissant cet écosystème et de présenter les stratégies de quelques pays triés sur le volet, nous avons souhaité proposer notre propre définition de l'internet des objets, en complément des nombreuses autres déjà existantes. En effet, il n'existe pas de définition officielle consensuelle et c'est dire toute la complexité du sujet.

Une fois cette définition posée, nous enchaînerons avec une présentation de quelques notions techniques essentielles, ainsi qu'un état du marché de l'IdO.

Nous terminerons par l'exposé de quelques recommandations d'ordre stratégiques[3], pour un écosystème IdO grand public plus sûr et respectueux de nos données personnelles, inspirées des rapports que nous avons évoqués plus haut, de nos lectures et des leçons apprises en étudiant les stratégies de puissances telles que la Chine, les Etats-Unis, l'Inde et Israël.

[1] https://www.bankinfosecurity.com/anthem-update-a-7946

[2] https://www.todayonline.com/singapore/hackers-stole-data-pm-lee-and-15-million-patients-major-cyberattack-singhealth

[3] Pour des recommandations plus pratiques et opérationnelles, vous reporter à la partie III relative à la réglementation qui les aborde.

II.L'Internet des objets grand public : Définition, architecture et vulnérabilités

II. L'IDO GRAND PUBLIC : DEFINITION, ARCHITECTURE ET VULNERABILITE

En évoquant l'Internet des objets en général, et ceux destinés au grand public en particulier, on se rend rapidement compte que l'imaginaire des auteurs et des cinéastes s'est transformé en réalité. Dans sa nouvelle « Il viendra des pluies douces[4] », publiée pour la première fois en 1950, Ray Bradbury[5] décrit une maison futuriste "intelligente", située en 2026, comme une merveille automatisée, accomplissant des tâches comme la cuisine, le nettoyage, et même la lecture de poésie. Dans les années 2000, la domotique était très présente dans les blockbusters[6] tel qu'Iron Man et son légendaire assistant connecté Jarvis[7]. Dans le monde des technologies, Mark Weiser, le défunt Directeur du Centre de recherches de Xerox à Palo Alto, préfigurait notre avenir lorsqu'il inventa, en 1991, le terme « d'informatique ubiquitaire », précurseur de l'Internet des objets. Il déclara que « *Les technologies les plus profondément enracinées sont les technologies invisibles. Elles s'intègrent dans la trame de la vie quotidienne jusqu'à ne plus pouvoir en être distinguées* ». Il ajouta également, que « *Des milliards d'objets connectés au réseau auraient le potentiel de changer profondément l'usage d'Internet en le rendant omniprésent dans la vie quotidienne ».*

Figure 1 : Objets connectés d'une maison intelligente
Source: (PDF) Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures (researchgate.net)

Aujourd'hui, les milliards d'objets connectés, ou Internet des Objets (IdO), ont le potentiel de révolutionner notre utilisation d'Internet en le rendant omniprésent. Ces dispositifs peuvent automatiser des tâches quotidiennes telles que la gestion de l'énergie de nos maisons, optimiser les processus industriels, et gérer les soins de santé à distance. Les données générées par ces objets permettent d'améliorer les services, de prédire les tendances et de guider les décisions. Par exemple, les capteurs des villes intelligentes peuvent réguler le trafic et réduire la consommation d'énergie. Les IdO augmentent

[4] Titre en Anglais "There Will Come Soft Rains"
[5] Ray Bradbury, né le 22 août 1920 à Waukegan, Illinois, et décédé le 5 juin 2012 à Los Angeles, Californie, était un écrivain américain renommé, surtout connu pour ses œuvres de science-fiction et de fantastique.
[6] Blockbusters sont des films à gros budget, conçus pour générer des revenus importants au box-office et caractérisés par des effets spéciaux spectaculaires.
[7] JARVIS est « Just A Rather Very Intelligent System » ce qui peut se traduire par "Juste un Système Plutôt Très Intelligent".

également notre confort et notre sécurité grâce à des systèmes de sécurité domestique et des appareils de santé connectés. Ils offrent des expériences utilisateur personnalisées et interactives, comme les assistants vocaux. Enfin, en optimisant l'utilisation des ressources, les IdO favorisent une économie durable et la réduction de l'empreinte carbone. L'Internet des objets promet ainsi de rendre Internet omniprésent, intégré et utile dans notre vie quotidienne. Dans le cadre de ce mémoire, nous avons retenu une définition inspirée de celles de l'Arcep et de France Stratégie, davantage orientée vers la protection des données personnelles et la cybersécurité, tout en y intégrant notre propre vision centrée sur la donnée et sa protection.

II.1 DEFINITION DE L'INTERNET DES OBJETS

L'Internet des objets (ou IoT pour Internet of Things) est un ensemble d'objets connectés collectant et échangeant des données plus ou moins sensibles, dont l'objectif de sécurité peut varier de faible à fort, via des technologies de réseaux qui se déclinent en fonction du domaine d'application et de la portée souhaitée. Nous le déclinons selon une architecture modulaire adaptative en fonction du contexte et des objectifs d'utilisation :

- Des **objets physiques** qui possèdent des capteurs connectés de manière plus ou moins sécurisée, dotés de capacités de calcul locales ou déportées. Véritables nœuds gardiens de cet écosystème ;
- Des **réseaux de communication numériques** filaires ou non filaires qui permettent d'acheminer les données issues de ces objets ;
- Des **espaces de stockages** distants pour les données recueillies ;
- Ces espaces hébergeant ou pas, des **applications** pour leur traitement à des fins d'exploitation décisionnelles.

Pour résumer, une infrastructure reliant les objets connectés via les réseaux au cloud, d'où ils sont gérés et où leurs données sont stockées et analysées, pour être ensuite exploitées en vue de futurs services.

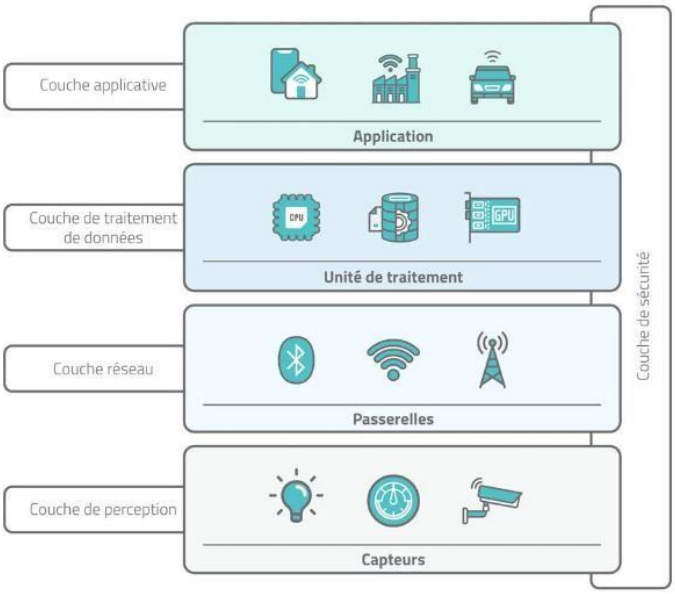


Figure 2 : Architecture de l'Internet des Objets
Source : https://iotindustriel.com/iot-iiot/architecture-iot-lessentiel-a-savoir/

II.2 ARCHITECTURE FONCTIONNELLE DE L'INTERNET DES OBJETS

Les dispositifs de l'Internet des objets varient en fonction des équipementiers, des technologies mises en œuvre, des protocoles utilisés, ainsi que des services utilisateurs fournis.

Selon le modèle de référence de l'Union Internationale des Télécommunications, l'architecture de l'IdO comprend quatre couches auxquelles sont associées des capacités de gestion et de sécurité[8] :

couche application;
couche de prise en charge des services et des applications;
couche réseau; couche dispositif.

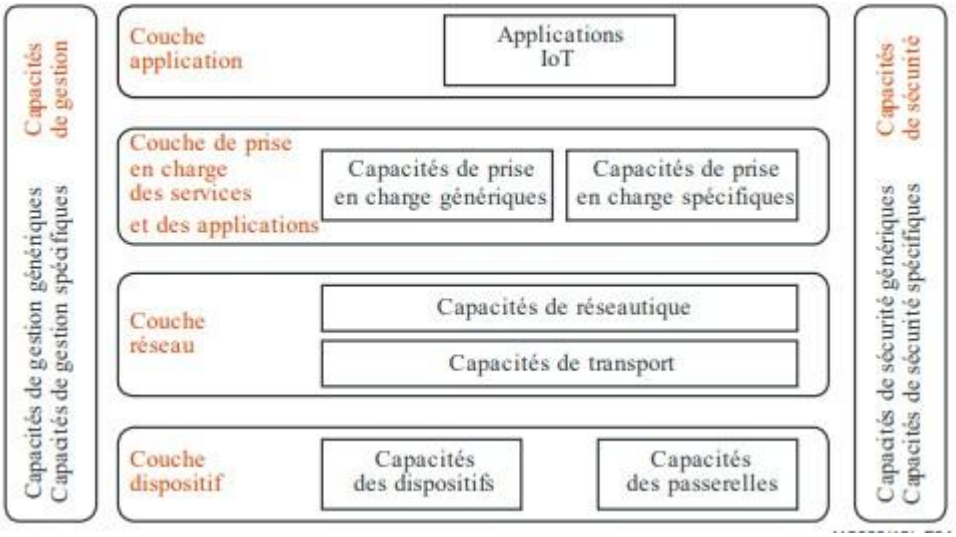


Figure 3 : – Modèle de référence de l'IdO par l'UIT
Source :UIT , Union International des télécommunications

Pour mieux cerner cette architecture technique prenons l'exemple qui suit de l'architecture d'un lampadaire intelligent[9].

[8] UIT-T: « Infrastructure mondiale de l'information, protocole internet et réseaux de prochaines génération » Y.2060, 2012, p 13

[9] https://iotindustriel.com/iot-iiot/architecture-iot-lessentiel-a-savoir/

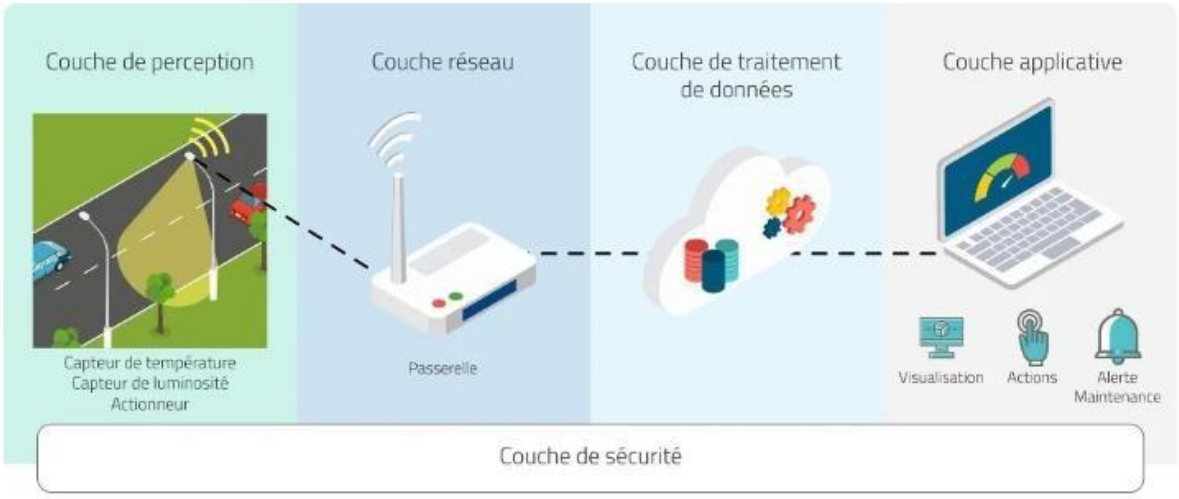


Figure 4 : Architecture topologique d'un lampadaire intelligent
Source : https://iotindustriel.com/iot-iiot/architecture-iot-lessentiel-a-savoir/

II.2.1 La couche perception

Cette couche constitue la fonction principale d'un dispositif IdO. Elle est chargée de convertir les signaux analogiques collectés du monde physique par les objets connectés en données numériques, et vice versa. Elle est également responsable de la collecte des informations, effectuée à l'aide de divers appareils tels que des cartes à puce, des identificateurs de radiofréquence (RFID), ainsi que des réseaux de lecteurs et de capteurs.

Cette couche regroupe différents objets physiques dotés de capteurs, de modules et/ou d'actionneurs, qui agissent comme un pont entre le monde réel et le monde numérique.

- **Les capteurs**

Ils permettent de recueillir des informations provenant du monde physique et les transmettent vers le système informatique. Ils traduisent une grandeur physique en un signal électrique, qui est ensuite numérisé avant d'être envoyé au système informatique.

Par exemple, un capteur de température convertit l'amplitude de la température en une tension électrique. Cette tension est ensuite numérisée et transmise aux couches supérieures.

Les grandeurs couramment mesurées incluent, entre autres : les systèmes à deux états (0,1), (fermé, ouvert), (éteint, allumé), la fréquence cardiaque (cardiofréquencemètre), le comptage d'impulsions (tachymètre), la température, la pression, la luminosité, la position et la vitesse.

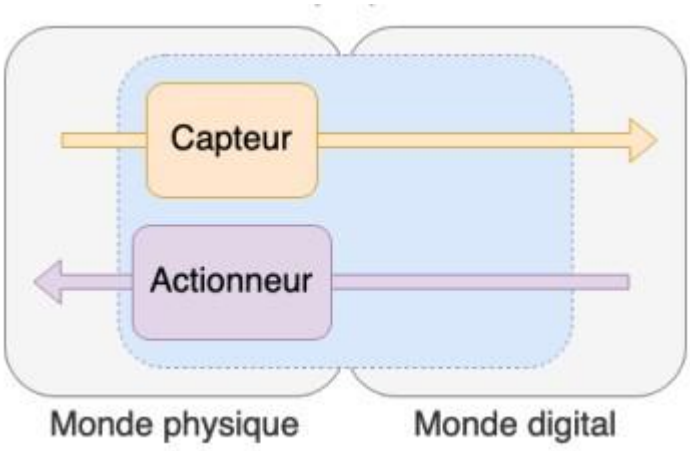


Figure 5 : COMPOSANTE SOFTWARE D'UN OBJET CONNECTE

- **Les actionneurs**

Ils traduisent les signaux électriques provenant du système IdO en actions physiques, c'est-à-dire qu'ils modifient leur état.

Par exemple, un actionneur peut fermer un robinet d'eau laissé ouvert par oubli du propriétaire de la maison.

Les actionneurs couramment utilisés incluent : l'allumage d'un éclairage, le déclenchement d'un avertisseur sonore, l'activation d'une machine, la génération de mouvements, la commande de robots, le contrôle de moteurs, et la régulation de débits (air, pression, liquides, etc.).

- **Identification par radiofréquence (RFID)**

La RFID est un type de technologie sans fil qui utilise des ondes radio pour identifier et suivre des objets. La technologie comprend trois composants : une étiquette ou un transpondeur RFID, un Lecteur RFID, et un système informatique. L'étiquette RFID contient une petite puce et une antenne qui, ensemble, stockent et transmettent des données au lecteur RFID. Le lecteur, à son tour, utilise des ondes radio pour communiquer avec l'étiquette et récupérer les données stockées. Cela permet à la RFID de fournir un suivi en temps réel et des capacités d'identification, améliorant l'efficacité, la précision et la sécurité.

Chaque étiquette électronique RFID a un identifiant unique appelé code de produit électronique (EPC) qui est le seul identifiant de recherche attribué à chaque cible physique. Des informations supplémentaires sur le produit sont données par une suite de chiffres qui lui sont imposés tels que le fabricant et la catégorie de produit avec sa date de fabrication et sa date d'expiration[10], etc.

[10] Younes Abbassi, Habib Benlahmer. Un aperçu sur la sécurité de l'internet des objets (IOT). Colloque sur les Objets et systèmes Connectés - COC'2021, IUT d'Aix-Marseille, Mar 2021, MARSEILLE, France. ffhal-03593723f

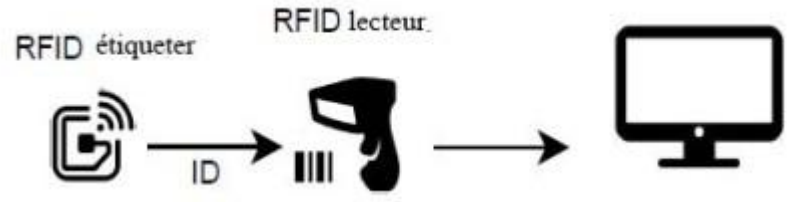


Figure 6 : ARCHITECTURE FONCTIONNELLE D'UN RFID

Les capteurs sans fil

Les capteurs sans fil jouent un rôle essentiel dans l'IdO en fournissant des services de détection et de communication. Un réseau de capteurs sans fil (WSN : Wireless Sensor Networks) se compose d'un grand nombre de capteurs intelligents déployés dans des environnements éloignés pour détecter et recueillir des données. Les données détectées sont transmises par une ou plusisieurs passerelles/stations de base.
En fonction de l'objet de l'étude et des résultats attendus, un seul réseau de capteurs peut être déployé ou couplé avec d'autres réseaux de capteurs.

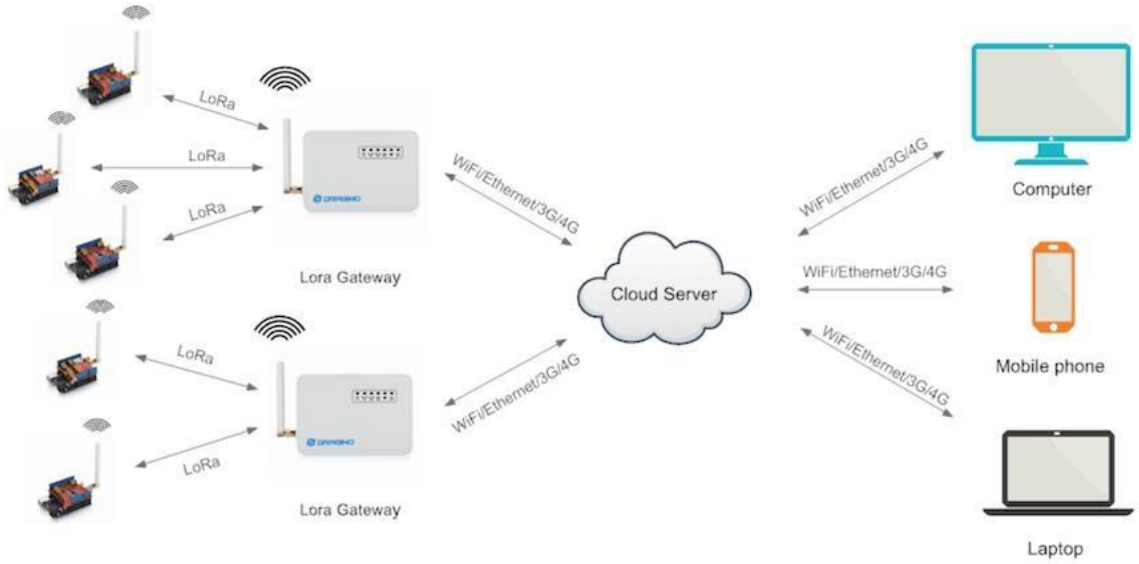


Figure 7 : Architecture d'un réseau LoRa
Source : http://cedric.cnam.fr/~bouzefra/

II.2.2 La couche réseau

Les données collectées, par tous ces appareils au niveau de la couche de perception, doivent être transmises et traitées. La couche réseau est chargée de la transmission de ces données et s'appuie sur un service de télécommunication. Celui-ci peut être filaire ou non, en fonction des contraintes techniques de déploiement ou selon un choix stratégique lié au type d'application utilisée et ou en fonction du débit ou de la portée disponible.

Suivant la couverture géographique, nous pouvons distinguer plusieurs types de réseaux IdO.

- WAN (Wide Area Network) : un réseau de plusieurs dizaines de kilomètres.
- LPWAN (Low Power Wide Area Network) : réseau de plusieurs dizaines de kilomètres (2 km en Ville 20 Km en Campagne) mais utilisant peu d'énergie. LPWAN est une nouvelle classe de réseau développé spécialement les objets connectés compte tenu de leur contrainte en mémoire et en consommation d'énergie. Nous pouvons la subdiviser en 02 catégories : LPWAN Cellulaire (LTE-M, Nb-IoT, Ec-GSM-IoT) et LPWAN non cellulaire (LoRaWAN, Sigfox, Weightless, etc).

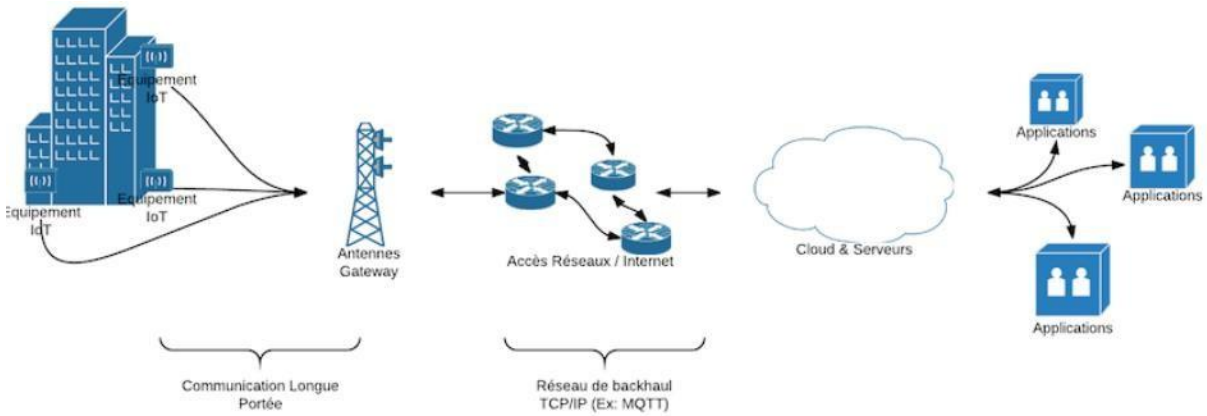


Figure 8 : ARCHITECTURE D'UN RESEAU LPWAN
Source : INRA, TIC2019_INRA-Reseau-LoRA_2019.pdf - M o n t p e l l i e r

- Personal Area Network (PAN) : le réseau de quelques mètres (Bluetooth)
- Local Area Network (LAN) : le réseau Internet privé de votre domicile ou de votre entreprise (Wifi)
- Satellite : un réseau pouvant atteindre plusieurs dizaines de milliers de kilomètres ; idéal pour la couverture des zones les plus reculées et isolées.

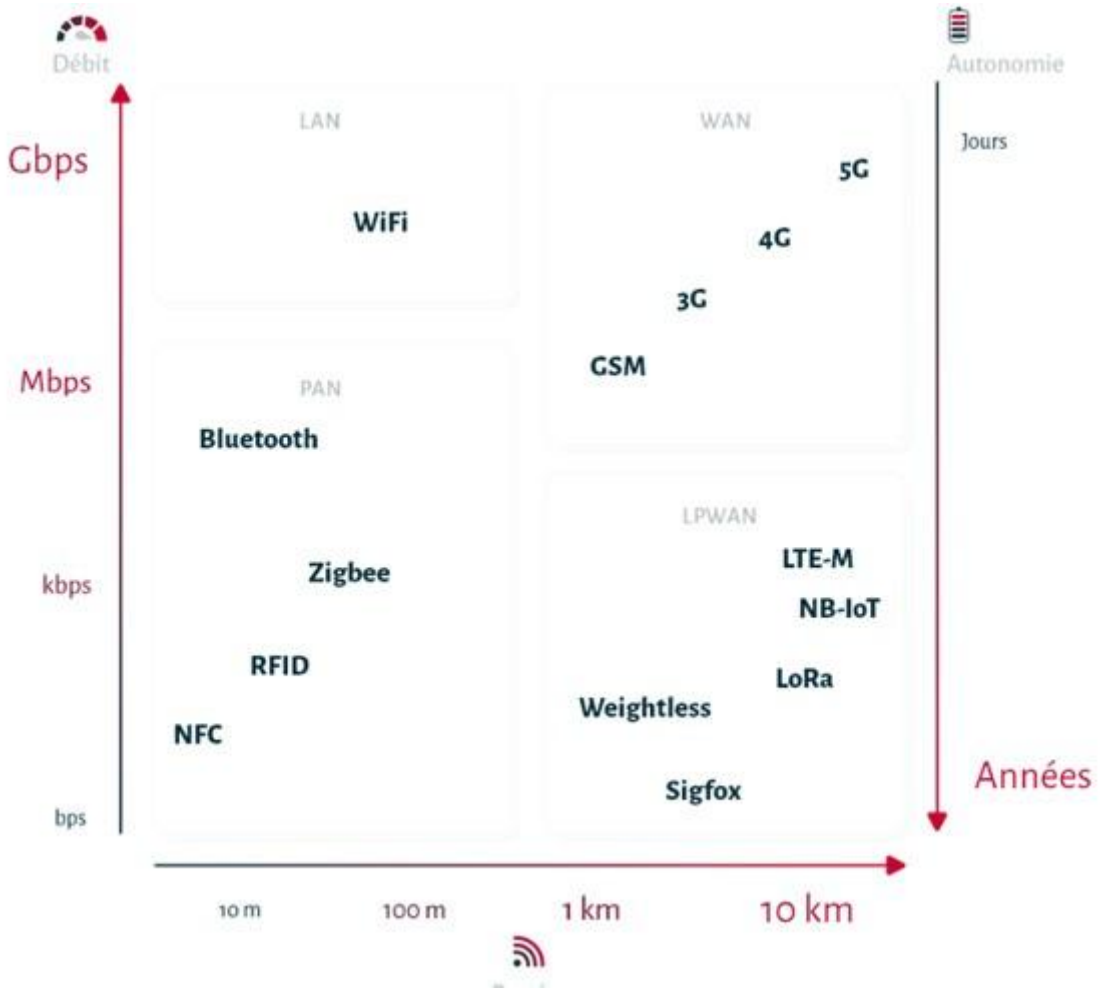


Figure 9 : COMPARATIF DES RESEAUX IDO

Source : www.matooma.com/fr/s-informer/actualites-iot-m2m/m2m-comment-connecter-vos-objets

Les technologies de communication largement utilisées en IdO sont : RFID, ZigBee, Bluetooth basse énergie (BLE), 6LoWPAN, Sigfox, NB-IoT, LTE-M et le réseau étendu à longue portée (LoRaWAN), Z-Wave.

a. Bluetooth

La technologie la plus utilisée par le grand public sous licence libre et basée sur la norme IEEE 802.15.1 Sa consommation d'énergie est relativement faible ainsi que sa portée (environ 10 mètres). Elle possède une bande passante intermédiaire (entre 1 et 3 Mb/s) mais amplement suffisante pour la plupart des utilisations classiques.

b. Bluetooth basse énergie (BLE)

BLE est une technologie de communication à courte portée qui réduit la consommation d'énergie comparé au Bluetooth classique. Elle est également basée sur la norme IEEE 802.15.1[11] et est largement utilisée dans les applications envoyant un volume réduit de

[11] IUT, Les fondamentaux de l'IoT, PRIDA, 24/08/2020

données comme dans les maisons intelligentes et domotique (serrures intelligentes, éclairage intelligent, capteurs...), dans le domaine de la Santé (moniteurs d'activité,

cardiofréquencemètres, glucomètres…), en contrôle industriel et automatisation et dans les systèmes d'accès et de contrôle d'identité, etc.

Sa portée tourne entre 50 -150 en vol d'oiseau avec des temps de latence 15 fois plus courts que Bluetooth et un débit de 1 Mbit/s. Il est toutefois à noter que les 02 technologies Bluetooth et BLE ne sont pas compatible.

c. ZigBee

La technologie ZigBee est conçue pour les communications sans fil de courte portée. Elle peut être utilisée dans les maisons, les compteurs et dans les dispositifs de soins de santé intelligents.
Son fonctionnement est similaire au Bluetooth mais dédié à l'IoT. Elle consomme peu d'énergie, et est fait pour envoyer de petits volumes de données (entre 20 et 250 Kb/s). Elle permet d'utiliser chaque objet comme "rallonge de connexion".
Par exemple, l'ampoule connectée de votre salon va permettre de connecter l'ampoule de votre chambre, comme un relai jusqu'au "hub", branché au réseau Internet.[12]

a. Z-Wave

Z-Wave est une technologie télécoms radio fréquence à faible consommation d'énergie principalement conçue par Z-Wave Alliance ZAD12837/ITU-T G.9959 pour la domotique et les produits tels que les contrôleurs de lampe ou les capteurs. Elle utilise la bande de fréquence de 868,42 MHz en Europe, 908 MHz aux US, et d'autres fréquences suivant les bandes 900 MHz ISM des régions ce qui réduit les interférences avec les réseaux Wi-Fi.

Elle peut s'étendre jusqu'à 30 m en espace clos et jusqu'à 100 m en espace libre avec un débit de données varie entre 9,6 Kbps et 100 Kbps[13].

b. IPv6 LoW Power wireless Area Networks (6LoWPAN)

6LoWPAN est une combinaison de deux protocoles : Internet Protocol version (IPv6) et LowPower Wireless Personal Network (LoWPAN). Elle a été conçue (Standard IETF–RFC 4944) pour permettre à IPv6 d'intégrer les appareils contraints et les réseaux 802.15.4 qui les interconnectent.

Elle permet d'atteindre un débit 250 kbit/s et une couverture d'environ 10 à 100 mètres selon l'environnement et des obstacles présents. Les cas d'usage les plus courants de 6LoWPAN sont la maison intelligente, l'agriculture intelligente et l'IdO industriel.

[12] https://www.matooma.com/fr/s-informer/actualites-iot-m2m/m2m-comment-connecter-vos-objets

[13] IUT, Les fondamentaux de l'IoT, PRIDA, 24/08/2020

c. LoRaWAN

LoRaWAN est un protocole de communication longue portée conçu pour les applications IdO à faible puissance et évolutives. Un réseau LoRaWAN est constitué d'appareils finaux, de passerelles et d'un serveur unique dans une topologie en étoile ou en étoile de l'étoile.
Les périphériques finaux peuvent communiquer avec une ou plusieurs passerelles en utilisant le schéma ALOHA (une passerelle multi-signal haute performance, permettant l'échantillonnage et l'analyse d'une grande variété de signaux provenant de nombreux

---

types de capteurs) par le biais des liens à un saut. Les passerelles sont connectées au serveur du réseau via le protocole Internet. Les communications sont bidirectionnelles et initiées par le dispositif d'extrémité.
En termes de débit, la fluctuation est entre 290bps – 50kbps avec une portée pouvant atteindre jusqu'à 15 km en zone rurale et jusqu'à 5 km en zones urbaines[14].

d. Sigfox

La technologie Sigfox fait partie de la famille des LPWAN. Elle utilise la bande de fréquence radio 868 à 869 MHz et 902 à 928 MHZ selon les pays avec un débit variable entre 100 à 600 bits/s et une couverture sur de longues distances, allant jusqu'à 50 km en zone rurale et 10 km en zone urbaine.

e. LTE-M, Nb-IoT, Ec-GSM-IoT

Le NB-IoT, Ec-GSM-IoT et le LTE-M représentent la réponse des opérateurs de réseaux cellulaires face à la concurrence des solutions de connectivité LPWAN non cellulaire tels que LoRa et Sigfox.
Ils constituent avec 5G les réseaux privilégiés dans le développement de l'Internet des Objets se basant sur le réseau déjà existant des opérateurs mobiles.

	sigfox	LoRaWAN	NB-IoT	LTE-M
Portée max ~	10 km en urbain	5 km en urbain	1 km en urbain	0.4 km en urbain
	50 km en rural	15 km en rural	10 km en rural	8 km en rural
Débit	100 bits/s	22 Kbits/s	20 - 250 Kbits/s	1 Mbits/s
Consommation en énergie	---	---	-	+
Coût de déploiement	--	--	+	+
Couverture	⋆ ⋆	⋆ ⋆ ⋆	⋆ ⋆	⋆ ⋆ ⋆
Roaming	Partiel	Partiel	Non	Roaming Actif
Sécurité	⋆ ⋆	⋆ ⋆	⋆ ⋆ ⋆ ⋆	⋆ ⋆ ⋆ ⋆
F(u)OTA / Acquittement	Non	Non	Oui	Oui

Figure 10 : Comparaison des réseaux LPWAN Cellulaires

Souce : https://www.matooma.com/fr/s-informer/actualites-iot-m2m/reseaux-lpwa-sommes

II.2.3 La couche traitement de la donnée

La couche de traitement accumule, stocke et traite les données provenant de la couche réseau. Cette couche se compose d'un certain nombre d'équipements (serveurs, des baies

[14] IUT, Les fondamentaux de l'IoT, PRIDA, 24/08/2020

de stockages) sur un réseau local ou externe pour la mémorisation des données, éventuellement des actionneurs et enfin des couches logicielles (Middleware) pour le traitement des informations réparties sur l'ensemble des éléments identifiés.

II.2.4 La couche applicative

La couche application reçoit les données de la couche de traitement de données et fournit les services requis aux utilisateurs IdO. Elle prend en charge une grande variété d'applications de contrôle et d'exploitation des dispositifs IdO dans les usages tels que la maison intelligente, les ampoules connectées, les réfrigérateurs connectés, les portiques connectés, les télévisions connectés, la vente au détail intelligente, les grilles intelligentes, les détecteurs de fumée connectés etc.
Les protocoles d'application les plus courants sont le protocole d'application contraint (CoAP) et le transport de télémétrie par file d'attente de messages (MQTT).

1. Constrained Application Protocol (CoAP)

Les appareils IdO étant limités en ressources, le protocole HTTP n'est pas adapté aux appareils à faible consommation en raison de sa complexité. CoAP a été conçu par Internet Engineering Task Force (IETF) pour inclure les caractéristiques de HTTP dédiées aux dispositifs IdO et pour les communications machine to machine. Comme le montre la figure 1.14, CoAP est un protocole de messagerie basé sur l'architecture REST.
Il comporte quatre types de messages :

- Confirmable ;
- Non confirmable ; • Accusé de réception et • Réinitialisation.

Il offre également des fonctionnalités qui ne sont pas disponibles sur HTTP, comme la notification push.

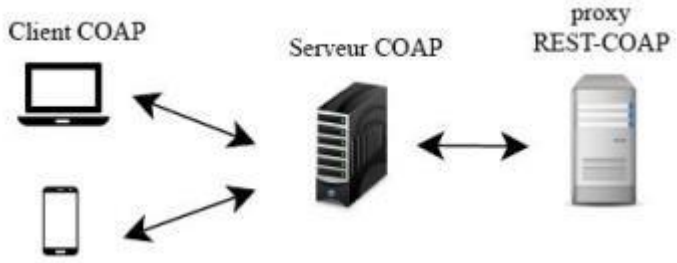


Figure 11 **:** Fonctionnement d'un CoAP

2. Message Queuing Telemetry Transport (MQTT)

MQTT est un protocole de messagerie léger qui assure la connectivité des réseaux et des utilisateurs avec des applications. Il est basé sur une architecture de publication/abonnement où le système se compose de trois éléments principaux : les éditeurs, les abonnés et un courtier.

Dans le contexte de l'IdO, les éditeurs sont des dispositifs intégrés qui envoient des données au courtier et les abonnés sont des serveurs d'applications.

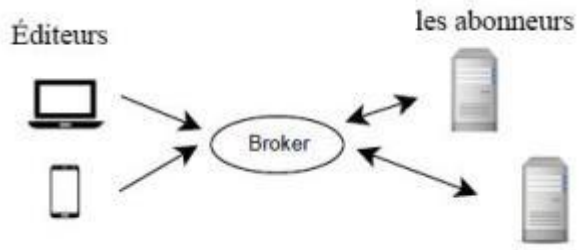


Figure 12 : Protocole de messageries au niveau des IdO

II.2.5 La couche sécurité

La couche sécurité est transversale aux autres couches précédentes. Elle a pour rôle d'assurer et garantir dans l'écosystème et au niveau de chaque couche de bout en bout :

- la confidentialité des données
- l'authentification des données échangées et des entités IdO eux-mêmes
- l'intégrité ou la sureté des données
- la non-répudiation qui permet au destinataire d'être certain que l'expéditeur est l'auteur des messages qu'il a générés
- l'anonymat des objets connectés
- De la sauvegarde de la disponibilité des ressources

En somme, nous pouvons conclure que, tout comme l'avènement de l'Internet des machines (IdM) dans les années 1960 et son essor fulgurant dans les années 2000 avec les réseaux sociaux ont conduit à la naissance et au développement de technologies et de protocoles de fonctionnement visant à garantir un service de qualité, de confidentialité, de disponibilité et d'intégrité, la naissance des IdO semble relancer cette course à l'innovation en matière d'applications, de protocoles, de technologies, de normes et de labellisations.

Face aux enjeux et risques cybernétiques introduits par l'Internet des machines (IdM), il est légitime de se demander : qu'en est-il de l'IdO ? Ces objets aux usages multiples, omniprésents dans notre quotidien, facilement accessibles sur le marché et à un grand public majoritairement non averti, sontils dépourvus de risques pour la cybersécurité de nos vies privées ?

Les IdO présentent-ils des vulnérabilités pour nos données personnelles et, par extension, pour la société dans son ensemble ?

II.3 MENACES ET VULNERABILITES

La sécurité de l'Internet des objets (IdO) destinés au grand public est essentielle pour protéger non seulement les dispositifs connectés, mais aussi les réseaux professionnels auxquels ils sont reliés, contre diverses menaces en ligne. L'Open Web Application Security Project (OWASP)[14] considère que les dix principales **vulnérabilités** de sécurité de l'IdO sont :

- Mots de passe faibles, devinables ou codés en dur,
- Services réseau non sécurisés,
- Interfaces écosystémiques non sécurisées,
- Absence de mécanisme de mise à jour sécurisé,
- Utilisation de composants non sécurisés ou obsolètes,
- Protection de la vie privée insuffisante,
- Transfert et stockage des données non sécurisés,
- Absence de gestion des dispositifs,
- Sécurité physique médiocre,
- Paramètres par défaut non sécurisés.

II.3.1 Les types d'attaques

Une enquête datant de 2022 sur les maisons intelligentes, portant sur les vulnérabilités, risques et contre-mesures [15] , décrit 12 différents **types d'attaques** contre les objets connectés grand public :

- **Attaques exploitant des mots de passe par défaut ou codés en dur** : Ils sont facilement devinables et souvent disponibles sur les sites des fournisseurs, permettent aux malwares comme Mirai de compromettre les dispositifs et de mener diverses cyberattaques, comme les attaques DDoS. Par exemple, en 2017, SplashData [16] a évalué plus de cinq millions de mots de passe divulgués sur Internet. Pour la cinquième année consécutive, les premières places restent inchangées : « 123456 » et « password». NordPass[17] a annoncé que le mot de passe le plus populaire en 2023 reste toujours « 123456 ».

[14] L'OWASP (Open Web Application Security Project) est une organisation mondiale à but non lucratif dédiée à la sécurité des applications web. https://owasp.org/www-project-internet-of-things/

[15] (PDF) Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures (researchgate.net)

[16] SplashData est une entreprise spécialisée dans la gestion des mots de passe et la sécurité des données. SplashData - Des outils de productivité puissants

[17] Les 200 mots de passe les plus courants | NordPass

- **Attaques par malware et botnet** : Des malwares comme Mirai[18], Bashlite[19], et Silex[20] ont ciblé les dispositifs IdO, exploitant des identifiants par défaut pour tenter des attaques par force brute[21] et ajouter ces dispositifs à l'armée de botnets telles que les attaques par déni de service distribué (DDoS). Mirai est l'un des malware botnet les plus connus, car il a été à l'origine de la plus grande attaque par déni de service distribué (DDoS) de l'histoire, atteignant un débit de plus de **1,7 térabit/seconde**.
- **Attaques par déni de service (DoS)** : Les appareils domestiques compromis peuvent lancer des attaques par déni de service (DoS[22]) ou déni de service distribué (DDoS[2324]), visant à empêcher l'utilisation légitime des services en inondant la cible de requêtes.
- **Attaques de scan** : Les attaquants identifient les victimes potentielles en utilisant des outils comme Shodan, Zmap, et Censys.
  Shodan[25] est un moteur de recherche puissant qui explore et indexe des dispositifs connectés tels que les serveurs, les caméras de sécurité, les routeurs, et même les systèmes de contrôle industriel.
  Conçu par John Matherly pour aider les entreprises à surveiller l'utilisation de leurs logiciels, Shodan est utilisé par des pirates pour identifier et prendre le contrôle de dispositifs mal sécurisés. En 2013, une vulnérabilité dans un logiciel utilisé par des immeubles, entreprises, et banques a été découverte, permettant à des pirates de contrôler 2 000 [25] systèmes, comme le chauffage et l'éclairage, via Shodan. Le Département de la Sécurité intérieure des États-Unis a confirmé que cette faille avait déjà été exploitée pour augmenter le chauffage d'une usine dans le New Jersey.
- **Attaque par falsification ou substitution de messages :** l'attaquant intercepte des messages valides pendant leur transit et les modifie pour que les destinataires les acceptent comme s'ils provenaient de l'expéditeur original. Par exemple modifier des traitements en soins de santé ou contrôler à distance des dispositifs tels que les serrures des portes, les thermostats, ou les systèmes de surveillance.
- **Attaque par répétition de messages :** Un attaquant peut enregistrer sélectivement certains messages et les rejouer ultérieurement sans modification. Cette attaque fournit intentionnellement des informations inexactes aux dispositifs ou serveurs et est souvent combinée avec une attaque de suppression de message. Elle peut atteindre des objectifs similaires à ceux des attaques de falsification ou de substitution de messages.
- **Attaque Sybil[26] :** L'attaquant crée plusieurs identités pour tromper les systèmes en envoyant de fausses informations, ce qui peut induire en erreur les systèmes de gestion

[18] Mirai est l'un des botnets IoT les plus connus. Il a été découvert en 2016 et a infecté des milliers d'appareils IoT en exploitant des mots de passe par défaut.
[19] **Bashlite**, découvert pour la première fois en 2014, il a évalué en plusieurs variantes, c'est un malware conçu pour infecter des appareils de l'Internet des objets (IoT). Il est également connu sous d'autres noms, tels que **Lizkebab**, **Gafgyt**, ou **Torlus**.
[20] **Silex** est un malware découvert en 2019 qui ciblait les appareils IoT pour les rendre inutilisables en effaçant leur mémoire et en causant des dommages irréversibles. Il a été créé par un adolescent et se distingue par sa capacité à rendre les appareils complètement inopérants.
[21] Une attaque par force brute : deviner un mot de passe ou une clé en essayant toutes les combinaisons possibles jusqu'à trouver la bonne.
[22] Une attaque **DoS** (Denial of Service) consiste à inonder un serveur ou un réseau de requêtes à partir d'une seule source jusqu'à ce qu'il ne puisse plus répondre aux demandes légitimes.
[23] Une attaque **DDoS** (Distributed Denial of Service) est similaire à une attaque DoS, mais elle utilise plusieurs machines pour lancer l'attaque.
[24] Moteur de recherche Shodan
[25] Shodan (site web) — Wikipédia (wikipedia.org)
[26] Cette attaque tire son nom du cas de "Sybil Dorsett", une femme diagnostiquée avec un trouble dissociatif de l'identité. Attaque Sybil — Wikipédia (wikipedia.org)

ou de décision. Par exemple, il peut envoyer de nombreux faux messages de capteurs de fumée pour faire croire qu'un incendie se propage dans la maison.

- **Attaque par usurpation d'identité** : Contrairement à l'attaque Sybil où l'attaquant essaie de créer de nombreuses fausses identités, dans le cas d'une attaque par usurpation d'identité, l'attaquant tente de se faire passer pour un utilisateur légitime afin d'utiliser des privilèges.

- **Espionnage** : En raison des limitations techniques des appareils IdO, les méthodes de chiffrement traditionnelles ne sont pas toujours appliquées. Cela permet à un attaquant d'accéder à des enregistrements vidéo de caméras lors de leur transmission ou à des informations sensibles comme des données bancaires, si elles ne sont pas suffisamment protégées.
- **Compromission physique d'un nœud** : Cela correspond à l'acte de capturer et de compromettre un nœud légitime du réseau domestique, c'est-à-dire de le reprogrammer par un attaquant. Ainsi, un nœud compromis qui exécute un code malveillant sous l'apparence d'un nœud légitime peut être utilisé pour lancer diverses attaques internes.
- **Attaque par apprentissage automatique adversarial** : beaucoup d'appareils IdO traitant l'image et la parole reposent sur des algorithmes d'apprentissage automatique qui sont assez efficaces pour aider à la détection d'attaques et d'intrusions. Mais ils sont vulnérables à certains types d'attaques. La plus courante est l'apprentissage automatique adversarial consistant à modifier des données légitimes avec des perturbations subtiles, souvent invisibles pour les humains, afin de tromper les systèmes d'IA et les amener à faire des erreurs tout en restant correct pour un observateur humain.
- **Attaque en utilisant des applications compromises et des permissions excessives** : afin d'accéder aux données des dispositifs ou de les utiliser pour affaiblir le système et augmenter la surface d'attaque.

II.3.2 Les vulnérabilités et scénarios d'attaques des IdO

Dans leur rapport intitulé Le paysage de la sécurité IdO 2023, en anglais « The 2023 IdO Security Landscape Report [28] », publié le 25 avril 2023, les sociétés NETGEAR [27] et

[27] NETGEAR est une entreprise américaine spécialisée dans la fabrication de matériel réseau domestiques et pour les petites entreprises, fondée en 1996.

Bitdefender[28] révèlent qu'une analyse des données provenant d'un échantillon mondial de **2,6 millions** de foyers intelligents protégés par NETGEAR Armor[29] a été effectuée pour identifier les vulnérabilités et scénarios d'attaque. Cette analyse a examiné **120 millions** d'appareils IdO, générant **3,6 milliards** d'événements de sécurité.

Figure 13 : Analyse des Vulnérabilités dans les Foyers Intelligents

Source : 2023-IoT-Security-Landscape-Report.pdf (bitdefender.com)

Huit attaques par jour ciblent en moyenne les foyers équipés d'objets connectés. C'est un chiffre élevé qui reflète l'essor des IdO dans nos foyers.

Dans le graphique ci-après, NETGEAR et Bitdefender donnent un aperçu des objets connectés les plus populaires dans une maison intelligente. Selon ce rapport, près de **41 %** des IdO connectés aux routeurs domestiques sont des smartphones, suivis par les ordinateurs de bureau et portables. Les appareils de streaming occupent la troisième place. Les tablettes, très populaires pendant la pandémie de COVID-19, ont vu leur utilisation augmenter lorsque les écoles ont commencé à les distribuer pour l'enseignement en ligne. Quant aux Smart TV, bien qu'elles ne représentent que 5,4 % des appareils, elles comptent parmi les IdO les plus vulnérables dans les maisons connectées. Enfin, les consoles de jeux représentent **4,2 %.**

[28] Bitdefender est une entreprise roumaine spécialisée dans la cybersécurité, fondée en 2001.

[29] NETGEAR et Bitdefender collaborent pour offrir des solutions de sécurité réseau intégrées, comme NETGEAR Armor, qui protège les appareils connectés des foyers intelligents contre diverses menaces en ligne.

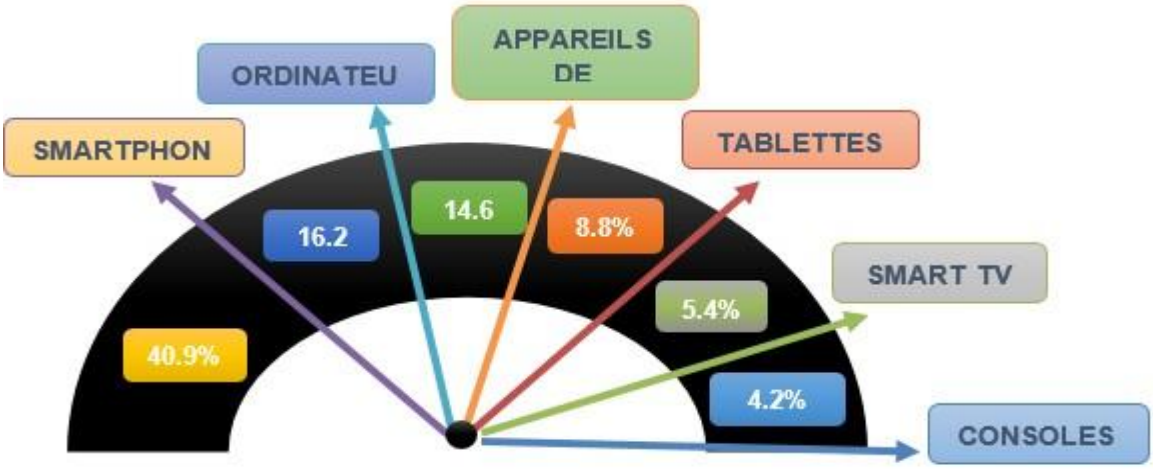


Figure 14: IdO les plus populaires dans une maison intelligente
Source : 2023-IoT-Security-Landscape-Report.pdf (bitdefender.com)

Selon cette étude, les dispositifs IdO les plus vulnérables en 2022 sont les Smart TV, elles concentrent plus de la moitié des vulnérabilités. Les prises intelligentes, devenues plus populaires en raison de la surveillance de la consommation d'énergie face à la hausse des coûts, sont fortement vulnérables.

La majorité des attaques observées en 2022 reposent sur des vulnérabilités courantes déjà répertoriées (CVE[30]), intégrées dans des outils d'attaque automatisés (Botnet[31]). Bien que ces vulnérabilités soient connues des fournisseurs de l'IdO comme des attaquants, les fabricants de firmware peuvent mettre un temps considérable à évaluer, corriger et fournir des mises à jour pour les appareils déjà déployés dans les maisons intelligentes, offrant ainsi potentiellement une fenêtre d'opportunité aux cybercriminels.

[30] **CVE** signifie **Common Vulnerabilities and Exposures** (Vulnérabilités et Expositions Communes en français). Il s'agit d'un système de référence pour identifier et nommer de manière unique les vulnérabilités et expositions de sécurité dans les logiciels et les systèmes informatiques.

[31] Un **botnet** est un réseau de dispositifs informatiques infectés par un logiciel malveillant (souvent appelés « bots » ou « zombies ») qui sont contrôlés à distance par un attaquant, souvent appelé « botmaster ». Les dispositifs infectés peuvent inclure des ordinateurs, des serveurs, des smartphones, ou même des appareils IdO comme des caméras de sécurité ou des routeurs.

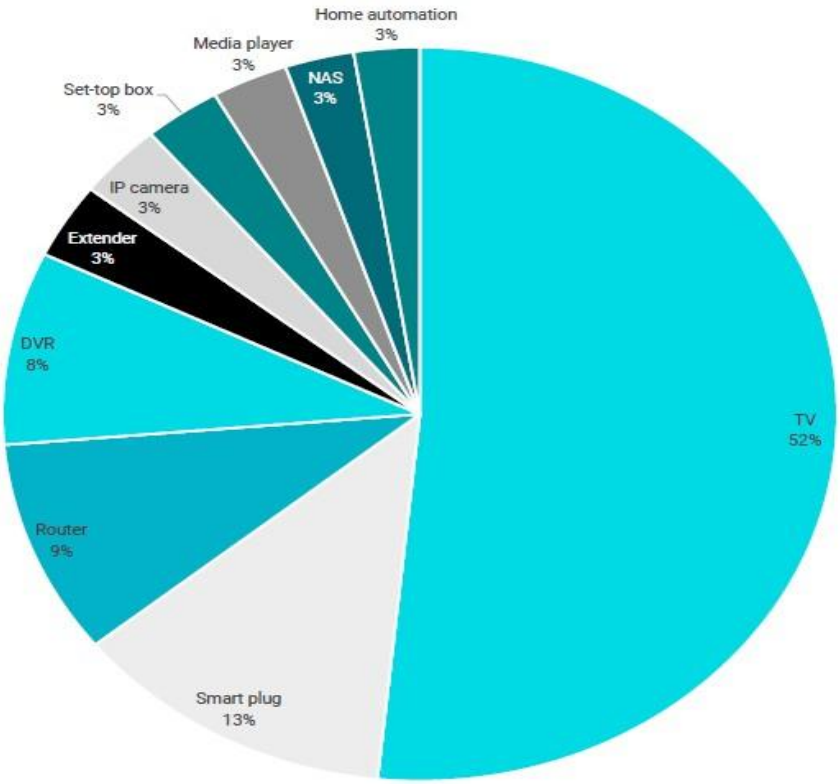


Figure 15 : Appareils IdO les plus vulnérables en 2022
Source : [2023-IoT-Security-Landscape-Report.pdf (bitdefender.com)]

Les attaques par déni de service demeurent le type d'attaque prédominant, représentant plus de **84** % des incidents enregistrés en **2022**. Les incidents visant des données sensibles constituent **11 %** du total, tandis que l'exploitation des dispositifs représente **2 %**.

En somme, les objets connectés grand public restent vulnérables et faciles à compromettre pour plusieurs raisons. Tout d'abord, beaucoup de dispositifs IdO présentent des failles de sécurité, telles que des mots de passe par défaut ou des mises à jour de sécurité rares. Ces appareils collectent souvent des données personnelles sensibles, comme les données de géolocalisation, des conversations, des photos, et des informations de santé, qui peuvent être monnayées ou exploitées à des fins publicitaires. De plus, ces dispositifs sont souvent connectés à d'autres dispositifs et réseaux, offrant aux attaquants un point d'entrée pour accéder à des systèmes plus critiques. Le problème principal réside dans le fait que de nombreux consommateurs ne sont pas conscients des vulnérabilités spécifiques des objets connectés qu'ils utilisent et ne comprennent pas toujours les implications des risques, qui seront expliqués en détail dans la suite.

II.3.3 Risques liés à l'utilisation des objets connectés grand public

Les principaux risques de cybersécurité des objets connectés, dont les répercussions touchent directement le grand public, peuvent être classés en trois catégories.

En premier la cybercriminalité, souvent motivée par le vol de données personnelles sensibles comme les numéros de carte bancaire et par la prise de contrôle des dispositifs pour des attaques à grande échelle, telles que les botnets, est favorisée par l'absence de mesures de sécurité adéquates lors de la fabrication des objets connectés. Des vulnérabilités

telles que des mots de passe faibles, des failles zero-day[32], et le manque de mises à jour régulières facilitent la réalisation de ces attaques.
Ces attaques sont souvent orchestrées par des botnet constitués de réseaux de dispositif IdO, infectés par des logiciels malveillants et contrôlés à distance par des cybercriminels. Ces objets connectés, appelés "bots" ou "zombies", sont utilisés pour des activités malveillantes comme les attaques DDoS, l'envoi de spams ou le vol de données. Boris Lecoeur, Directeur Général de Cloudflare[33] (Crédit Cloudflare), avait indiqué en avril 2024 une augmentation significative des attaques DDoS, +117 % sur le trimestre précédent et assure que « *N'importe qui peut mener une attaque DDoS suffisamment sophistiquée, des kits sont même à vendre sur le darknet pour quelques dollars* ». Mirai, Rift[34], Gafgyt[35], Bushido[36], Hakai[37] et Muhstik[40] sont les familles de malwares les plus utilisées pour cibler les dispositifs IdO.

En 2023, l'équipe de recherche de Zscaler a constaté que les attaques de malwares à l'encontre des dispositifs IdO avaient augmenté de 400 % au premier semestre 2023 par rapport à la même période en 2022. Les botnets, principalement les malwares Mirai et Gafgyt, dominent toujours les attaques, représentant 66 % des charges utiles des attaques.

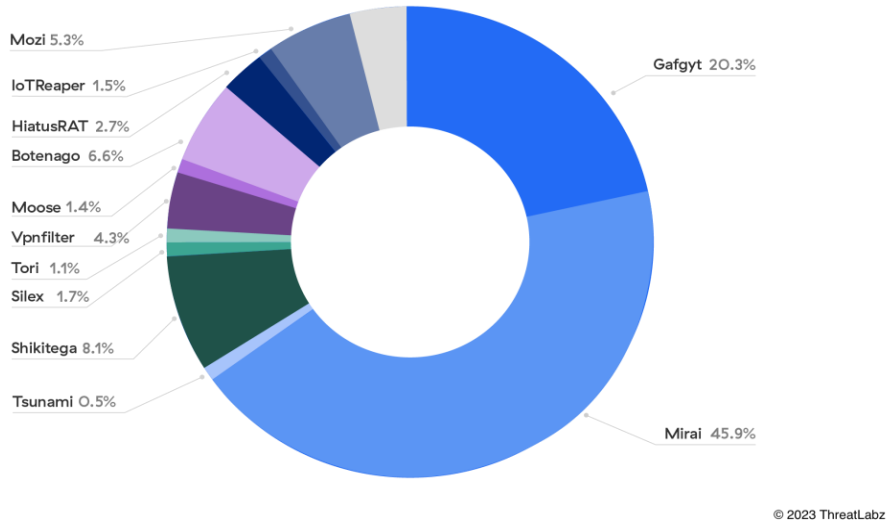


Figure 16 : malwares IdO **selon** Zscaler, **janv-juin 2023**
Source : Rapport 2023 sur les menaces liées à l'IoT et à l'OT en entreprise par Zscaler ThreatLabz

L'atteinte à la vie privée constitue le deuxième risque auquel le grand public est confronté en utilisant certains dispositifs IdO, tels que les caméras, microphones et divers capteurs,

[32] Une attaque **zero-day** est une cyberattaque qui exploite une vulnérabilité logicielle qui n'a pas encore été découverte ou corrigée par les développeurs du logiciel. Le terme "zero-day" signifie que les développeurs ont eu "zéro jour" pour se préparer ou réagir à la vulnérabilité.
[33] **Editeur Cloudflare,** protège 20 % de l'internet mondial donc des millions de sites d'entreprises et des milliers en France (dont Mano Mano, Carrefour, Norauto, etc.)
[34] **Rift** est un botnet moins connu mais qui cible également les appareils IdO. Il utilise des techniques similaires à Mirai pour infecter les dispositifs.
[35] **Gafgyt** est un autre botnet IdO qui cible principalement les routeurs et les caméras de sécurité.
[36] **Bushido** est un botnet IdO qui cible les appareils utilisant des systèmes d'exploitation Linux.
[37] **Hakai** est un botnet qui cible principalement les routeurs et les dispositifs IdO mal sécurisés. [40]
Muhstik est un botnet IdO qui cible les routeurs et les dispositifs de stockage en réseau.

qui peuvent recueillir des informations sur les habitudes de vie, les déplacements et les données de santé des utilisateurs. L'analyse de cette grande quantité de données personnelles peut permettre un profilage détaillé à des fins de marketing et de ciblage publicitaire. Souvent sans le consentement explicite des utilisateurs, cela représente une atteinte à la vie privée particulièrement préoccupante dans le cadre des installations domestiques.

Plusieurs scandales impliquant les courtiers en données et la protection de la vie privée ont souvent révélé des pratiques douteuses de collecte et d'utilisation des informations personnelles. Ces courtiers collectent et agrègent ces informations pour créer des profils détaillés des individus, qu'ils vendent ensuite à des entreprises pour diverses utilisations, notamment l'envoie de publicité personnalisée afin d'influencer leurs opinions et comportements de manière subtile et intrusive. Le groupe Data Broker Watch [38] , qui surveille et analyse les activités des courtiers de données, affirme que ces derniers « *sont un facteur clé de la perte croissante de la vie privée, du capitalisme de surveillance endémique, du micro-ciblage, de la désinformation, ainsi que de la nature addictive des expériences numériques* », des assertions autant choquantes qu'effrayantes !
En effet, aux États-Unis, les courtiers peuvent accumuler jusqu'à 1 500[39] informations sur chaque individu. En Europe, même si le RGPD est en vigueur, les courtiers trouvent les moyens de contourner les règles, par exemple en manipulant le concept d'« intérêt légitime » ou en profitant de l'inattention des internautes concernant leurs consentements. A titre d'exemple le scandale de Cambridge Analytica, a révélé que les données personnelles de 87 millions d'utilisateurs de Facebook avaient été collectées sans leur consentement et utilisées pour influencer les élections présidentielles américaines de 2016. Plusieurs cas spécifiques de violations de vie privées seront détaillés dans le chapitre suivants.

Le troisième risque concerne la sécurité physique des personnes utilisant des dispositifs IdO tels que les prises intelligentes, les serrures connectées et les caméras, qui gagnent en popularité. Cependant, des vulnérabilités dans ces dispositifs peuvent permettre à des individus malintentionnés de localiser des maisons susceptibles d'être cambriolées à l'aide de caméras, de microphones et de capteurs, manipuler à distance des appareils comme des machines à laver pour provoquer des inondations, coordonner les appareils d'une communauté pour surcharger le réseau électrique, espionner des enregistrements vidéo et audio pour extorquer des informations privées, voire pire, manipuler des appareils de santé pour nuire physiquement aux personnes. De plus, ces appareils peuvent être détournés à des fins d'espionnage, comme la surveillance des utilisateurs via des caméras de sécurité. En 2019, des employés d'Amazon travaillant pour la société de sécurité Ring[40] ont abusé de leur accès aux caméras de sécurité pour espionner les clients et harceler les utilisateurs via les haut-parleurs intégrés.

Cependant, un autre aspect lié à la collecte d'informations des objets connectés par les états est à considérer. Ces données sont exploitées pour diverses raisons, allant de la sécurité

[38] https://databrokerswatch.org/
[39] https://clearcode.cc/blog/what-is-data-broker/
[40] https://africa.businessinsider.com/news/new-details-emerge-about-amazons-ring-staff-spying-on-customers-and-also-revealsthat/6gs0dyr

nationale, la surveillance politique à l'espionnage des états. Les chercheurs de Zscaler , dans leur rapport intitulé « ThreatLabz 2023 sur les menaces liées à l'IoT et à l'OT d'entreprise »[41] affirment que « *Les appareils des catégories de divertissement et domotique, comme les smart TV, les consoles de jeux, les décodeurs et les caméras IP, sont les principaux contributeurs au trafic à destination de la Chine et de la Russie. Bien qu'une grande partie de ce trafic soit légitime et non malveillant, ce sont des destinations que ThreatLabz considère comme suspectes en raison de leur potentiel d'espionnage gouvernemental et d'autres vulnérabilités ».*

En 2013, Edward Snowden, un ancien employé de la NSA, a révélé les programmes de surveillance massive par les États-Unis, comme PRISM[42] et XKeyscore[43]. Ces programmes ont collecté des données personnelles de millions de personnes à travers le monde, souvent sans leur consentement. La NSA, avaient aussi la capacité de pirater des webcams pour surveiller les utilisateurs en temps réel. Cela inclut des webcams intégrées aux ordinateurs portables et des caméras de sécurité domestiques.
En 2021, un consortium de journalistes et d'organisations de défense des droits de l'homme ont révélé Pegasus qui est un logiciel espion développé par la société israélienne NSO Group, permettant de surveiller à distance les smartphones. Ce logiciel était capable de collecter des informations telles que les appels, les messages, les contacts, les emails, ainsi que d'activer les caméras et les microphones des appareils ciblés. Nous avons examiné ce sujet en détail dans le chapitre consacré à la stratégie de la Chine et des États-Unis.

Des exemples concrets de cyberattaques et de violations de la vie privée impliquant des objets connectés utilisés par le grand public, sont présentés en annexe.

II.4 REPONSES AUX DEFIS DE L'INTERNET DES OBJETS

En somme, les objets connectés, bien qu'avancés et sophistiqués, s'intègrent profondément dans notre quotidien en offrant confort et bien-être, à tel point que leur présence devient souvent invisible et leur fonctionnement pris pour acquis. Toutefois, cette invisibilité masque des conséquences graves, allant du simple vol de coordonnées bancaires à des perturbations majeures dans les infrastructures critiques, voire à de la surveillance de masse, posant des risques de violation des droits de l'homme et de la vie privée.

L'avènement de l'IA augmenterait significativement les capacités des cybercriminels pour attaquer les dispositifs IdO, exploiter les données sensibles et compliquer les mesures de sécurité nécessaires pour protéger ces systèmes. Pour sa part, David Kerr, VP de Strategy Analytics, affirme que « *l'intelligence artificielle va devenir omniprésente sur les plateformes mobiles, domestiques, automobiles et informatiques. L'optimisation de l'expérience*

[41] https://www.zscaler.fr/blogs/security-research/2023-threatlabz-report-indicates-400-growth-iot-malware-attacks
[42] **PRISM,** permettait à la NSA de collecter des données directement auprès des grandes entreprises de technologie, comme Google, Facebook, et Microsoft. Les informations collectées comprenaient des e-mails, des conversations en ligne, et des informations sur les utilisateurs, souvent sans mandat spécifique.
[43] **XKeyscore** : Un autre programme permettant de collecter et d'analyser un vaste volume de données Internet. XKeyscore était capable d'accéder à des informations telles que les activités en ligne des utilisateurs, les historiques de navigation, et les communications électroniques.

utilisateur sur plusieurs appareils, systèmes d'exploitation et interfaces utilisateur constituera un champ de bataille essentiel ».

Pour survivre dans ce champ de bataille, l'humain constitue le premier facteur de risque à adresser. Il est crucial de sensibiliser les individus de manière percutante aux enjeux associés aux objets connectés qu'ils utilisent quotidiennement avec une quasi-affection. L'utilisateur doit être conscient des risques liés à ces objets et appliquer des gestes simples mais efficaces, tels que se renseigner sur les aspects de sécurité de tout appareil connecté avant l'achat, changer le mot de passe lorsque cela est possible, et mettre régulièrement à jour les logiciels pour garantir la sécurité de ses dispositifs.

Ces mesures étant minimales et insuffisantes, plusieurs institutions et organisations tels que l'ENISA s'accordent sur l'importance d'instaurer des protections dès la phase de fabrication des objets connectés grand public à travers une réglementation robuste et prospective, à l'instar des secteurs de la santé et de l'automobile. Une telle réglementation doit couvrir la confidentialité des données, la sécurité des dispositifs, la coordination internationale et la protection des consommateurs, dans un contexte où l'IdO est omniprésent, avec une connectivité accrue et une intégration croissante de l'intelligence artificielle. Dans ce contexte, la future loi sur le cyber résilience (Cyber Resilience Act) est bientôt applicable dans l'Union européenne. Nous avons choisi de ne pas nous attarder davantage sur ce sujet, car ce mémoire consacre tout un chapitre aux réglementations des objets connectés.

Pour conclure, si la maison futuriste "intelligente" imaginée par Ray Bradbury en 1950 est devenue réalité en 2024, il est tout à fait envisageable que le scénario anticipé par un expert de Fortinet, où une attaque DDoS viserait une entreprise suisse via un botnet composé de millions de brosses à dents connectées, se réalise également, à moins que des mesures rigoureuses ne soient prises pour sécuriser les objets connectés.

III. État du marché de l'Internet des objets : Tendances actuelles et projections futures

III. ÉTAT DU MARCHE DE L'IDO : TENDANCES ACTUELLES ET PROJECTIONS FUTURES

Analyser l'évolution des objets connectés a été un véritable défi pour nous en raison des complexités liées à la variabilité des sources, aux définitions parfois incohérentes, et à la rapidité de l'évolution du marché. La tâche devenait encore plus ardue lorsqu'il s'agissait d'obtenir des chiffres précis sur les IdO destinés au grand public, en raison de la diversité des dispositifs, de l'adoption inégale à travers le monde, de la fragmentation des données et de l'absence de normes unifiées.

En effet, les estimations du nombre d'appareils IdO varient considérablement d'une source à l'autre. Des organisations telles que IdO Analytics[44], Strategy Analytics[48], Gartner[49] et International Data Corporation[45] publient souvent des études de marchés avec des chiffres différents en raison de leurs méthodologies spécifiques, souvent payantes et inaccessibles pour le grand public. Par exemple : IdO Analytics[51] et Extrapolate[46] propose des études à partir de 3000 €. De plus, la définition d'un « dispositif IdO » peut diverger : certains incluent les objets connectés simples, tandis que d'autres se concentrent sur des dispositifs plus sophistiqués avec des capacités d'analyse avancées. Certaines estimations comptabilisent également les smartphones, les ordinateurs portables et les PC comme objets connectés, tandis que d'autres ne les incluent pas. Enfin, le nombre considérable de nouveaux dispositifs introduits chaque année par millions complique davantage l'obtention de chiffres précis et à jour.

En ce qui concerne l'évaluation du marché des objets connectés destinés au grand public, elle se heurte à une grande diversité de dispositifs, allant des montres intelligentes et assistants vocaux aux réfrigérateurs connectés, thermostats intelligents et ampoules connectées, avec une liste qui continue de s'allonger. Ce secteur évolue également à un rythme extrêmement rapide, rendant difficile la création de bases de données précises et à jour. L'adoption de ces objets varie considérablement selon les régions : elle peut être rapide et généralisée dans certains pays, tandis qu'elle reste lente et limitée dans d'autres. De plus, les données disponibles sur les IdO grand public sont souvent fragmentées, provenant de sources multiples telles que les fabricants, les distributeurs, les cabinets de recherche et les entreprises de télécommunications. À cela s'ajoute l'absence de normes globales unifiées pour la catégorisation et le suivi des objets connectés, ce qui entraîne des divergences dans la manière dont les dispositifs sont comptabilisés et rapportés. Toutefois et malgré ces difficultés, **tous les acteurs de ce marché s'accordent à reconnaître la massification de l'Internet des objets et son expansion rapide et omniprésente.**

[44] IdO Analytics est une société de recherche et de conseil spécialisée dans l'Internet des Objets (IdO). https://IdO-analytics.com [48] Strategy Analytics, fondée en 1996, spécialisée dans l'analyse des marchés de la technologie, des médias et des télécommunications. [49] Gartner, fondée en 1979, spécialisée dans le conseil et de recherche en technologies de l'information (TI) basée aux États-Unis. https://www.gartner.com/en

[45] International Data Corporation (IDC), fondée en 1964 et basée à Framingham, Massachusetts, spécialisée dans la fourniture de services de conseil et d'études de marché dans le domaine des technologies de l'information, des télécommunications et des technologies grand public. IDC est une filiale de la société de médias et de recherche IDG (International Data Group). [51] https://IdO-analytics.com/product/IdO-commercialization-business-model-adoption-report-2024/

[46] https://www.extrapolate.com/information-technology-communication-IdO/consumer-IdO-market/87454

III.1 TAILLE ET CROISSANCE DU MARCHE DES IDO

Statista a annoncé le 12 juin 2024[47] que le nombre d'appareils de l'Internet des objets (IdO) dans le monde devrait presque doubler, passant de **15,9** milliards en **2023** à plus de **32,1** milliards d'appareils d'ici **2030**. En **2033**, la Chine sera le pays avec le plus grand nombre d'appareils IdO, comptant environ **8** milliards d'appareils destinés au grand public. Le segment grand public représente environ **60 %** de tous les appareils IdO en 2023. Cette proportion devrait rester stable au cours des dix prochaines années. Les principaux cas d'utilisation des appareils IdO dans le segment grand public incluent les dispositifs Internet et multimédias, comme les smartphones, dont le nombre devrait dépasser **17** milliards d'ici 2033.

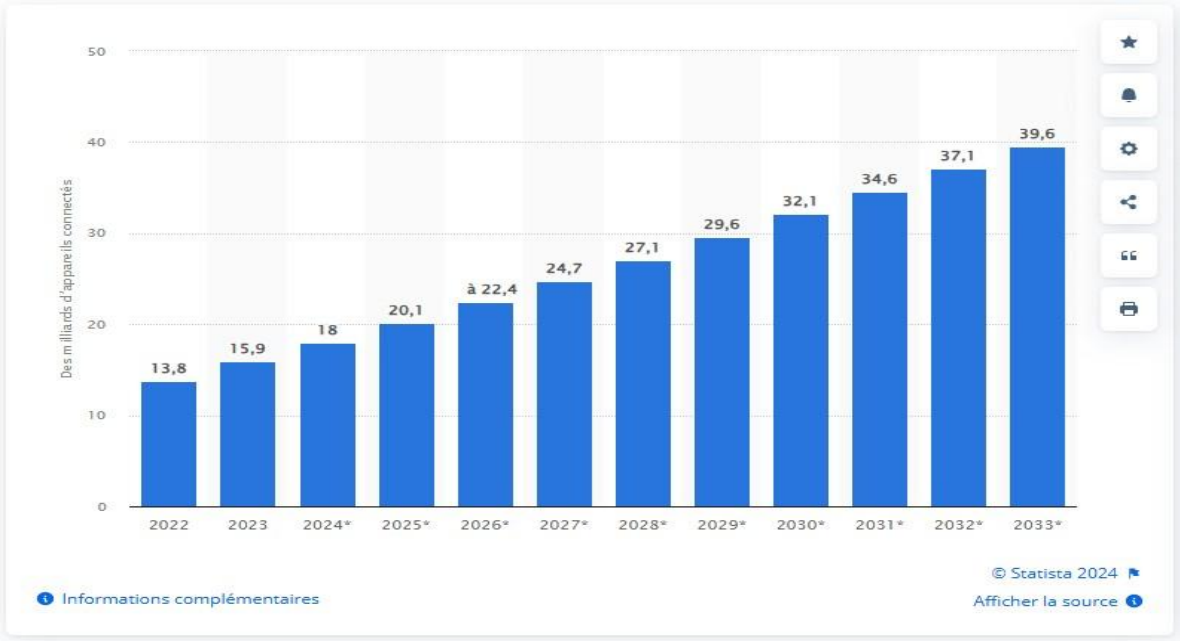


Figure 17 : Nombre et prévision des dispositifs (IdO) dans le monde
Source : Connexions IdO dans le monde 2022-2033 | Statista

Monsieur Frédéric Charles[48], a souligné lors de l'entretien qu'il nous a accordé suite à sa contribution du 18/02/2024 dans le média numérique ZDNet [49] que la croissance du déploiement des objets connectés n'a pas fléchi depuis **2019**. « *En 2010, on atteignait le 1er milliard d'objets connectés, et en 2017, **Cisco** en prévoyait 30 milliards en 2022. En 2023, **Strategy Analytics** estimait dans une étude leur nombre à 22 milliards dans le monde (smartphones, enceintes, téléviseurs, montres, tablettes, ordinateurs portables/bureaux,*

[47] https://www.statista.com/statistics/1183457/IdO-connected-devices-worldwide/
[48] Directeur Stratégie & Innovation chez SUEZ Smart Solutions, Passionné de technologies et partage son analyse personnelle de la transformation numérique des entreprises et de la ville intelligente de demain.
[49] Quel réseau demain pour les objets connectés ? - ZDNET

etc.) ce qui est moins qu'attendu, mais qui confirme cependant une croissance à deux chiffres qui ne fléchit pas. Les secteurs professionnels et la maison connectée ont les plus fortes croissances, ce dernier étant le territoire d'Amazon. ***Aujourd'hui, on annonce 38 milliards d'objets connectés en 2025 et 50 milliards en 2030 ».***

C'est fascinant de voir à quel point l'Internet des objets (IdO) a évolué et continue de croître à un rythme exponentiel. Les prévisions de Siemens[50] en 2020 soulignent cette croissance impressionnante, avec des chiffres qui montrent une augmentation rapide du nombre d'objets connectés, passant de **27** milliards en **2020** à une estimation de **75** milliards en **2025.** Cela signifie qu'il y aura presque dix objets connectés par personne sur Terre !

Lors de la convention mondiale de l'Internet des objets qui a été tenue en Chine en juillet 2023, M. HE Xuming, président du comité exécutif du WIDOC[51], a fait observer que les IdO mondiaux devraient augmenter de plus de **20 %** et dépasser les **18** milliards en **2023**. D'ici **2030**, ce nombre devrait dépasser les **80** milliards.

En termes de chiffres d'affaires, Statista a annoncé en mai 2024, que les revenus mondiaux liés à l'IdO devraient atteindre 336 milliards de dollars américains en 2024 et dépasser les 621 milliards de dollars américains en 2030, soit une augmentation de près de 85 % en six ans. De plus, le nombre d'appareils connectés à l'IoT dans le monde devrait doubler au cours de cette période.

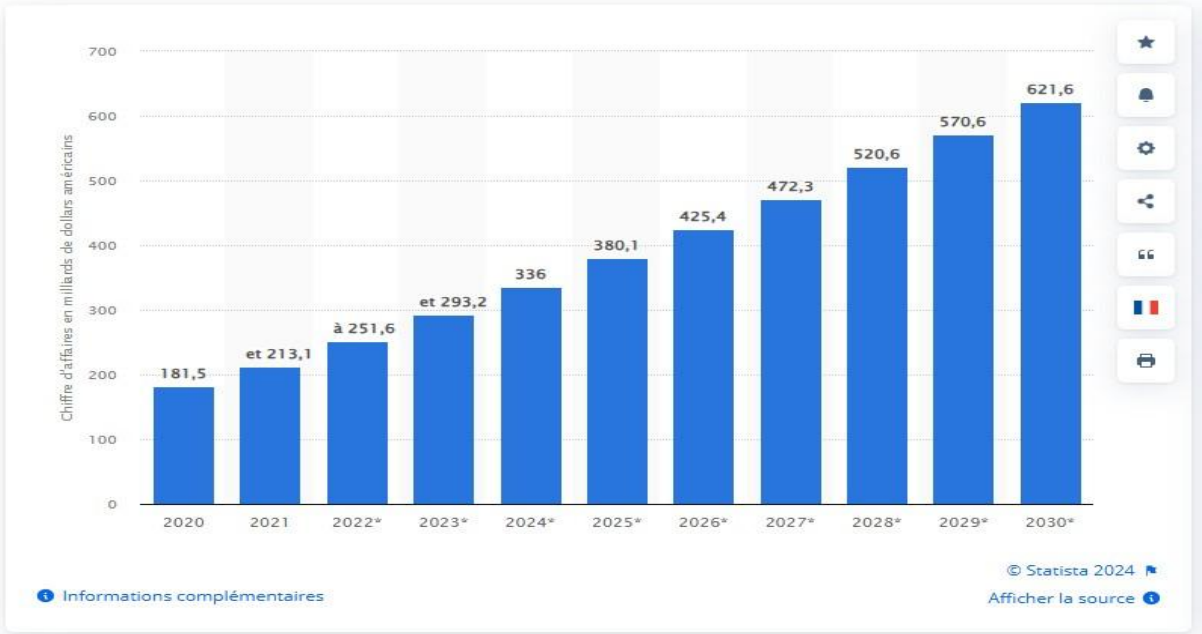


Figure 18 : CA annuel de IdO dans le monde de 2020 à 2030 en milliards $
Source : Chiffre d'affaires mondial de l'IdO en 2030 | Statista

[50] https://www.siemens.com/fr/fr/entreprise/stories/innovation-technologies/jumeau-numerique/histoire-IdO.html

[51] WIDOC 2024-Convention mondiale de l'Internet des objets (WIDOC) , ou World Internet of Things Convention**,** est une organisation internationale dédiée à l'avancement et à la promotion de l'Internet des Objets (IdO) à l'échelle mondiale. Le WIDOC réunit des experts, des entreprises, des gouvernements et des organisations de différents secteurs pour discuter des tendances, des défis, et des opportunités liées à l'IdO.

Concernant les dépenses dans le monde de l'Internet des objets (IdO), Statista rapporte qu'en **2023**, elles ont atteint **805** milliards de dollars, une hausse par rapport à l'année précédente mais inférieure aux prévisions de **1,1** trillion de dollars en raison de la pandémie de coronavirus, avec l'Asie-Pacifique en tête du marché, suivie par l'Amérique du Nord puis l'Europe, le Moyen-Orient et l'Afrique. De plus en plus d'organisations investissent dans l'IdO et leur nombre s'élevait à **2 552** mille organisations en Europe en mai **2020**.
Le financement s'est élevé à plus de **5** milliards de dollars américains. De plus, les dépenses technologiques dans les initiatives de villes intelligentes ont atteint **104** milliards de dollars américains dans le monde en **2019**.

Comme nous pouvons le constater, l'expansion des objets connectés reste incontestable !!

III.2 MOMENTS CLES DE L'EVOLUTION DE L'INTERNET DES OBJETS

L'Internet des objets (IdO) a vu le jour dans les années 90 et s'est développé au fil du temps :

- **Début des années 90** : L'idée de contrôler des appareils électroniques à distance, comme des grille-pains et des machines à café connectés à Internet, commence à se populariser.
- **1995** : Bill Gates, cofondateur de Microsoft, évoque pour la première fois le concept de l'Internet des objets dans son livre *The Road Ahead*.[52]
- **1998** : Kevin Ashton[53] présente la notion d'Internet des objets au Massachusetts Institute of Technology (MIT).
- **1999** : Création du laboratoire Auto-ID, spécialisé dans les objets connectés via la RFID et les réseaux de capteurs sans fil.
- **2005** : L'Union internationale des télécommunications (UIT) publie un rapport intitulé : « *L'Internet des objets »*, officialisant le concept et explorant les interactions entre les mondes physique et virtuel.
- **2009** : La Commission européenne publie « *L'Internet des objets : le plan d'action européen »*, décrivant les perspectives et les défis de l'IdO et définissant un plan d'action.
- **2012** : Le nombre d'objets connectés à l'échelle mondiale atteint environ **8,2** milliards.

III.3 FACTEURS CLES DE CROISSANCES DES IDO

La prolifération des appareils connectés, dont le nombre a explosé, s'explique par les progrès réalisés dans l'électronique, les télécommunications, le traitement des données, ainsi que par les capacités de calcul. De ce fait, les objets connectés ne sont plus de simples capteurs : ils fonctionnent au sein de réseaux et peuvent créer, communiquer, agréger, analyser et agir sur des données. Ces améliorations se sont accompagnées d'une baisse significative du coût de ces technologies.

[52] *The Road Ahead* est un livre écrit par Bill Gates, publié en 1995. Dans cet ouvrage, Gates explore les tendances futures de la technologie et de l'informatique, et introduit pour la première fois le concept d'Internet des objets (IoT).

[53] Kevin Ashton est un pionnier de la technologie et l'un des fondateurs du terme "Internet des objets"

La baisse des coûts des capteurs a favorisé l'adoption des objets connectés dans divers secteurs. Par exemple, le prix des puces RFID de base est passé de **0,50-1 USD** à environ **0,05-0,10 USD** par puce. Bien que les puces RFID avancées (chiffrées, réinscriptibles) soient encore plus coûteuses, elles offrent des fonctionnalités améliorées. Un cas notable est celui de Decathlon, qui utilise la RFID pour optimiser la traçabilité des produits, accélérer le passage en caisse et améliorer la gestion des stocks, permettant de réaliser les inventaires en magasin cinq fois plus rapidement grâce aux lecteurs RFID. Néanmoins, les puces RFID peuvent potentiellement être lues à distance, soulevant des préoccupations concernant la confidentialité des données.

Cette tendance de diminution des coûts est également observée dans les technologies de communication nécessaires pour connecter ces objets. Par exemple, en 2010, le coût moyen d'un module Wi-Fi était d'environ **10-15 USD**, tandis qu'en 2024, il est tombé à environ **2-5 USD**. De même, un module Bluetooth coûtait en moyenne d'environ **5-10 USD** en 2010, contre **1-3 USD** en 2024. Les modules 4G, autrefois à **50-100 USD**, ont été remplacés par des modules 5G, disponibles à environ **10-20 USD** en 2024, rendant ces technologies plus accessibles.

L'émergence des réseaux 5G et 6G stimulent la croissance des IdO et représentent des avancées majeures par rapport à la 4G, offrant des vitesses de connexion bien supérieures et une latence réduite. La 4G, avec des vitesses réelles autour de **100 Mbps** et une latence de **50 ms**, était principalement adaptée aux smartphones et limitée pour les objets connectés nécessitant des réponses rapides. En comparaison, **la 5G**[60] atteint des vitesses pratiques de **1 Gbps** avec une latence d'environ **1 ms**, permettant des applications avancées telles que la réalité augmentée, les véhicules autonomes et les villes intelligentes. **La 6G**, en développement, vise des vitesses jusqu'à **100 Gbps** et une latence inférieure à **1 ms**, ouvrant la voie à des innovations comme les hologrammes en temps réel.

Les progrès réalisés dans les satellites en orbite basse (LEO) et les chipsets compatibles avec la connectivité terrestre et satellitaire révolutionnent le secteur de l'IdO intelligent, générant une compétition intense entre les entreprises et les nations pour dominer le marché de la connectivité satellite. Cela garantit que les appareils IdO peuvent fonctionner partout sur le globe. Les satellites facilitent une multitude d'applications IdO, allant de l'agriculture intelligente (suivi des conditions météorologiques et de la santé des cultures) à la logistique (suivi des expéditions) et à la gestion des infrastructures (surveillance des pipelines et des réseaux électriques). Les acteurs principaux dans ce domaine incluent : Starlink de SpaceX[61], OneWeb[54]et Amazon Project Kuiper[55]. L'Union Européenne a lancé en 2023 un projet de constellation satellitaire appelé IRIS [56] (Infrastructure for Resilience, Interconnection, and Security by Satellite), pour renforcer la souveraineté numérique, améliorer la connectivité

[54] OneWeb, Britannique, accent sur les gouvernements, les entreprises et les utilisateurs maritimes et aeriens. Cible les applications IdO dans les secteurs de l'industrie, de la logistique, du maritime, de l'aviation et les services d'urgence. https://oneweb.net/

[55] Amazon Project Kuiper, USA, vise a concurrencer directement Starlink. Amazon prevoit d'integrer ses services cloud avec la connectivite satellite pour des solutions IdO avancees. https://www.aboutamazon.com/what-we-do/devices-services/project-kuiper

[56] IRIS² | https://www.euspa.europa.eu/eu-space-programme/secure-satcom/iris2 Agence de l'UE pour le programme spatial (europa.eu)

et offrir des services de communication sécurisés, se positionnant comme une alternative aux constellations non européennes tels que Starlink et OneWeb. De plus, Kinéis, entreprise française, est principalement orientée vers le marché de l'IdO avec un réseau de petits satellites en orbite basse (LEO) qui offrirait une couverture mondiale et une communication de données à faible bande passante.

La forte croissance du marché des objets connectés est également attribuable à la demande des consommateurs pour des solutions pratiques et innovantes qui améliorent leur confort,

[60] https://www.tomsguide.fr/6g-le-reseau-sera-10-fois-plus-rapide-que-la-5g-mais-ne-sortira-pas-avant-2030/

[61] Starlink (SpaceX) USA, repose sur une constellation massive de satellites en orbite basse (LEO) pour réduire la latence. Cible les secteurs de l'agriculture, du transport, des infrastructures critiques et les opérations maritimes et aériennes. https://www.starlink.com/fr

leur bien-être et leur sécurité. Dans le secteur industriel, les objets connectés permettent une gestion plus efficace des ressources, une meilleure maintenance prédictive et une optimisation des opérations, ce qui contribue à accroître la productivité et à réduire les coûts.

Ces facteurs, associés aux technologies émergentes telles que l'IA, l'apprentissage automatique, et le big data, créent un environnement propice à l'expansion rapide de l'IdO.

III.3.1 Segmentation du marché de l'IdO par région

D'après les prévisions de Statista[65] en 2024, la Grande Chine devrait être la région comptant le plus d'appareils connectés à l'IdO d'ici 2030, avec plus de 8 milliards d'appareils. L'Amérique du Nord et L'Europe suivront.

En 2022, l'Allemagne dominait le marché de l'IdO grand public en Europe avec 5,7 milliards de dollars. Le marché allemand devrait croître à un taux annuel composé de 11,7 % entre 2023 et 2030, atteignant 13,8 milliards de dollars en 2030.

La Chine et l'Extrême-Orient représentent les marchés les plus importants pour la maison intelligente en termes de volume de ventes, avec 40 % des appareils fabriqués vendus dans cette région.

Le nombre de maisons intelligentes devrait dépasser 400 millions en 2024. Les assistants vocaux ou enceintes intelligentes, avec 40 millions d'unités vendues en 2022, sont le segment le plus populaire et devraient doubler en 2024.

[65] https://www.statista.com/statistics/1194715/iot -annual-revenue-regionally/

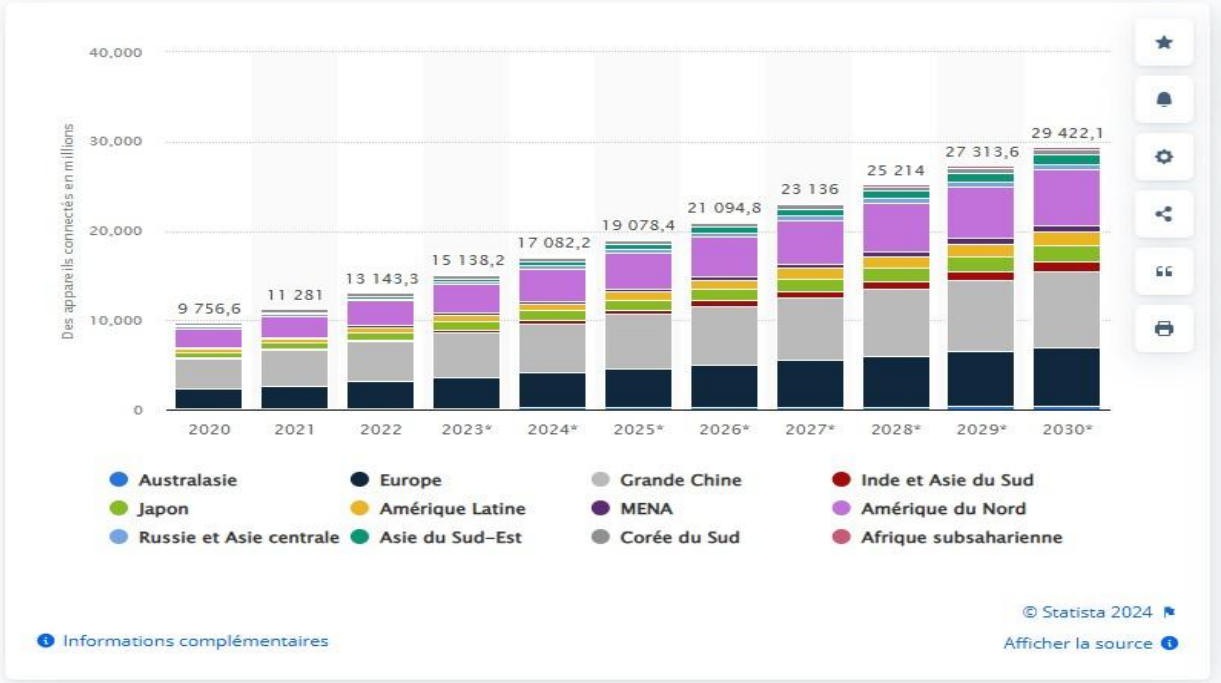


Figure 19 : Nombre (IdO) en millions par région de 2020 à 2030
Source : Chiffre d'affaires annuel de l'IdO par région 2030 | Statista

III.3.2 Segmentation du marché de l'IdO par application

Le marché de l'Internet des objets (IdO) est vaste et diversifié, avec des applications dans de nombreux secteurs. Voici une segmentation par application avec quelques chiffres clés :

- **Domotique** : Appareils connectés pour la maison intelligente (thermostats, éclairage, sécurité), colliers et bracelets pour animaux, etc…
- **Cités intelligentes** : Gestion du stationnement, amélioration du trafic, optimisation de l'éclairage, gestion des déchets, gestion des bornes de recharge électrique, etc…
- **Bâtiments intelligents** : Confort et bon cadre de vie aux occupants, maintenance préventive des bâtiments, bâtiments plus sûrs et maintenance énergétique, etc…
- **Industrie 4.0** : Logistique, maintenance prédictive, sécurité des équipes et des infrastructures, contrôle qualité de la production, gestion de l'énergie….
- **Santé et sécurité des personnes** : Téléassistance mobile et fixe, surveillance à distance de patients, bracelets pour senior ou travailleur isolé.
- **Transition énergétique** : Optimisation énergétique des bâtiments professionnels, des établissements publics et des habitats individuels
- **Agriculture** : Robots, stations météo connectées, boîtiers géo localisés sur tracteurs, etc…

Notre analyse étant axée sur les objets connectés destinés au grand public, nous nous concentrerons exclusivement sur les IdO de cette catégorie d'utilisateurs, incluant la domotique.

En septembre 2024, Statista[57] annonce qu'en 2022, il était enregistré dans le monde, près de :

- **340** millions d'écouteurs qui sont désormais les objets connectés portables les plus vendus.
- **135** millions de montres connectées offrant divers services tels que le suivi de la santé et des performances sportives via des applications comme Strava.

Sur ces deux segments, Apple reste leader avec **30 %** de parts de marché pour les smartwatchs en **2022**. Au total, la marque à la pomme aurait vendu pour plus de **8** milliards de dollars de montres, accessoires et objets connectés pour la maison au troisième trimestre **2023**.

Concernant le marché de la domotique ou maison intelligente, en 2024, le département de recherche de Statista[67] a publié que le nombre de maisons intelligentes dans le monde devrait augmenter continuellement entre 2023 et 2028, d'un total de 424,5 millions d'utilisateurs (+117,69 %). Ce chiffre devrait atteindre un nouveau sommet de 785,16 millions d'utilisateurs en 2028.

Le chiffre d'affaires [68] mondial du marché de la maison intelligente devrait croître continuellement entre 2023 et 2028, d'un un total de 96,7 milliards de dollars américains (soit 71,74 %). En 2028, ce chiffre devrait atteindre un pic de à 231,6 milliards de dollars.

Les enceintes intelligentes ou les assistants vocaux[58] sont parmi les objets de domotique les plus vendus. Entre 2024 et 2029, le volume mondial des assistants vocaux devrait croître de 135,4 millions d'unités (soit +59,52 %), atteignant un sommet de 362,89 millions d'unités en 2029.

En plus des services liés au divertissement, la domotique s'est développée sur la gestion énergétique et la sureté des logements. Au total, le chiffre d'affaires mondial des équipements connectés liés à la sécurité à domicile s'élevait à **3,3** milliards de dollars dans le monde en **2022**.

Des entreprises comme Google, Amazon et Apple ont popularisé les maisons intelligentes grâce à leurs assistants vocaux, devenus des centres de contrôle essentiels. Les fournisseurs chinois tels que Xiaomi, Baidu et Alibaba ont également contribué de manière significative aux ventes mondiales de ces appareils. En plus des assistants vocaux, ces entreprises élargissent leur offre avec des produits comme les sonnettes vidéo intelligentes, Ring d'Amazon et Nest de Google étant les leaders dans ce domaine en 2022.

Dans l'espace public, les outils de surveillance se développent de plus en plus. Il est estimé

[57] https://fr.statista.com/themes/2972/les-objets-connectes/#topicOverview
[58] https://www.statista.com/forecasts/1367982/smart-speaker-market-volume-worldwide

I. [67] HTTPS://WWW.STATISTA.COM/FORECASTS/887613/NUMBER-OF-SMART-HOMES-IN-THE-SMART-HOME-MARKET-IN-THEWORLD

II. [68] HTTPS://WWW.STATISTA.COM/FORECASTS/887554/REVENUE-IN-THE-SMART-HOME-MARKET-IN-THE-WORLD

que le chiffre d'affaires lié à la reconnaissance faciale augmentera de plus de **200 %** dans le monde entre **2021** et **2027**.

III.3.3 Segmentation du marché de l'IdO par technologie

Le déploiement des objets connectés continue de croître, renforçant la demande pour les réseaux IdO et stimulant l'émergence de nouvelles solutions. **Satellite, 5G, Sidewalk, NBIoT, LTE-M… de nouvelles topologies physiques arrivent pour les réseaux IdO.**

Dans l'environnement domestique, le Wifi domine. Toutefois, dès que la portée des répéteurs devient insuffisante, il devient nécessaire de recourir à d'autres solutions de connectivité telles que la 4G, la 5G ou les satellites, ce qui implique des investissements importants pour leur déploiement.

Figure 20 : Différentes connectivités des IdO
Source : https://www.zdnet.fr/blogs/green-si/quel-reseau-demain-pour-les-objets-connectes-39964316.htm

C'est ainsi qu'Amazon a lancé **Sidewalk**, un réseau qui exploite la connectivité locale pour faire fonctionner ses appareils Alexa (haut-parleurs connectés) et Ring (sonnettes et caméras) vendus à ses clients. Sur le marché de la domotique, le réseau Sidewalk couvre 90 % de la population américaine, presque par "design", puisque 90 % de la population est à proximité d'un appareil Alexa, que ce soit chez elle ou chez un voisin. Et cela sans investissement direct en infrastructure. **Amazon a ainsi pris une avance considérable aux États-Unis en créant une synergie entre ses services Cloud et un réseau de collecte de données à faible débit.**

Figure 21 : Couverture des IdO Sidewalk aux USA
Source : imgurl:https://www.zdnet.fr/wp-content/uploads/zdnet/2024/03/image_2024-02-18_214827883-2.png - Recherche (bing.com)

Sigfox[59], en revanche, a échoué en raison de la rude concurrence et du coût élevé de ses infrastructures. Le réseau a été démantelé après sa faillite, malgré son bon fonctionnement et ses clients.

Les **LPWAN** (Low Power Wide Area Networks) sont adaptés aux objets non connectés à une source électrique et dont les batteries devraient durer environ 10 ans. Ces réseaux pourraient se développer davantage pour les dispositifs nécessitant peu de bande passante et une faible consommation d'énergie, ce qui pourrait favoriser l'expansion de réseaux encore peu déployés comme **le NB-IoT (Narrow Band IoT) et le LTE-M (Long-Term Evolution for machines),** une déclinaison de la 4G spécialisée pour l'IoT.

La Chine est engagée massivement dans le NB-IoT. Des brevets chinois tirent aussi parti du NB-IoT et créent une autre dépendance. La domination du NB-IoT est donc fortement décentrée sur l'Asie et nettement moins sur les Amériques.

III.4 LES TENDANCES EMERGENTES

En plus d'une connectivité plus rapide et plus fiable grâce à l'adoption de la 5G, des technologies satellites et radio novatrices, les tendances émergentes dans le marché de l'Internet des objets (IdO) pour 2024 s'articulent autour de :

L'Edge AI, une tendance qui va transformer l'écosystème IdO, où le traitement de l'IA se fait directement dans les objets connectés, sans passer par le cloud. Avec des dispositifs plus puissants et des algorithmes améliorés, l'IA s'intègre de plus en plus dans notre quotidien, permettant aux objets de prendre des décisions en temps réel, indépendamment des

[59] Sigfox, fondée en 2010, elle était une entreprise française spécialisée dans les réseaux bas débit pour l'Internet des objets (IoT).

serveurs distants. Par exemple, les caméras de sécurité comme Nest Cam et Arlo analysent les images en temps réel pour détecter les mouvements suspects et identifier des

personnes. Les assistants vocaux tels qu'Amazon Echo et Google Nest Hub exécutent des commandes et contrôlent des dispositifs domestiques sans passer par le cloud.

L'interopérabilité de la domotique grâce à la norme Matter 1.2. Développée par la Connectivity Standards Alliance, Elle vise à assurer une intégration fluide entre dispositifs de différents fabricants et renforce la sécurité grâce à des mécanismes de chiffrement robustes. L'objectif est de simplifier l'expérience utilisateur et de promouvoir une adoption plus large des dispositifs connectés. Par exemple, avant Matter 1.2, vous deviez utiliser des applications distinctes pour contrôler une lampe Philips Hue et un thermostat Nest. Avec Matter 1.2, vous pouvez gérer ces appareils via une seule application compatible, comme Google Home, et créer des automatisations telles que régler la température lorsque vous allumez la lumière.

Enfin, **la sécurité des IdO** deviendra une priorité majeure. Les fabricants investiront davantage dans des solutions pour protéger les données des utilisateurs. Les réglementations concernant la protection des données personnelles collectées par les dispositifs IdO, abordées dans le chapitre III, ainsi que les lois sur l'intelligence artificielle, telles que la législation de l'Union européenne et le décret du président Biden, exigeront que les entreprises du secteur restent informées et se conforment aux normes en vigueur pour garantir une adoption sécurisée et éthique de ces technologies.

IV.Législation et réglementation de l'Internet des objets : Cadres juridiques et enjeux

IV. LEGISLATION ET REGLEMENTATION DE L'IDO : CADRES JURIDIQUES ET ENJEUX

Dans le cadre de notre étude portant sur les risques et la sécurité des objets connectés destinés au grand public, il convient de rappeler que nous avons sciemment écarté les segments liés à l'automobile[71], l'énergie[72] et la santé[73]. Ceux-ci sont suffisamment régulés, ce qui les rend moins vulnérables aux cyberattaques que les objets connectés liés à la domotique, au bien-être, aux dispositifs de géolocalisation et aux jouets numériques, objet de notre analyse.

FIGURE 22 : ILLUSTRATION DES OBJETS CONNECTES (IDO) GRAND PUBLIC

Source : Vos appareils intelligents partagent-ils vos informations personnelles ? (legalscoops.com)

On constate aujourd'hui une prolifération importante de ces objets connectés grand public. Des appareils tels que des ampoules, thermostats, caméras de surveillance, bracelets connectés et téléviseurs intelligents inondent de plus en plus nos marchés, tandis que les consommateurs investissent davantage dans ces technologies, qui leur permettent de réaliser des économies sur leur facture d'énergie tout en apportant confort et tranquillité au sein de leur foyer.

Néanmoins, ces objets, souvent fabriqués avec des normes de sécurité insuffisantes, sont vulnérables aux cybermenaces. Il suffit qu'ils soient connectés à Internet, allumés et non protégés pour offrir une opportunité redoutable aux pirates informatiques afin d'accéder à

[71] **UN R 155 et UN R 156** : Règlements de la CEE-ON, entrés en vigueur en juillet 2022, ils requièrent la mise en place d'un système de management de la cybersécurité et à garantir la sécurité des systèmes électroniques dans l'industrie automobile. **La norme ISO/SAE 21434** : Obligatoire, elle est utilisée comme références pour la conception sécurisée des systèmes embarqués et des communications dans les véhicules connectés.

[72] **Loi de Programmation Militaire (LPM) :** En France, elle inclut des mesures spécifiques visant à renforcer la protection et la sécurité des infrastructures critiques, y compris celles du secteur de l'énergie.

ISO 27019 : Norme spécifique pour la sécurité de l'information dans le secteur de l'énergie, fournissant des lignes directrices pour protéger les infrastructures critiques contre les menaces numériques.

[73] **Directive sur les dispositifs médicaux (MDR 2017/745) :** règlement de l'Union européenne adopté en mai 2017, il a pour but de renforcer la sécurité des dispositifs médicaux au sein de l'UE.

EN 60601-1 : Norme relative aux exigences générales pour la sécurité de base et les performances essentielles des appareils électromédicaux.

Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) : Elle fixe le cadre de la sécurisation des systèmes d'information de santé en France.

RGPD : en vigueur depuis mai 2018, impose des obligations strictes concernant la protection des données personnelles, y compris les données de santé.

des informations personnelles, de perturber les réseaux domestiques ou même de participer à des attaques massives contre d'autres systèmes.

Monsieur Bernard Benhamou, secrétaire général de l'Institut de la Souveraineté Numérique, lors de notre entretien, a mentionné que Mirai était l'un des logiciels malveillants les plus spectaculaires ayant marqué l'année 2016 en infectant des objets connectés. En exploitant des vulnérabilités sur des caméras et des routeurs domestiques, des attaques en déni de service distribué (DDoS) ont ciblé d'importants fournisseurs de services DNS, tels que Dyn. Ces attaques ont paralysé des géants du web tels qu'Amazon, Twitter, Netflix, GitHub, Spotify et OVH, ainsi que d'autres sites importants, rendant l'accès à ces services impossibles pour des millions de personnes à travers le monde pendant plusieurs heures. Le secrétaire général de l'Institut de la Souveraineté Numérique a également souligné un autre aspect important des objets connectés : ceux-ci pourraient transmettre, à l'insu de leurs utilisateurs, des informations sans lien avec leur fonction principale à des fins commerciales. Il a cité l'exemple de l'aspirateur autonome Roomba[60], qui récupérait les plans des pièces des maisons de ses clients grâce aux capacités cartographiques qui y étaient intégrées. À noter que d'autres exemples d'attaques sont cités dans le chapitre vulnérabilités.

Toutefois, la perception des cybermenaces liées aux objets connectés par le grand public reste insuffisante même si l'on observe une prise de conscience croissante des consommateurs quant aux risques associés à l'utilisation de ces technologies, notamment en ce qui concerne la sécurité des données personnelles. Cette sensibilisation est le fruit d'un travail continu mené par plusieurs organismes.

À titre d'exemple, la Commission nationale de l'informatique et des libertés (CNIL)[61] qui joue un rôle clé en sensibilisant le grand public aux enjeux de la vie privée et de la sécurité des données liées aux objets connectés. Nous citerons ses conseils sur l'utilisation des téléviseurs connectés[62], robots connectés [63], les jouets connectés[64] et notamment, les assistants vocaux qui font partie de notre quotidien. La CNIL a donc, publié un livre blanc intitulé "À votre écoute - Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux"[65] dans lequel elle met en lumière les défis posés par la collecte de données personnelles via les commandes vocales, alors que la voix est une caractéristique biométrique pouvant permettre l'identification d'une personne.

Le site Cybermalveillance.gouv.fr contribue activement à la sensibilisation du grand public aux cyberattaques, y compris celles ciblant les objets connectés, en offrant des outils, des informations et un soutien pour améliorer la sécurité numérique. En collaboration avec la CNIL et l'Unaf[66], deux supports de sensibilisation ont été spécialement conçus et publiés en

[60] Rapport intitulé : Internet des objets & souveraineté numérique - Perspectives industrielles et enjeux de régulation, Coordonné par Bernard Benhamou, Secrétaire général de l'Institut de la Souveraineté Numérique, p. 102.
[61] https://www.cnil.fr/fr/technologies/objets-connectes
[62] https://www.cnil.fr/fr/televiseurs-connectes-les-conseils-de-la-cnil
[63] https://www.cnil.fr/fr/robots-connectes-et-donnees-personnelles-les-conseils-de-la-cnil
[64] https://www.cnil.fr/fr/jouets-connectes-quels-conseils-pour-les-securiser
[65] https://www.cnil.fr/fr/votre-ecoute-la-cnil-publie-son-livre-blanc-sur-les-assistants-vocaux
[66] Unaf - Assistance aux victimes de cybermalveillance

juin 2024 pour aider les familles et les seniors à adopter les bonnes pratiques et à naviguer en toute sécurité dans l'univers numérique[67].

De même, la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF) fournit des conseils pratiques au public, notamment en encourageant à s'informer avant l'achat, à effectuer des mises à jour régulières, à modifier les mots de passe par défaut et à limiter l'accès des objets connectés à d'autres appareils électroniques[68]. En mai 2024, nous avons sollicité la DGCCRF pour nous apporter des éléments sur les lois, règlements, menaces, contrôle de la cybersécurité des objets connectés fabriqués en France ou importés et mis sur le marché français à destination du grand public. La réponse Madame Marine SEDIRA, Responsable événementiel à la DGCCRF fut la suivante : "*Les résultats et retours des contrôles seront connus l'année prochaine et le bureau métier vient de créer un poste justement sur ce sujet. Le sujet est extrêmement intéressant, porteur et vaste"*, ce qui témoigne de l'importance qui est accordée à cette question par cette Direction. Vous pouvez consulter l'échange de mail en annexe.

De plus, plusieurs travaux ont été publiés sur le sujet de l'Internet des Objets destinés au grand public. Le rapport de France Stratégie, intitulé "Le monde de l'Internet des objets : des dynamiques à maîtriser", explore les différentes dynamiques de l'IdO, soulignant son impact significatif sur divers aspects de notre vie quotidienne et économique. Il examine les stratégies nécessaires pour en tirer le meilleur parti tout en maîtrisant ses effets. D'autre part, le rapport conjoint de l'Association Française pour le Nommage Internet en Coopération (AFNIC) et de l'Institut de la Souveraineté Numérique, intitulé "Internet des Objets & Souveraineté Numérique - Perspectives industrielles et enjeux de régulation", se concentre spécifiquement sur les implications de l'IdO dans le contexte de la souveraineté numérique.

Toutefois, ces louables efforts et actions d'information et d'éducation ne permettent pas toujours au consommateur de s'approprier ces objets et surtout de se protéger des risques potentiels. Les causes de cette difficulté résident parfois dans un manque de clarté dans la communication des risques par les fabricants ou dans la complexité perçue de l'utilisation de ces technologies.

Il est donc évident que la sensibilisation aux menaces potentielles, bien que fondamentale, n'est pas suffisante pour protéger les consommateurs. Les objets connectés destinés au grand public offrent un potentiel de croissance significatif, nécessitant des actions plus audacieuses en termes de protection contre les risques cyber.

IV.1 COMPRENDRE LA REGLEMENTATION DES OBJETS CONNECTES

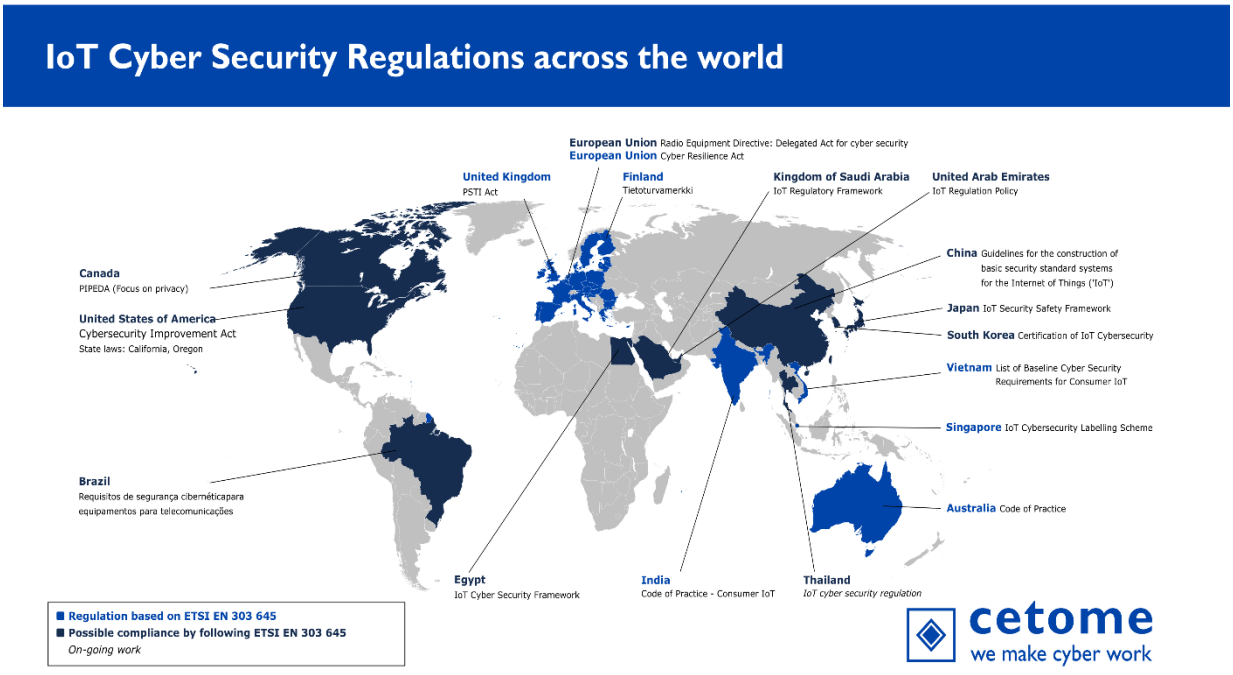
[67] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermalveillance-gouv-fr-cnil-unaf-reflexes-cyber-famillesseniors
[68] https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/objets-connectes

L'année 2024 est une année charnière dans l'évolution de la réglementation de la cybersécurité des objets connectés, elle est marquée par des progrès significatifs dans les lois et réglementations en vigueur au sein de certaines juridictions, telles que l'Union

Européenne, les États-Unis et le Royaume Uni. Bien que ces pays aient déjà mis en œuvre un arsenal réglementaire solide pour renforcer la cybersécurité, **il n'existe toujours pas de réglementation complète et spécifique en vigueur visant directement à protéger le grand public contre les risques cyber liés aux objets connectés.**

Dans ce contexte, plusieurs états se mobilisent par la mise en œuvre d'un cadre juridique visant à garantir que les fabricants mettent en place des mesures de sécurité adéquates. Celles-ci s'alignent avec les approches de la « Security by Design » et de la « Privacy by Design » lors de la conception et de la fabrication. Ces deux concepts fondamentaux permettent de développer des systèmes robustes et fiables, réduisant ainsi le risque de cyberattaques et de violations de données, y compris sur les objets connectés.
Ces mesures auront un impact à la fois sur les fabricants et sur le grand public. Cela signifie que les fabricants sont obligés de garantir un certain niveau de protection contre les vulnérabilités actuelles et futures, ce qui nécessite des investissements supplémentaires dans le développement et la maintenance de produits sécurisés. Les consommateurs, quant à eux, bénéficieront de produits plus sûrs et plus fiables, probablement plus chers, mais avec moins de risques d'exploitation de leurs données personnelles et d'intrusion dans leur vie privée. La confiance dans les technologies de l'internet des objets sera ainsi renforcée, ce qui facilitera leur intégration dans la vie quotidienne.

La figure ci-dessous illustre le panorama des réglementations en matière de cybersécurité des objets connectés à travers le monde, établi par le cabinet de conseil indépendant en sécurité, Cetome[69].



[69] https://cetome.com/panorama

Figure 23 : Réglementations Mondiales des Objets Connectés

Source : https://cetome.com/panorama

Dans ce qui suit, nous examinerons les lois et directives essentielles pour la sécurité des objets connectés et explorerons le contexte et les implications de ces initiatives.

IV.2 AU ROYAUME UNI

IV.2.1 Loi sur la sécurité des produits et des infrastructures de télécommunications.

Entrée en vigueur le 29 avril 2024, la Loi sur la sécurité des produits et des infrastructures de télécommunications, connu également sous le nom de "Product Security and Telecommunications Infrastructure (PSTI) Act" est une nouvelle législation obligatoires au Royaume-Uni constituée de deux parties : la première établit de nouvelles exigences de sécurité pour les « objets connectés » et la deuxième couvre les modifications apportées au code des communications électroniques du Royaume-Uni, qui régit l'accès aux infrastructures de télécommunications, et qui n'est pas couverte par ce document.

La première partie de cette législation a un impact direct sur les entreprises fabricant des objets connectés destinés au grand public. Il s'agit de décharger les consommateurs de la responsabilité de sécuriser leurs propres appareils en veillant à ce qu'une cybersécurité solide soit intégrée dans ces produits dès leur conception. Cela implique la conformité aux nouvelles exigences de sécurité des produits connectés à savoir : des mots de passe uniques qui ne peuvent pas être réinitialisés aux paramètres d'usine, des informations claires sur la période d'assistance, y compris les mises à jour et les correctifs de sécurité vitaux, le signalement des vulnérabilités de sécurité par les fabricants, et enfin la délivrance d'une déclaration de conformité pour chaque dispositif mis sur le marché.

Les fabricants qui enfreignent cette nouvelle législation seront passibles d'amendes allant jusqu'à 10 millions de livres sterling ou 4 % de leur chiffre d'affaires mondial. Il y a une pénalité supplémentaire pouvant aller jusqu'à 20 000 £ par jour en cas de violation continue par la suite. L'Office for Product Safety and Standards (OPSS) est responsable de l'application de cette loi depuis le 29 avril 2024[70].

Cette décision du Royaume-Uni s'aligne étroitement avec la loi sur la cyber-résilience de l'Union Européenne, créant un cadre comparable pour les normes de cybersécurité des objets connectés.

[70] https://www.complianceandrisks.com/blog/the-product-security-and-telecommunications-act-psti-what-you-need-to-know/

IV.3 EN EUROPE

IV.3.1 R*èglemen*t délégué (UE) 2022/30 complétant la Directive dite RED

La directive RED (directive européenne 2014/53/UE) est une législation de l'Union Européenne qui définit des exigences essentielles en matière de sécurité, de santé, de compatibilité électromagnétique et d'utilisation efficace du spectre radio des équipements radioélectriques.

L'acte délégué (UE) 2022/30 est venu la compléter pour intégrer des éléments relatifs à la cybersécurité et à la protection des données des appareils sans fil avant leur vente sur le marché de l'UE. Ces mesures couvrent des appareils tels que les téléphones portables, les montres connectées, les trackers de fitness et les jouets sans fil qui sont de plus en plus présents dans notre quotidien.
Cette loi fixe de nouvelles exigences légales en matière de protection de la cybersécurité, que les fabricants devront prendre en compte dans la conception et la production des produits concernés.

Les appareils devront donc renforcer la résilience des réseaux en intégrant des fonctionnalités pour prévenir les dommages aux réseaux de communication et empêcher leur utilisation pour perturber des sites web ou d'autres services. Ils devront également mieux protéger la vie privée des consommateurs et les droits des enfants en intégrant des mesures pour empêcher l'accès ou la transmission non autorisé de données personnelles et enfin réduire le risque de fraude monétaire, notamment en améliorant le contrôle de l'authentification des utilisateurs pour éviter les paiements frauduleux.

Figure 24 : LOGO CE
Source : Marquage CE — Wikipédia (wikipedia.org)

L'acte délégué sera complété par une loi sur la cyber-résilience (Cyber Resilience Act), visant à couvrir davantage de produits, en examinant l'ensemble de leur cycle de vie.

En août 2022, la Commission Européenne avait demandé au Comité européen de normalisation (CEN) et au Comité européen de normalisation électrotechnique (CENELEC) d'élaborer de nouvelles normes harmonisées pour les équipements radioélectriques spécifiés dans ce règlement. Cependant, Le CEN et le CENELEC ont demandé une prolongation de la période spécifiée dans la demande afin de pouvoir traiter les questions complexes et les problèmes rencontrés et fournir des normes harmonisées de haute qualité. Le 20 juillet 2023, la Commission européenne a décidé de reporter la date d'application du Règlement délégué (UE) 2022/30. Initialement prévue pour le 1er août 2024, la nouvelle date pourrait être décalée d'un an, soit au 1er août 2025.

IV.3.2 Règlement Général sur la Protection des Données (RGPD 95/46/CE)

Instauré par l'union européenne le 14 avril 2016 et effectif depuis le 25 mai 2018 dans l'UE et le Royaume-Uni, le RGPD est un cadre réglementaire qui vise à renforcer les droits des personnes physiques en matière de protection des données personnelles, qui jusqu'ici l'étaient par la loi française Informatique et libertés de 1978 sous l'égide de la CNIL (Commission Nationale de l'Informatique et des Libertés).

Il s'applique à toutes les organisations qui traitent des données personnelles des résidents européens en exigeant qu'elles soient traitées de manière sécurisée, proposant des sanctions accrues pour les entreprises non conformes, pouvant atteindre jusqu'à 4% de leur chiffre d'affaires annuel mondial ou 20 millions d'euros, le montant le plus élevé étant retenu.

Les objets connectés fonctionnant grâce aux données personnelles de leurs utilisateurs, se voient directement impactés par l'application du ce règlement. Ces objets doivent respecter les principes fondamentaux de traitement des données à caractère personnel, tels que leur minimisation ainsi que la préservation de leur intégrité et de leur confidentialité. Il est également essentiel d'assurer la transparence avec les personnes concernées et de protéger ces informations contre toute violation. Plutôt qu'un contrôle a posteriori, le RGPD a instauré un état d'esprit basé sur la notion de 'privacy by design', visant à ne collecter que les données strictement nécessaires pour le fonctionnement des objets connectés.

Des mesures techniques et organisationnelles adéquates devront également être entreprises afin d'assurer la traçabilité des données personnelles. En cas de fuite de données, les fabricants ont l'obligation d'en informer la CNIL ainsi que les utilisateurs concernés dans un délai de 72 heures.

Bien que le RGPD serve de modèle inspirant pour d'autres régions du monde, démontrant qu'il est possible de concilier progrès technologique et respect de la vie privée, il ne garantit pas une protection totale à lui seul. Il est indispensable d'agir sur d'autres leviers pour garantir que les objets connectés soient sécurisés et que les utilisateurs soient vigilants et conscients des risques.

IV.3.3 La loi sur la cybersécurité de l'Union européenne

La loi sur la cybersécurité de l'Union européenne (règlement (UE) 2019/881 du 17 avril 2019), également connue sous le nom de Cybersecurity Act, est entrée en vigueur depuis le 27 juin 2019 dans l'UE et au Royaume-Uni. Cette législation vise à renforcer la sécurité des produits, services et processus liés aux technologies de l'information et de la communication (TIC) en établissant un cadre pour la certification de la cybersécurité de ces technologies au sein de l'UE.
Avec l'adoption de cette loi, l'Agence Européenne Chargée de la Sécurité des Réseaux et de l'Information, connue en anglais sous le nom de European Network and Information Security Agency (ENISA) [71], a été renommée Agence de l'Union Européenne pour la Cybersécurité. Cependant, l'acronyme historique ENISA a été conservé pour des raisons de continuité et de reconnaissance. Le rôle de l'ENISA a ainsi été renforcé, avec davantage de ressources et de responsabilités pour mieux soutenir les États membres, les institutions de l'UE, ainsi que les entreprises en matière de cybersécurité.

Le 31 janvier 2024, la Commission Européenne a annoncé l'adoption du premier schéma de certification européen, EUCC (EU Common Criteria)[72], aligné sur les réglementations en cybersécurité de l'UE. Il sera publié au Journal officiel de l'UE et entrera en vigueur 20 jours après, avec les premiers certificats disponibles un an plus tard. Le schéma EUCC harmonise les règles de certification pour les produits TIC dans l'UE et intègre les caractéristiques des schémas nationaux existants. L'ANSSI, représentant la France, a contribué à son élaboration et sera responsable de délivrer les certifications en France. Ce schéma volontaire soutient les récentes évolutions du cadre européen en matière de cybersécurité, notamment la législation sur la cyber résilience, qui sera abordée ci-dessous et qui imposera des exigences strictes pour tous les produits matériels et logiciels dans l'UE ainsi que celles introduites par la directive NIS 2[73] et le règlement eIDAS V2[74].

Le groupe européen de certification de cybersécurité, en anglais, European Cybersecurity Certification Group (ECCG) est un organe consultatif créé dans le cadre de la loi sur la cybersécurité de l'UE. Son rôle principal est de conseiller et d'assister la Commission européenne dans l'élaboration et la mise en œuvre des schémas de certification de cybersécurité à l'échelle européenne.

L'ANSSI, en tant qu'autorité compétente représentant la France au sein de l'ECCG, se prépare à devenir l'Autorité Nationale de Certification de Cybersécurité (ANCC)[75]. À ce titre, l'ANSSI sera responsable de surveiller la bonne application des différents schémas de certification européens en France. Elle se prépare également à certifier les services nécessitant un niveau d'assurance élevé, conformément à cette même législation, qui exige que ces certificats soient délivrés par une ANCC.

---

[71] ENISA signifie Agence de l'Union européenne pour la cybersécurité. L'acronyme "ENISA" provient du nom original de l'agence, à savoir l'Agence européenne chargée de la sécurité des réseaux et de l'information, avant qu'elle ne soit renommée pour refléter son mandat élargi en matière de cybersécurité.
[72] EUCC, premier schéma européen de certification de cybersécurité adopté | ANSSI
Règlement d'exécution relatif à l'adoption d'un système européen de certification de cybersécurité fondé sur des critères communs | Façonner l'avenir numérique de l'Europe (europa.eu)
[73] La directive NIS 2 (Network and Information Systems Directive 2) est une mise à jour de la première directive NIS 1, adoptée par l'Union européenne pour renforcer la cybersécurité des réseaux et systèmes d'information.
[74] Le règlement eIDAS V2 (Electronic Identification, Authentication and Trust Services, version 2) est une révision du règlement eIDAS original de l'Union européenne.
[75] Cybersecurity Act | ANSSI

À l'avenir, il est prévu que la certification de cybersécurité devienne obligatoire pour certains produits, notamment les appareils IdO (Internet des Objets). Ces appareils conformes seront étiquetés pour indiquer leur conformité aux normes de cybersécurité de l'UE, ce qui aidera les consommateurs à identifier facilement les produits sécurisés.

Alors que le règlement (UE) 2019/881 établit des schémas de certification pour garantir que les produits, services et processus adhèrent à des normes de sécurité élevées, la loi sur la cyber résilience met l'accent sur l'intégration de la sécurité dès la conception des produits

numériques. Ensemble, ces deux initiatives constituent un cadre complet pour la cybersécurité au sein de l'UE, en couvrant à la fois la conception sécurisée des produits et la certification de leur conformité en matière de sécurité.

IV.3.4 La proposition de loi de l'Union Européenne sur la cyber-résilience

La proposition de loi de l'UE sur la Cyber-Résilience, connue également sous le nom de "Cyber Resilience Act (CRA)" a été annoncée par la présidente de la Commission Européenne, Ursula von der Leyen en septembre 2021, lors de son discours sur la stratégie de l'UE en matière de cybersécurité. Cette législation, la première du genre à l'échelle de l'UE, viendra compléter d'autres législations dans ce domaine, en particulier, le règlement sur la cybersécurité de l'UE, la directive sur la sécurité des réseaux et des systèmes d'information (NIS 2) et le règlement général sur la protection des données (RGPD).

Cette loi aura pour objectif de garantir que les produits connectés à Internet et les logiciels mis sur le marché de l'UE soient plus sécurisés, que les fabricants soient responsables de la cybersécurité d'un produit tout au long de son cycle de vie et que les consommateurs soient informés en amont sur le niveau de cybersécurité des produits qu'ils achètent et utilisent. Ces exigences seront introduites sur un large éventail de produits, tels que les jouets et les appareils électroniques.

Le système d'alerte de l'UE, qui sera mis en place, permettra aux autorités nationales de préserver la sécurité des consommateurs et des entreprises, si des produits non conformes sont détectés.

Figure 25 : Logo de l'EU Cyber Resilience Act
Source **:** Loi sur la cyberrésilience | Façonner l'avenir numérique de l'Europe (europa.eu)

De telles obligations concernent les opérateurs économiques : des fabricants aux distributeurs et importateurs. Les fabricants devront subir un processus d'évaluation de la conformité pour démontrer si les exigences spécifiées relatives à un produit ont été remplies. Lorsque la conformité du produit aux exigences de cybersécurité applicables aura été démontrée, les fabricants et les développeurs établiront une déclaration de conformité UE et pourront apposer la marque CE.

La marque CE indiquera la conformité des produits numériques avec le Cyber Resilience Act, permettant leur libre circulation dans l'UE. Le grand public et les entreprises seraient, donc, en mesure de faire des choix plus éclairés et en toute confiance.
Les États membres nommeront des autorités de surveillance du marché, qui seront chargées de veiller au respect des obligations du Cyber Resilience Act. En cas de nonconformité, il sera demandé aux opérateurs d'éliminer le risque, de prohiber ou de restreindre la mise à disposition d'un produit sur le marché, ou d'ordonner le retrait ou le rappel du produit. Chacune de ces autorités pourra infliger des amendes aux entreprises qui ne respectent pas les règles. Le Cyber Resilience Act établit des niveaux d'amendes administratives qui devraient être prévus dans les lois nationales en cas de non-conformité.

Il y a lieu de rappeler que la proposition du règlement sur la cyber-résilience a été publiée le 15 septembre 2022. Le 30 novembre 2023, le Parlement européen et le Conseil sont parvenus à un accord politique. À la suite de cet accord, le texte a été voté par le Parlement le 12 mars 2024. Il devra à présent être formellement adopté par le Conseil et entrera en vigueur 20 jours après sa publication au Journal officiel de l'Union européenne.

Le règlement devrait, donc, entrer en vigueur au second semestre de 2024. Les opérateurs économiques et les États membres auront 36 mois pour s'adapter aux nouvelles exigences. Une exception à cette règle est l'obligation, pour les fabricants, de déclarer les vulnérabilités et incidents activement exploités, qui s'appliqueraient 21 mois après l'entrée en vigueur, car elles nécessitent moins d'ajustements organisationnels que les autres nouvelles obligations. La Commission demandera aux organisations européennes de normalisation de développer des normes techniques pour de nombreuses catégories de produits couvertes par le Cyber Resilience Act, qui s'adresse, en particulier, aux fabricants des produits numériques essentiels pour la sécurité et le bon fonctionnement des infrastructures critiques et des services essentiels. La Commission examinera ensuite périodiquement la loi et fera un rapport sur son fonctionnement.

En somme, la loi sur la cyber résilience introduit des exigences obligatoires pour les fabricants de produits numériques, incluant logiciels, matériel et dispositifs IdO, afin d'assurer le respect des normes de cybersécurité dès la conception et tout au long du cycle de vie des produits. Le Cyber Resilience Act vise à établir des normes uniformes en cybersécurité à travers l'UE, réduisant ainsi les incidents, les coûts de remédiation et les impacts négatifs, tout en renforçant la confiance du grand public et en protégeant les droits fondamentaux des consommateurs, notamment en matière de protection des données personnelles et de la vie privée. Elle impose également des obligations légales et des sanctions pour non-conformité, créant ainsi un environnement d'application plus rigoureux.

IV.4 AUX ETATS-UNIS D'AMERIQUE

IV.4.1 Loi américaine sur l'amélioration de la cybersécurité des (IdO).

En 2024, il n'existe toujours pas aux États-Unis de cadre réglementaire national ni d'ensemble complet de normes en matière de cybersécurité pour les objets connectés. En mars 2019, la loi sur l'amélioration de la cybersécurité de l'IdO, connue également sous le nom de "US IOT Cybersecurity Improvement Act" a été introduite par des membres du Sénat américain (S.734) et de la Chambre des représentants (H.R. 1668). Adoptée le 4 décembre 2020, cette loi vise à sécuriser les dispositifs IdO utilisés au sein du gouvernement fédéral afin de protéger les infrastructures critiques contre les cybermenaces. Les agences fédérales doivent s'assurer que les appareils IdO qu'elles utilisent répondent à certaines exigences de sécurité, telles que la gestion des vulnérabilités, l'authentification forte et les mises à jour régulières des logiciels.

Le National Institute of Standards and Technology (NIST) est chargé de développer des normes et des directives spécifiques pour ces appareils IdO. Tout achat gouvernemental doit être conforme à ces directives. Les fabricants qui ne suivent pas ces recommandations se verront refuser l'accès aux vastes marchés du gouvernement fédéral. La loi appelle également les fabricants d'appareils IdO à adopter des politiques de communication coordonnée, garantissant un partage rapide des informations en cas de découverte de vulnérabilités. En vertu de cette loi, les agences fédérales américaines ne sont pas autorisées à acquérir ou à utiliser des appareils IdO jugés « non conformes » par le NIST à partir du 4 décembre 2022. Les auteurs de cette loi ont évité de réglementer directement le secteur privé, afin de ne pas freiner l'innovation.

IV.4.2 Loi californienne sur la cybersécurité de l'IdO SB-327

La Californie a adopté la première loi américaine sur la cybersécurité des objets connectés avec le projet de loi SB-327[76], voté en août 2018 et effectif le 1er janvier 2020. Cette loi oblige les fabricants de tout appareil connecté à Internet, directement ou indirectement, à intégrer des mesures de sécurité « raisonnables » pour prévenir les accès et modifications de données non autorisés.

Elle exige des identifiants uniques par dispositif et la création de nouveaux mots de passe par les utilisateurs lors de la configuration initiale. L'objectif est de mieux gérer les risques associés à l'augmentation de la connectivité. La loi s'applique à toutes les entités qui fabriquent des appareils connectés mis en vente en Californie. La loi n'énonce ni sanctions ni amendes précises, mais confère aux procureurs généraux et locaux le pouvoir exclusif d'application de la loi.

Les « caractéristiques de sécurité raisonnable » ne sont plus une option en Californie même si plusieurs observateurs déclarent que le texte de loi reste vague et manque d'instructions

[76] California IoT Cybersecurity Law SB-327

détaillées pour les fabricants d'objets connectés. Cependant, la loi californienne SB-327 est un premier pas important vers le renforcement de la sécurité des objets connectés dans cet état.

En résumé, la loi californienne sur la cybersécurité des objets connectés (SB-327) s'applique uniquement aux fabricants vendant des appareils connectés à Internet en Californie. En revanche, la loi américaine sur l'amélioration de la cybersécurité des objets connectés établit des normes pour les appareils utilisés par les agences gouvernementales et s'applique à l'ensemble des États-Unis. Ces deux lois peuvent donc coexister et se compléter pour renforcer la cybersécurité des appareils IdO.

IV.4.3 Marque de confiance en cybersécurité des États-Unis.

Le décret présidentiel 14028, promulgué par le Président des États-Unis, Joe Biden, le 12 mai 2021, vise à renforcer la cybersécurité en réponse aux cyberattaques malveillantes persistantes et de plus en plus sophistiquées qui menacent le secteur public, le secteur privé, ainsi que la sécurité et la vie privée du peuple américain.

Pour ce faire, le NIST a été chargé de mettre en œuvre plusieurs programmes, notamment la cybersécurité pour les IdO du grand public et la Federal Communications Commission (FCC) gérera son implémentation.

Le 18 juillet 2023, l'administration Biden-Harris annonce le “US CYBER TRUST MARK” visant à créer un label de certification volontaire pour les appareils IdO destinés au grand public et qui répondent à des critères de sécurité spécifiques, tels que la protection des données personnelles, la résilience face aux attaques cybernétiques, et les mises à jour de sécurité régulières.

Figure 26 : Label de Confiance Cyber des USA
Source **:** L’étiquette U.S. Cyber Trust Mark permettra aux utilisateurs de choisir les bons appareils intelligents (androidheadlines.com)

L'objectif est de fournir aux consommateurs américains des outils leur permettant de prendre des décisions éclairées sur la sécurité relative à des produits qu'ils choisissent d'introduire dans leur foyer.

Les participants à l'annonce incluent : Amazon, Best Buy, Carnegie Mellon University, CyLab, Cisco Systems, Connectivity Standards Alliance, Consumer Reports, Consumer Technology Association, Google, Infineon, Information Technology Industry Council, IoXT, KeySight, LG Electronics U.S.A., Logitech, OpenPolicy, Qorvo, Qualcomm, Samsung Electronics, UL Solutions, Yale et August U.S. Le programme devrait être opérationnel en 2024 et s'appuiera sur des critères de cybersécurité spécifiques publiés par le National Institute of Standards and Technology (NIST).

Contrairement à l'IoT Cybersecurity Improvement Act, qui est obligatoire pour les appareils utilisés par les agences fédérales, le Cyber Trust Mark est volontaire pour les fabricants de produits IdO grand public.

IV.4.4 Le CLOUD Act

Bien que nous ayons choisi de nous concentrer sur les lois et règlements directement liés aux dispositifs IdO, nous avons jugé utile d'aborder le CLOUD[77] Act américain en raison de ses implications sur les données personnelles, y compris celles collectées par les objets connectés et de son conflit avec le RGPD.

Issu à l'origine d'un contentieux entre Microsoft et le gouvernement des États-Unis, le CLOUD Act, ou loi sur la clarification de l'utilisation légale des données à l'étranger, est une loi fédérale américaine adoptée en 2018. Elle permet à l'administration américaine d'accéder aux données privées détenues par entreprises basées aux États-Unis ou de nationalité américaine, quel que soit leur pays d'implantation. Son objectif est de faciliter l'accès à ces données dans le cadre d'enquêtes, sans recourir à une demande d'entraide judiciaire internationale. Parmi les entreprises concernées, on peut citer des géants tels que Facebook, Google ou Microsoft.

Figure 27 : Grand sceau des États-Unis
Source : Great Seal of the United States (obverse) - Loi sur les communications stockées — Wikipédia (wikipedia.org)

[77] Clarifying Lawful Overseas Use of Data Act

92 Microsoft Corp. c. États-Unis — Wikipédia (wikipedia.org)

Cette loi a soulevé de nombreuses questions et débats sur la protection des données personnelles, la souveraineté des États et la coopération internationale. Comme de nombreuses lois américaines à portée extraterritoriale, cette législation prévaut de facto sur la législation du pays où l'entité est implantée et offre ainsi au gouvernement américain un outil de contrôle potentiellement puissant.

Un conflit est apparu entre le RGPD et le CLOUD Act depuis son adoption en 2018. Selon l'article 48 du RGPD, une décision d'un pays tiers exigeant le transfert ou la divulgation de données personnelles ne peut être reconnue ou exécutée que si elle repose sur un accord international, comme un traité d'entraide judiciaire. Or, le Cloud Act, qui n'est pas un accord international, ne respecte pas ces exigences.

Un exemple notable de ce conflit est l'affaire **Microsoft Corp. v. United States**[92]. En 2013, le gouvernement américain a exigé que Microsoft lui fournisse des courriels stockés sur un serveur en Irlande pour une enquête criminelle. Microsoft a contesté cette demande,

arguant que les données étrangères ne devraient pas être soumises à la juridiction américaine sans passer par des accords d'entraide judiciaire. Avant qu'une décision ne soit rendue par la Cour suprême des États-Unis, le CLOUD Act a été adopté en mars 2018. Cette loi a permis de résoudre le conflit en autorisant les autorités américaines à accéder aux données stockées à l'étranger par des entreprises américaines, tout en introduisant des mécanismes pour contester ces demandes en cas de conflit avec les lois locales.

Ainsi, les données traitées et stockées en Europe peuvent être soumises aux lois américaines et réclamées par le gouvernement des États-Unis. Par ailleurs, l'effet extraterritorial des lois dans le domaine numérique ne se limite pas au CLOUD Act : de plus en plus de législations, comme le RGPD, le Digital Markets Act (DMA)[78] et le Digital Services Act (DSA)[79], ont aussi cet effet au-delà des frontières. Ce phénomène s'étend également à d'autres régions du monde, comme l'Australie, l'Afrique du Sud, l'Inde et la Chine. La loi chinoise sur la sécurité des données (DSL), par exemple, s'applique aux données situées à l'étranger lorsqu'elles sont jugées pertinentes pour la sécurité nationale de la Chine, répondant en partie au CLOUD Act américain.

L'Union Européenne cherche à renforcer la sécurité des données personnelles en imposant un cadre international pour leur transfert. Le 27 juin 2023, le Conseil de l'UE a définitivement adopté le règlement **e-Evidence**, un texte qui, à l'image du CLOUD Act américain, permet aux autorités judiciaires des pays de l'UE de demander directement des preuves numériques aux fournisseurs de services, sans devoir passer par les autorités du pays où sont stockées ces données. Même s'il ne s'agit pas d'une réponse directe au CLOUD Act, l'e-Evidence

[78] Loi sur les marchés numériques (DMA) **https://digital-markets-act.ec.europa.eu/legislation_en**

[79] Loi sur les services numériques (DSA) **https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digitalage/digital-services-act_en**

s'inscrit dans une tendance globale visant à adapter les lois aux défis posés par les données numériques, souvent stockées au-delà des frontières.

Dans un contexte où le Cloud Act, en tant que loi extraterritoriale, et la prédominance des éditeurs américains sur les données numériques peuvent menacer la souveraineté des données personnelles, il est capital que l'UE établisse des accords internationaux qui assurent une protection élevée des données personnelles à l'échelle mondiale. En attendant, des solutions comme le recours à des fournisseurs de services cloud basés en Europe et le chiffrement des données, offrent des alternatives efficaces pour contrer les effets des lois extraterritoriales.

IV.5 PERSPECTIVES ET EVOLUTIONS DE LA REGLEMENTATION DES OBJETS (IDO) GRAND PUBLIC

Il ressort de ce qui précède qu'il n'existe pas de réglementation dédiée et en vigueur visant spécifiquement à sécuriser les objets connectés destinés au grand public, à l'exception de quelques lois en application, notamment en Angleterre et en Californie.

Cependant, plusieurs lois sont en vigueur, mais applicables à des domaines spécifiques de l'internet des objets, parfois volontaires, et ne couvrant que certaines parties de cet écosystème. En Europe et en France, ce constat est confirmé dans le rapport de France Stratégie, intitulé « *Le monde de l'Internet des objets : des dynamiques à maîtriser", où l'on peut lire que « l'Internet des objets se fonde sur un cadre de régulation déjà riche, avec de nombreuses dispositions au niveau européen et national, mais fragmenté et générateur de complexité, pour les entreprises notamment* ». Le rapport recommande particulièrement, « d'analyser *l'opportunité d'une loi cyber globale »*.

Dans ce contexte, il est essentiel de souligner que l'année 2024 constitue un tournant majeur, marquant une prise de conscience des grandes puissances internationales quant à la nécessité d'établir une régulation plus cohérente et complète pour sécuriser l'Internet des Objets.

En effet, plusieurs régulateurs à l'échelle mondiale mettent progressivement en place des cadres législatifs en réponse aux risques croissants associés à la prolifération des objets connectés dans la vie du grand public. Ce cadre réglementaire imposera des normes de sécurité aux fabricants, les incitant à investir dans la sécurité et la conformité. Cela entraînera une augmentation des coûts de production et d'exploitation, impactant ainsi les

prix d'achat des objets connectés pour le grand public. D'un point de vue économique, les exigences réglementaires pourraient freiner l'innovation et retarder le lancement de nouveaux produits, limitant ainsi la disponibilité des dernières technologies pour les consommateurs. De plus, les petites entreprises pourraient éprouver des difficultés à se conformer à ces normes strictes, ce qui réduirait leur présence sur le marché. Sur le plan des échanges internationaux, la diversité des réglementations compliquerait la conformité, la rendant chronophage et coûteuse pour les fabricants opérant sur ces marchés.

Bien que les avantages de la réglementation des objets connectés soient justifiés par la promotion d'une utilisation sûre et responsable de ces technologies et par la prévention des coûts bien plus élevés engendrés par une cyberattaque réussie, la réglementation agit comme un levier essentiel en établissant un cadre légal et des normes pour la protection des données et la sécurité informatique. Elle incite les organisations à adopter des mesures de sécurité rigoureuses, renforce la responsabilité et la transparence, et favorise une réponse coordonnée aux cybermenaces, contribuant ainsi à un écosystème numérique plus sûr.

Pour les pays de l'Union Européenne, un développement historique est la mise en place de la loi européenne sur la cyber-résilience. Ce règlement impose des exigences strictes en matière de cybersécurité pour les produits numériques, y compris les objets connectés, de la conception à la mise sur le marché. Cette loi pourrait devenir une norme internationale, transformant le paysage de la conception des objets connectés, redéfinissant les modèles commerciaux et révolutionnant les canaux de distribution à travers le continent. Comme le RGPD, cette législation fournit un modèle que d'autres pays peuvent suivre. À long terme, cette loi offrirait aux fabricants européens un avantage concurrentiel sur les marchés mondiaux.

Toutefois, au-delà des considérations économiques, la réglementation des objets connectés, y compris ceux destinés au grand public, représente un pilier fondamental de la souveraineté numérique, devenant un objectif stratégique de la Commission Européenne pour le développement des technologies de l'Internet des objets. Thierry Breton, commissaire européen au marché intérieur, aborde les enjeux liés à la souveraineté numérique de l'Europe, en appelant l'Union européenne à 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 informa-tionnel, 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 indus-trielles qui attisent tous les regards, au premier rang desquels les GAFAMs et autres BATX. Sécuriser les réseaux 5G est un im-pératif : aucune vulnérabilité n'est permise dans ces infrastruc-tures critiques. Nous y travaillons. En outre, nous finalisons une nouvelle stratégie de cybersécurité - un « bouclier cyber euro-péen » - 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 indus-trielles, 5G, cybersécurité, puissance de calcul vont conditionner notre souveraineté pour des décennies ».*

Il devient évident que la souveraineté numérique de l'Union Européenne ne soit plus limitée qu'à la maîtrise des infrastructures informationnelles où à la garantie d'une indépendance vis-à-vis des technologies non européennes. L'enjeu est beaucoup plus important dans la mesure où il faudra veiller à ce que l'internet des objets ne remette pas en cause les libertés fondamentales des européens. A titre d'illustration, le scandale de Cambridge Analytica en 2018, une société britannique de conseil politique et de communication stratégique, qui a utilisé des données personnelles de millions d'utilisateurs de Facebook sans leur consentement pour influencer les opinions politiques, notamment lors des élections présidentielles américaines de 2016 et du référendum sur le Brexit. Ce scandale a mis en lumière la possibilité que ces technologies conditionnent 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. Cette situation est d'autant plus alarmante, étant donné l'expansion progressive et massive de l'intrusion des objets connectés dans la vie privée des citoyens.

Ainsi, nous pouvons déduire qu'à travers cette proposition de loi sur la cyber résilience, l'Union Européenne garantira, notamment, que ces technologies respectent la vie privée des citoyens et leurs droits fondamentaux. Il s'agit d'une spécificité qui distingue, d'ores et déjà, l'Europe des stratégies adoptées par d'autres États.

V.Manœuvres stratégiques autour de l'internet des objets : Chine, Etats-Unis, Israël et Inde

V. MANŒUVRES STRATEGIQUES AUTOUR DE L'INTERNET DES OBJETS : CHINE, ETATS-UNIS, ISRAËL ET INDE

V.1 LES GEANTS DE L'IDO : RIVALITES SINO-AMERICAINES

Dans cette partie, nous allons nous focaliser sur la stratégie des 2 plus gros pourvoyeurs mondiaux d'infrastructures d'IdO, la Chine et les Etats-Unis. Il y a quelques années, cette dernière nation avait pris une avance certaine mais il semblerait que la Chine ait réussi à combler ce retard et se hisser en tant que leader mondial sur ce marché, même si cette position présente encore quelques fragilités.

Nous allons tenter d'apporter un éclairage sur leurs stratégies de développement de l'internet des objets mais également leurs objectifs visés et les risques que cela représente pour la France, l'Europe et le reste du monde.

Nous allons également essayer de nous inspirer des bonnes pratiques de ces 2 grandes nations, notamment sur l'aspect de protection des données personnelles et de cybersécurité de l'internet des objets.

V.1.1 Une stratégie libérale versus une stratégie d'Etat-Parti centralisée

Etats-Unis et Chine partagent une vision commune de l'importance stratégique de l'IdO, mais adoptent des approches différentes en fonction de leurs priorités économiques, sécuritaires et nature du régime politique respectifs.

Le Bureau de la politique scientifique et technologique de la Maison Blanche (OSTP - Office of Science and Technology Policy) avait identifié et réaffirmé en 2022, certains domaines d'application de l'IdO comme étant des technologies critiques pour l'innovation future et la sécurité nationale. [80]

La stratégie de développement de l'IdO des États-Unis d'Amérique est plutôt bien connue et documentée -centrée sur l'innovation, la compétitivité et la collaboration public-privé, avec une forte priorité sur la cybersécurité-. Nous allons naviguer dans les méandres des deux stratégies et mettre un peu plus en lumière celle de la Chine.

« *La crise financière mondiale accélère la naissance d'une nouvelle révolution technologique et industrielle. Il est d'une importance décisive pour l'avenir de notre pays que nous développions des industries émergentes d'importance stratégique et que nous capturions le terrain économique, scientifique et technologique élevé ; par conséquent, nous devons saisir les opportunités, identifier les priorités et obtenir des résultats.... Nous allons... accélérer la R&D et l'application de l'Internet des Objets.* », a déclaré le premier ministre Wen en 2010 pour souligner les enjeux de l'IdO.

Depuis que la Chine a pris conscience de la puissance de la technologie en tant qu'outil d'influence, le progrès technologique est devenu un baromètre essentiel de puissance et de sécurité nationales pour ses dirigeants. Éviter de prendre du retard par rapport aux autres puissances internationales est ainsi devenu une obsession permanente.

Avant même que la Chine n'ait lancé son plan stratégique pour le développement de l'IdO, les Etats-Unis, l'union européenne et le Japon avaient déjà le leur, qui avaient consacré l'IdO comme une priorité, et étaient plus ou moins avancés. Il devenait donc urgent pour la Chine d'enrayer ce retard et d'empêcher d'autres pays d'établir ou de creuser leur avance en matière de capacités IdO. *« Toute dépendance à l'égard de la technologie étrangère constitue un risque majeur pour la sécurité nationale chinoise ».*[81]

C'est dans ce contexte que la Chine a commencé à inscrire les initiatives pour le développement de l'IdO dans son 12ème plan quinquennal (2011-2015) et a continué dans ses plans quinquennaux successifs, montrant une progression continue et une expansion des objectifs et des investissements dans ce domaine crucial.

[80] Technologies for American Innovation and National Security | OSTP | The White House
[81] SOSi_China's Internet of Things.pdf, page 16

Pour rappel, les plans quinquennaux chinois sont des feuilles de route économiques et sociales élaborées par le parti communiste chinois (PCC) et le gouvernement chinois pour définir les priorités nationales et les orientations de développement du pays sur une période de cinq ans. Ils ont été introduits en 1953, inspirés par les plans quinquennaux soviétiques. A ce jour, la Chine a adopté un total de quatorze plans quinquennaux, chacun définissant des objectifs spécifiques pour la période suivante.

Voici un aperçu des principaux plans quinquennaux liés à l'IdO en Chine :

1. **12ème Plan quinquennal (2011-2015)** : Introduction de l'IdO en tant que projet scientifique majeur, mise en place des bases pour son développement technologique avec des investissements massifs dans l'infrastructure et les recherches en architecture alternative pour l'internet futur.[82]
2. **13ème Plan quinquennal (2016-2020)** : Confirmation de l'IdO comme élément central de la stratégie numérique de la Chine, avec des initiatives visant à renforcer le développement technologique et les capacités de cybersécurité. Inclusion d'objectifs spécifiques pour l'augmentation des parts de marché dans certains domaines tels que les robots de fabrication autonomes, des véhicules partiellement autonomes, et des équipements de fabrication intelligente.[83]
3. **14ème Plan quinquennal (2021-2025)** : Introduction d'objectifs ambitieux pour l'économie numérique, y compris l'IdO. Concentration sur l'amélioration de l'infrastructure numérique, la transformation numérique des industries, et le développement des services publics numériques. Objectifs d'intégration de l'IdO dans divers secteurs tels que la fabrication industrielle, l'agriculture, les services publics et la gestion des urgences (UNEP LEAP).[84]

Le plan stratégique chinois s'appuie sur plusieurs piliers dont les suivants :

- Soutien du gouvernement ❾ Investissements massifs et incitations financières
- Partenariats et collaborations internationales (accords de partage de technologie, initiatives R&D conjointes, …). Voir en annexe, une sélection de partenariats sinoeuropéens dans le domaine de l'IdO[85]
- Investissements dans des entreprises technologiques étrangères (acquisition et transfert de technologie facilités, pénétration de nouveaux marchés)
- Innovation technologique ❾ 5G (Leader mondial, connectivité massive, débits élevés et faible latence), IA (intégrée aux solutions IdO, amélioration de la capacité de

[82] The Connection of Everything: China and the Internet of Things | Merics

[83] Analyzing China's 2021–2025 Informatization Plan: A DigiChina Forum (stanford.edu)

[84] Translation: 14th Five-Year Plan for National Informatization – Dec. 2021 (stanford.edu)

[85] MericsChinaMonitor70InternetOfThings2.pdf, page 6

traitement et la prise de décision), Big data et cloud computing (pour gérer les vastes quantités de données générées par l'IdO et rendre leur traitement efficace et optimisé)

- Stratégie de standardisation et influence dans les organismes internationaux, jugée intéressante à développer davantage. La Chine ne veut plus refaire la même erreur et a tiré les leçons de la dernière révolution industrielle durant laquelle les Etats-Unis, l'Europe, le Japon et la Corée du sud ont pu assoir leur domination en grande partie grâce au contrôle des normes internationales.

« *Les normes sont les rênes du pouvoir, le discours du pouvoir et le pouvoir de contrôler. Par conséquent, 'celui qui prend la main sur les normes a le monde dans sa paume'* »[86], cette déclaration datant de 2015 est du président chinois Xi Jinping.
Pour paraphraser Zhang Xiaogang, l'ancien directeur de l'Organisation internationale de normalisation (ISO) et de l'Association chinoise du fer et de l'acier (CISA), « *Celui qui contrôlera la norme, contrôlera la technologie et le marché.* »

Cette stratégie n'est pas nouvelle et depuis 20 ans, les plus hautes instances du pouvoir chinois martèlent leur discours sur la nécessité d'exporter les normes techniques chinoises à l'international en s'appuyant sur la toute puissante administration chinoise de normalisation (SAC – Standardization Administration of China). Elles vont jusqu'à mettre en place un système d'incitation financière pour les entreprises qui proposent des normes internationales et un soutien financier pour les aider à intégrer les organisations de normalisations.[87]

C'est donc dans cette logique que la Chine développe ses propres normes nationales pour l'IdO et cherche à les promouvoir à l'échelle internationale visant ainsi à gagner en influence stratégique et à assoir sa domination sur le marché.

En l'occurrence, le caractère centralisé du pouvoir chinois facilite l'élaboration de normes complexes comme celles des villes intelligentes nécessitant le concours et la coordination d'une multitude d'acteurs. Les normes de cet ordre arrivent déjà testées et éprouvées au sein des organismes de normalisation internationaux et sont systématiquement adoptées. Comme l'illustre la figure ci-dessous, la Chine multiplie les accords bilatéraux (plutôt asymétriques) pour la normalisation -Son premier en 2002, 98 avec 55 pays revendiqués en 2022-.

[86] Guo Zhanheng, « 习近平标准化思想与浙江实践 » [Réflexions de Xi Jinping sur la normalisation et la mise en pratique dans le Zhejiang], Zhejiang Daily, 25 septembre 2015.

[87] Il faut, la plupart du temps, payer des cotisations annuelles pour intégrer des organisations d'établissement des normes. Pour l'UIT, elles peuvent aller d'un peu plus de 4 000 $ pour les centres universitaires à près de 35 000 $ pour les entreprises.

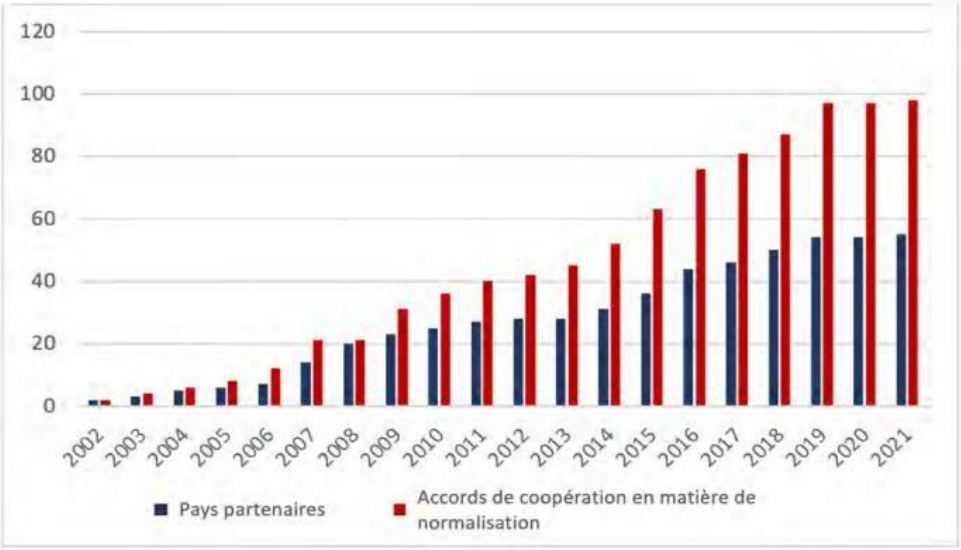


Figure 25 : Nombre de partenaires et d'accords de coopération de la Chine (2002-21)
Source : sr97_chinas_digital_ambitions_mar2022_french.pdf

Sans entrer dans les détails, cette stratégie semble porter ses fruits, les experts chinois sont extrêmement actifs dans tous les organismes de normalisation internationaux, participant aux ébauches et révisions des normes des organismes les plus reconnus (ISO, IEC, UIT)[88], renforçant leur gouvernance en leur sein et convoitant des postes de direction de leur comités techniques et groupes de travail.

Pour ne citer qu'un exemple, la prédominance de la Chine dans les UIT se vérifie par ailleurs dans ce cas précis de la réunion d'octobre 2021 du groupe 20 de l'UIT-T, qui se consacre à l'IdO et aux villes intelligentes. Un total de 94 normes y a été proposé, dont 53 par des acteurs chinois. Leurs homologues sud-coréens suivent, avec 21 contributions. [89]

V.1.2 La donnée, matière première du capitalisme et du communisme de

[88] International Organization for Standardization (ISO), Union Internationale des télécommunications (UIT), International Electrotechnical Commission (IEC)

[89] sr97_chinas_digital_ambitions_mar2022_french.pdf, page 115

surveillance de masse

La Chine a adopté une approche stratégique hybride (Top-Down et Bottom-Up) pour assoir son influence dans le domaine de l'IdO.

D'une part, elle développe une infrastructure numérique d'envergure à l'échelle internationale pour établir la base de sa conquête industrielle, du bas vers le haut. Cette infrastructure comprend des systèmes physiques tels que les capteurs et puces intelligents, les centres de données mais également tout l'écosystème autour de l'IdO et qui contribue à le rendre exploitable, efficace et efficient. C'est ainsi que la Chine a donné une haute priorité, au même titre qu'à l'IdO, à des technologies telles que l'IA, la 5G, le Big Data et le Cloud Computing car toutes interconnectées et se complétant mutuellement. En effet, l'IdO génère de vastes quantités de données qui sont analysées par l'IA et le Big Data, tandis que le cloud computing offre l'infrastructure nécessaire pour stocker et traiter ces informations massives de manière efficace et évolutive.

D'autre part et dans le même temps, comme déjà évoqué précédemment, elle met tout en œuvre pour établir les règles de l'environnement numérique et notamment celui de l'IdO, du haut vers le bas en fixant et en influençant les normes techniques internationales afin de conserver son avantage en matière d'infrastructure et de marché. [90]

La chine ne cherche pas uniquement à tirer un profit économique de sa suprématie technologique mais surtout à accroitre sa puissance et son influence dans le monde. Mais ce qui l'intéresse le plus est la captation des données et en particulier les données personnelles des citoyens du monde mais également de ses propres citoyens sans que l'objectif visé ne soit tout à fait le même.

C'est un élément central qui nous est révélé par le 14ème plan quinquennal (2021-2025) qui consacre et qui met l'accent sur les données, *qui sont désormais désignées comme un facteur de production majeur, aux côtés de la terre, du capital et du travail*.[91] Faut-il rappeler que le parti communiste chinois (PCC) reste marxiste ?

Certains diront que la donnée est l'Or des temps modernes. Mais la donnée à elle-même ne suffit pas selon M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique. *La donnée est un instrument de création de valeur qui peut être multiple et qui n'est pas liée uniquement à son contenu mais également à la manière dont elle est structurée de manière à pouvoir être réutilisée dans beaucoup d'autres secteurs*, nous confiait-il lors de son interview.

[90] sr97_chinas_digital_ambitions_mar2022_french.pdf, pages 10 et 11

[91] https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national- informatization-dec-2021/

Cette matière première est exploitée par les autorités chinoises à des fins multiples selon son origine (domestique ou internationale) et l'objectif visé.

La Chine a une approche différente de la protection des données personnelles par rapport à l'Occident – Hors Etats-Unis qu'on évoquera plus loin dans ce chapitre-. Son Etat-parti considère les données comme une ressource stratégique importante comme nous avons eu l'occasion de l'évoquer auparavant et il y a une volonté d'accumuler de grandes quantités de données pour alimenter son intelligence artificielle, son Big-data et améliorer son système de surveillance, influencer et manipuler l'opinion publique et évidemment en tirer un avantage économique et technologique.

Par ailleurs, selon Yang Wang, chercheur à l'université de Syracuse, *la culture chinoise a moins de considération pour la vie privée que la culture occidentale et que la plupart des Chinois se sont habitués à la certitude de la surveillance étatique…Le mot le plus courant pour exprimer le concept de vie privée, **yinsi**, n'est apparu dans le dictionnaire chinois qu'au milieu des années 1990*.[92] Rien de très étonnant pour une société d'essence communiste où le groupe prime sur l'individu, dirions-nous.

La Chine n'a adopté ses premières lois sur la protection des données personnelles qu'en 2021, avec la Loi sur la sécurité des données (Data Security Law, DSL) et la Loi sur la protection des renseignements personnels (Personal Information Protection Law, PIPL). Ces lois visent à restreindre l'accès aux données personnelles, à l'exception des autorités gouvernementales. Les articles 4 et 5 de la DSL imposent que la sécurité des données soit alignée sur la 'vision globale de la sécurité nationale' du Parti-État, avec un mécanisme centralisé pour la prise de décision et la coordination des politiques.

De plus, la DSL précise que les entreprises chinoises sont soumises aux lois chinoises, même en dehors de la Chine, si leurs activités de traitement des données peuvent affecter la sécurité nationale, l'intérêt public ou les droits des citoyens chinois.

Ensuite, la PIPL réglemente les entités qui traitent des données personnelles, mais ne restreint pas les organes de l'État, qui peuvent accéder aux données sans informer les individus concernés. Par exemple, l'article 18 de la PIPL permet aux gestionnaires de données de ne pas informer les personnes si l'accès reste confidentiel ou n'a pas besoin d'être annoncé.

En somme, ces lois montrent clairement qu'aucune législation ne restreint l'État chinois dans l'utilisation des données collectées par les entreprises, que ce soit au niveau national ou international. Par conséquent, toutes les données de nos objets connectés grand public acquis auprès d'entreprises chinoises peuvent être transférées sur des serveurs en Chine et mises à la disposition des autorités chinoises à leur convenance.

[92] L'âge du capitalisme de surveillance, Shoshana ZUBOFF, page 525

La Chine ne fait pas preuve de la même rigueur concernant la sécurité des objets connectés qu'elle exporte à travers le monde que pour ceux qu'elle commercialise sur son marché domestique. En effet, pour ces derniers, elle impose des lois et des régulations contraignantes - la Loi sur la cybersécurité (2017) et la Loi sur la protection des données personnelles (2021) - aux entreprises opérant en Chine pour protéger les données et sécuriser les objets connectés. Les données doivent être localisées sur des serveurs en Chine, et les dispositifs d'IdO doivent obtenir des certifications de sécurité et être soumis à des audits réguliers pour garantir leur conformité aux normes de sécurité nationale.

Certes, il est de la responsabilité des pays importateurs de mettre en place les mécanismes de contrôle et les exigences de sécurité requises pour autoriser les objets connectés grand public sur leur territoire, même si, avec le libre marché, il est compliqué de tout contrôler. Si la Chine se souciait de la qualité des produits et de la sécurité numérique de ses clients étrangers, elle produirait et livrerait des objets connectés selon les mêmes standards et exigences que ceux de son marché intérieur. Ce scénario relèverait de l'utopie !

La réalité est que le laxisme des autres et la permissivité du libre marché arrangent les affaires de la Chine. Pourquoi investirait-elle dans la sécurisation des objets connectés grand public alors que cela représente un coût important ? Son intérêt est plutôt de promouvoir des dispositifs d'IdO grand public à bas prix afin d'inonder les marchés occidentaux, notamment, y intégrer des fonctionnalités de collecte de données pour les rapatrier sur des serveurs localisés en Chine, et, le cas échéant, exploiter les failles de sécurité inhérentes à ces objets dénués de sécurité.

On pourrait citer une multitude d'exemples de ce type d'objets connectés fabriqués en Chine, peu ou pas du tout sécurisés, comme ceux exposés ci-dessous.

En 2018, les montres connectées pour enfants représentaient près de la moitié du marché mondial des montres connectées. Bien que les statistiques récentes soient difficiles d'accès, c'est dans ce contexte que l'affaire des montres connectées pour enfants a éclaté en Allemagne.

Elle a mis en lumière les risques des appareils IdO destinés aux enfants. C'est ainsi que la Bundesnetzagentur (Agence fédérale allemande des réseaux) a interdit la vente de certaines montres connectées pour enfants. Elles sont principalement fabriquées en Chine et étaient équipées de cartes SIM et d'une fonction d'écoute à distance.

Les autorités allemandes compétentes ont dévoilé que ces dispositifs d'IdO pouvaient être piratés pour écouter les conversations des enfants et suivre leurs déplacements sans le

consentement des parents. La Bundesnetzagentur a qualifié ces montres de « dispositifs d'espionnage interdits » et a conseillé aux parents de les détruire. [93]

La CNIL a réalisé une très bonne vidéo ainsi qu'un article de sensibilisation à l'usage des montres connectées pour enfants et les enjeux sur leur vie privée. [94],[95]

En 2019, Monsieur Cuisine Connect de Lidl de la marque SilverCrest, un robot-cuiseur connecté à internet par Wi-Fi, conçu en Allemagne, produit en Chine et vendu en Allemagne, en Belgique, en Suisse, au Royaume-Unis et en France. Il était équipé d'un micro secret non activé mais fonctionnel et il tournait sous Android 6.0 obsolète avec 26 patchs de sécurité de retard par rapport à la version de l'époque.[96]

En 2020, des chercheurs en sécurité de CheckPoint ont révélé une faille de sécurité sur certains modèles d'aspirateurs-robots Xiaomi. Ces derniers, équipés de caméras pour la navigation, collectaient des données détaillées sur l'agencement des habitations et même des plans précis des pièces. Toutes ces données étaient envoyées et stockées sur des serveurs en Chine sans le consentement des clients. Il a également été découvert qu'il était possible d'accéder en direct aux flux vidéo des caméras de ces appareils, avec tous les risques que cela représente en termes d'espionnage et d'atteinte à la vie privée.

La source de cette information renvoie à une publication de CheckPoint Research que nous n'avons pas pu consulter. En cherchant à la vérifier, nous avons trouvé la thèse d'un chercheur allemand de l'Université de Darmstadt consacrée à l'analyse de sécurité de l'écosystème IoT de Xiaomi. Les conclusions de cette thèse sont plutôt flatteuses pour ce constructeur, qui semble avoir des produits mieux sécurisés que ceux de la concurrence.[97] En revanche, il a été corroboré que l'appareil collecte et télécharge sur le cloud Xiaomi un grand nombre de données par jour. Outre les éléments justifiés, ces données comprennent les noms et les mots de passe des réseaux Wi-Fi auxquels l'appareil se connecte, ainsi que les cartes détaillées des pièces. Fait surprenant, ces données restent dans le système même après une réinitialisation d'usine. Ainsi, quelqu'un qui achèterait un modèle d'occasion et le « rooterait » pourrait facilement obtenir toutes ces informations.[98]

Par ailleurs, des chercheurs de Singapour et du Maryland ont démontré qu'il était possible d'écouter une conversation via un aspirateur-robot non équipé de micro ni de caméra. Ils

[93] https://www.zdnet.fr/actualites/montres-connectees-les-parents-les-boudent-les-enfants-vont-les-adorer-39870312.htm
[94] https://video.cnil.fr/w/iZaAZAxGHUApbJLCSV97pN

[95] https://www.cnil.fr/fr/montres-connectees-pour-enfants-quels-enjeux-pour-leur-vie-privee

[96] Monsieur Cuisine Connect : micro caché, Android non sécurisé... les dessous du robot cuiseur de Lidl - Numerama

[97] Security analysis of the XIAOMI IoT ecosystem, Dennis Giese, Master Thesis, 10 juillet 2019, Technische Universität Darmstadt

[98] https://www.kaspersky.com/blog/xiaomi-mi-robot-hacked/20632/

ont exploité les propriétés du Lidar (Laser) utilisé pour la navigation de cet appareil afin de retranscrire une conversation ou l'ambiance sonore d'une pièce. Cette technique, complexe et sophistiquée, n'est pas à la portée des néophytes et une méthode d'écoute bien connue par certains services de renseignement.[99]

Déjà évoqué sur la partie réglementation de ce mémoire, fin 2016, le fameux malware Mirai botnet a été utilisé pour orchestrer plusieurs attaques massives par DDOS (Déni de service distribué) en exploitant des vulnérabilités sur des appareils IdO. C'est ainsi que le fabricant

d'appareils IdO Hangzhou Xiongmai Technology Co. Ltd a été forcé de rappeler plus de 10 000 webcams après qu'elles aient été victimes d'une attaque. Les investigations ont montré que ces équipements auraient été mis sur le marché sans aucun dispositif de sécurité de base.

En 2017, c'est plus de 175 000 caméras connectées, produites par Shenzhen Neo Electronics et installées dans plusieurs pays, qui étaient accessibles à distance en raison de failles de sécurité dans l'accès à ces appareils.

Enfin, tous ces exemples illustrent la défaillance manifeste des dispositifs IdO, censés rendre nos foyers intelligents, mais au prix d'une captation massive de nos données personnelles et d'une atteinte caractérisée à notre vie privée.

La Chine s'est donné les moyens de conquérir le monde des IdO en déployant les ressources d'un État-parti à travers une stratégie agressive d'investissements massifs, une politique d'innovation dans les technologies avancées, un lobbying pour imposer ses normes au sein des organismes internationaux de normalisation, et une approche commerciale défiant toute concurrence pour inonder le marché mondial avec ses infrastructures IdO. Tout cela vise à contrôler ce qui est devenu un facteur de production majeur : les données. Nos données personnelles, que les autorités chinoises prétendent protéger, mais qu'elles utilisent à leur convenance pour nous espionner, nous inonder de publicités ciblées, nous influencer et modeler nos comportements au sens large. Bienvenue dans le communisme de surveillance !

Mais ce n'est que le reflet du capitalisme de surveillance[100] et le fruit d'une lutte acharnée où l'élève tente de surpasser son maître.

En effet, les Etats-Unis sont pionniers dans le domaine….

Depuis que Google a fait basculer le capitalisme de marché dans une nouvelle dimension, celle du capitalisme de surveillance, ce ne sont pas nos données en tant que telles qui les intéressent, mais plutôt ce qu'elles révèlent de nos comportements. L'objectif de cette captation massive de données n'est plus l'amélioration des produits et services au profit du consommateur, mais plutôt l'influence du comportement de ce dernier au profit des

[99] https://www.journaldugeek.com/2020/11/24/attention-robot-aspirateur-espionner/

[100] Shoshana ZUBOFF définit le capitalisme de surveillance comme une nouvelle forme de marché qui revendique l'expérience humaine privée comme matière première dont elle se sert dans des opérations secrètes d'extraction, de production et de vente.

annonceurs. Ce modèle économique rapporte des centaines de milliards de dollars à des entreprises comme Google, Meta et Microsoft.

Avant d'aller plus loin, rappelons le contexte et les conditions d'apparition de ce capitalisme de surveillance. C'était celui d'une « guerre contre la terreur », en 2001 à la suite des attentats visant les tours jumelles du World Trade Center. Ce « singularisme de la surveillance » a permis à des entreprises technologiques, de développer leurs capacités de captation de données et de surveillance sans aucune entrave et avec la bénédiction des

autorités américaines, gouvernement et agences de renseignement, sous prétexte de sécurité nationale et de protection du monde libre.[101]

Les déclarations des plus hauts responsables américains de l'époque sont révélatrices de cet état d'esprit. Le Général Michael Hayden qui a dirigé la National Security Agency (NSA) et la Central Intelligence Agency (CIA) raconte dans un entretien de 2014 avoir été auditionné, un an après l'attaque du 11/09, par une commission d'enquête mixte – commission de renseignement de la chambre des représentants et du sénat - pour examiner les causes de l'attaque du 11/09 et le sous-texte était : « how did you guys let this happen ? »[102]
Il en est ressorti qu'il fallait, que les agences de renseignement américaines, « *élargissent leur ouverture, élargissent leur art opérationnel pour qu'elles soient plus capables de capter ce type de communication* ». Comprendra qui pourra et qui voudra mais c'est ainsi qu'est né le programme de surveillance, Stellar Wind, plus communément connu programme 215. Il s'appuie sur des mastodontes technologiques tels que Google (« *qui fournit des masses de choses* »), Facebook (la plus importante production mondiale de photographie numérique), YouTube (le seul au monde qui atteigne et dépasse l'exaoctet – 1Md Go -), Twitter (des milliers de tweets/sec) et les opérateurs de télécommunication (sms et voix).[103] C'est ainsi qu'en 2013, le directeur du renseignement de la CIA pouvait se targuer dans une déclaration : « *Nous sommes quasiment en mesure d'informatiser toutes les informations générées par les êtres humains* » et d'ajouter que la mission technologique de la CIA était de « *profiter…des flots massifs d'informations apparus sur la planète* »

Et toutes les sources de collecte de données sont bonnes à prendre. Et quelle aubaine et belle opportunité que l'IdO pour la NSA et pas uniquement d'ailleurs. Lors de la conférence Defense One Tech Summit, organisée à Washington D.C. en 2016, Richard Ledgett, le directeur adjoint de la NSA de l'époque, avait expliqué que ses services se préparaient à étendre la collecte de données à l'Internet des objets. Les dispositifs médicaux, tels que les stimulateurs cardiaques, sont également concernés. Il estimait qu'ils pourraient constituer

[101] Shoshana ZUBOFF y dénonce la collusion entre le gouvernement américain et les entreprises technologiques, qui protège le pouvoir privé de ces dernières, mettant en danger les démocraties libérales et les droits démocratiques de tous les citoyens.

[102] Comment avez-vous laissé cela se produire ?

[103] https://www.gsb.stanford.edu/insights/former-nsa-head-michael-hayden-agency-cannot-survive-without-being-more-transparent

une nouvelle source d'informations sensibles, « *un outil dans la boîte à outils* » du renseignement, avait-t-il ajouté.[104]

Un point important à prendre en compte est le fait que les États-Unis n'ont pas de loi fédérale unique et globale régissant la collecte et l'utilisation des données personnelles. Au lieu de cela, le régime de protection des données existant aux États-Unis est composé d'un ensemble disparate de lois fédérales et étatiques, de principes, de règles, de règlements et de lignes directrices qui traitent de divers aspects de la protection des données. Ces dispositions se chevauchent, se complètent et se contredisent occasionnellement avec différents degrés d'application. Par exemple, les lignes directrices élaborées par les agences gouvernementales et les groupes industriels n'ont pas force de loi, mais sont considérées comme des "best practices" de plus en plus utilisées comme base d'application.

Plusieurs lois fédérales réglementent différents aspects de la confidentialité des données et des informations personnelles sensibles aux États-Unis, y compris la protection des consommateurs, les informations financières et médicales, le crédit à la consommation, les adresses électroniques et les numéros de téléphone, ainsi que l'interception des communications électroniques et le sabotage informatique.

Certains États ont également promulgué des lois pour fournir une protection supplémentaire des données aux États-Unis, principalement conçues pour traiter, dissuader et punir l'accès non autorisé et les violations de la sécurité. La Californie, par exemple, est particulièrement prolifique et en avance sur le reste du pays dans l'adoption de lois sur la confidentialité des données. Elle a été le premier État à adopter une loi de notification des violations de la sécurité, établissant un précédent que d'autres États et territoires ont suivi. Elle a également une loi interdisant aux téléviseurs intelligents avec capacités de reconnaissance vocale d'utiliser les mots et les conversations enregistrés à des fins publicitaires, ce qui en fait l'un des rares États à traiter spécifiquement de la confidentialité des données à l'ère de l'Internet des objets (IdO). En mars 2018, les 50 États ainsi que le District de Columbia, Porto Rico et les Îles Vierges américaines avaient adopté une législation exigeant que les personnes et les entreprises ayant un accès autorisé aux données notifient les consommateurs concernés en cas de violation de la sécurité impliquant des informations personnelles.[105]

Pourtant tout avait bien commencé avec le projet d'Aware Home lancé en 2000 par une équipe d'informaticiens et d'ingénieurs de Georgia Tech. Ils imaginèrent un IdO en symbiose entre humains et maison, respectueux des données personnelles de l'individu et qui contribue à l'amélioration de la vie du consommateur et à son service. Ce dernier reste maitre de la restitution de son expérience en données et libre arbitre de l'usage et de la destination de ses propres données. Le consommateur est la fin en soi et non pas le moyen de la fin des annonceurs.[106]

---

[104] https://www.silicon.fr/nsa-exploiter-internet-objets-sante-150066.html

[105] Traduction China's Internet of Things / John Chen, Emily Walz, Brian Lafferty, Joe McReynolds, Kieran Green, Jonathan Ray, and James Mulvenon / Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, October 2018, Pages 145 et 146

[106] Guido Noto La Diega et Ian Walden, « Contracting for the «'Internet of Things' :Looking into the Nest » (research paper, Queen Mary University of London, School of Law, 2016)

M. Bernard Benhamou, secrétaire général de l'Institut de souveraineté numérique, nous en avait déjà parlé lors de notre entretien. Il avait cité l'exemple d'un détecteur de fumée intelligent capable, à partir des données collectées, de contribuer à l'établissement de profils médicaux précis. Cet appareil était également muni d'un détecteur de présence (à première vue, sans lien avec l'objet du dispositif) qui est en mesure de capter les mouvements des occupants de la maison. Si ces mouvements se produisent à des heures inhabituelles de la nuit, ces informations recueillies sur une longue période pourraient révéler des problèmes de santé, par exemple. De plus, si ce détecteur de fumée pouvait se connecter à d'autres objets connectés tels qu'un dispositif de fitness ou de sport qui mesure une panoplie de paramètres de santé, on obtiendrait un agrégat de données susceptible d'affiner un profil médical. Cela montre la puissance des données comportementales, même issues d'un objet connecté anodin, dans l'élaboration de profils très précis.

Il nous a également rapporté l'anecdote d'un journaliste d'un grand quotidien américain qui enquêtait sur les courtiers en données et avait demandé à l'un d'eux l'autorisation d'accéder à son propre profil. Ce qu'il avait découvert l'avait stupéfait, car il était indiqué comme étant prédisposé aux pathologies rénales, prédisposition que son médecin lui avait confirmée par la suite.
« L'âge du capitalisme de surveillance » de la sociologue et chercheuse Shoshana Zuboff, confirme cette sophistication de la collecte massive des données personnelles et décortique tout le mécanisme complexe et opaque qui la sous-tend.

Brosses à dent connectées, ampoules connectées, prises connectées, balances connectées, fours connectés, frigos connectés, téléviseurs intelligents, enceintes connectées, assistants personnels connectés, caméras domestiques connectées, etc. Elle nous y raconte comment on est passé de l'Aware Home imaginé pour servir ses occupants à une maison truffée d'espions connectés au service du capitalisme de surveillance.

Elle y explique tout un rouage savant de collecte et de transformation de nos données personnelles dans le but de notre asservissement comportemental.
On va illustrer brièvement ce mécanisme au travers d'un exemple parmi d'autres qu'elle a développés dans son ouvrage.

Le thermostat connecté Nest créé par la maison-mère de Google, Alphabet, accomplit de nombreuses tâches imaginées dans l'aware home. Il collecte les données de son propre usage et de son environnement, il traque les mouvements des habitants de la maison et ses applications peuvent se connecter et collecter des données d'autres objets connectés tels que la voiture, le four, le frigo, les équipements de fitness et les lits intelligents. À la suite de sa fusion avec Google, il y a intégré l'IA de Google et les fonctionnalités de son assistant personnel intelligent. Toute cette masse de données est téléchargée et stockée sur les serveurs de Google.

Chaque thermostat Nest est accompagné des « conditions générales d'utilisation », d'une « politique de confidentialité » et d'un « contrat de licence de l'utilisateur final » où il y est

indiqué le peu de considération que porte Google au respect des données personnelles et à la vie privée ainsi qu'à leur confidentialité. Ces données peuvent être partagées avec des tierces parties et d'autres objets intelligents à des fins d'analyses prédictives et de vente à d'autres parties non spécifiées.[107]

Deux chercheurs en droit de l'université de Londres ont analysé en détail les conditions d'utilisation de Nest et ont mis en évidence un écosystème d'une multitude d'applications et d'objets connectés, chacun disposant de conditions d'utilisation tout aussi complexes. De telle sorte que le simple achat d'un thermostat connecté nous mènerait à analyser un millier de contrats, selon le résultat de leurs recherches.[108]

Mais comme on le sait tous, personne ne lit jamais ces contrats rédigés sciemment en petite police de caractère. Une étude empirique portant sur 543 participants s'intéressant aux questions relatives à la protection des données est tout à fait édifiante. La durée moyenne de consultation des documents accompagnant la vente d'un nouveau service en ligne était de 14 secondes alors qu'il aurait fallu au moins 45 minutes pour bien cerner le contrat.[109]

Évidemment, les conditions d'utilisation stipulent qu'en cas de refus de leur adoption par le client, les fonctionnalités de l'équipement seraient fortement dégradées et sa sécurité gravement compromise en l'absence de mise à jour.

Voilà comment Google, Amazon, Meta et Microsoft[110,111] instrumentalisent l'efficacité et la sécurité des produits afin de soumettre les clients à leur stratégie éhontée d'extraction et de captation massive de leurs données personnelles.

Que ce soient les aspirateurs-robots Roomba de l'entreprise iRobot qui génèrent des plans de maison détaillés et précis dans le but de les revendre ou bien le matelas intelligent du lit sleep number, le principe est toujours le même : sans le consentement explicite du client à l'utilisation de ses données personnelles et à l'intrusion dans sa vie privée, l'efficacité et la sécurité des produits seraient considérablement compromises.

[107] L'âge du capitalisme de surveillance, Shoshana ZUBOFF, page 24

[108] Guido Noto La Diega et Ian Walden, « Contracting for the «'Internet of Things' :Looking into the Nest » (research paper, Queen Mary University of London, School of Law, 2016)

[109] Jonathan A. Obar et Anne Oeldorf-Hirsch, « The biggest Lie on the internet : Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services », in Facebook/Social Media 2 (TPRC 44 : The 44th research conference on Communication, Information and Internet Poilicy, Arlington, VA : Social REsearch Network, 2016)

[110] En Pages 27 et 43 de son ouvrage 'L'âge du capitalisme de surveillance', Shoshana Zuboff semble accorder encore de la crédibilité à Apple concernant le traitement des données personnelles de ses clients. Elle conclut comme suit : « *Apple s'est jusqu'ici fixé une ligne de conduite, en promettant de s'abstenir de nombreuses pratiques que je range dans le régime capitaliste de surveillance. Son comportement à cet égard n'est pas parfait, sa ligne est parfois floue, et il se pourrait qu'Apple change d'orientation et se contredise.* »

[111] Il semblerait qu'Apple mettrait en avant une politique stricte de protection de la vie privée, *en soulignant que la collecte de données personnelles se fait avec le consentement explicite des utilisateurs*. Ils ont, par ailleurs, introduit des fonctionnalités comme le "Privacy Nutrition Label" et des options pour limiter le suivi publicitaire (Apple permet aux utilisateurs de désactiver le suivi publicitaire via une option dans les paramètres).

D'une part, ces fabricants insistent sur le choix libre et éclairé du client au partage de ses données. D'autre part, les clients qui ne consentent pas à le faire s'exposent à voir le produit, qu'ils ont par ailleurs payé, réduit à une coquille vide.

Plus grave encore, iRobot offre la possibilité à ses clients de suspendre la collecte des données en modifiant le mot de passe wifi par exemple mais il continue à enregistrer les données de cartographie et d'utilisation qui sont envoyées sur le cloud. Ceci afin de pouvoir être affichées sur un smartphone ou tout autre terminal, selon les dires de son PDG.[112]

Comme déjà évoqué auparavant, ce capitalisme de surveillance sert ses propres intérêts mais également les intérêts du gouvernement américain qui a contribué à sa naissance et à son épanouissement.

Dans un contexte américain de politiques de protection des données personnelles disparates et permissives, les entreprises technologiques de l'IdO et à leur tête Google, Meta et Microsoft pillent l'expérience privée de leurs clients, la soumettent au processus de « datafication » et engrangent des milliards de dollars en la monnayant auprès des instigateurs du marketing comportemental.

Les océans de données amassées dans cette obscure entreprise font l'affaire des agences de renseignements américains qui, invoquant le prétexte de la sécurité nationale, continuent à protéger, perpétuer et à faire prospérer un système de violation manifeste de la vie privée des citoyens du monde entier.

V.1.3 Un cas d'école : Le crédit social chinois, mythe ou réalité

Avant de conclure sur cette partie, nous ne pouvons pas ne pas revenir en Chine afin d'évoquer ce qui pourrait être de pire dans la captation et le détournement de nos données personnelles.

À l'ère du « totalitarisme numérique », nous avons voulu nous intéresser au système de crédit social (SCS) chinois, qui nous semblait être un cas d'école de captation massive des données personnelles des habitants en Chine (citoyens chinois et étrangers) ainsi que des entreprises, afin d'évaluer leur niveau de vertu, selon le discours officiel. Après 43 SCS pilotes, il devait être généralisé à tout le territoire chinois en 2020, mais sans standard national, il a été reporté à 2022 avec la publication d'un décret national clarifiant plus ou moins les contours du dispositif. Il s'appuierait sur un réseau de plusieurs centaines de millions de caméras intelligentes à reconnaissance faciale – on parlait de 600 millions de caméras en 2020 -, [113] et la coopération de plusieurs grandes entreprises dont les BATX : Baidu (Google chinois), Alibaba (Amazon chinois), Tencent (Meta chinois) et Xiaomi (Apple chinois).

[112] L'âge du capitalisme de surveillance, Shoshana ZUBOFF, page 318
[113] https://www.rts.ch/info/monde/11137943-la-chine-veut-noter-tous-ses-habitants-et-installe-600-millions-de-cameras.html

Quelle est la part du fantasme occidental de la réalité sur le terrain ? Selon la chercheuse Shazeda Ahmed, de l'université de Stanford et de Berkeley, Il y a beaucoup de désinformation et de mythes à ce sujet.[114]

Selon elle, il n'existe pas de système de notation mais plutôt un système de listes noires et il en existe des dizaines, pas une seule. Les punitions, parmi tant d'autres, peuvent consister à empêcher de mettre ses enfants dans une école privée, ou bien de prendre des transports tels que le train à grande vitesse ou l'avion, car en vertu de la loi chinoise, ces services sont considérés comme des formes de « consommation de luxe ». En 2018, près de 17 millions de Chinois n'ont pas eu le droit de prendre l'avion et 5 millions le train à grande vitesse[115]. Cela met la pression sur les contrevenants à la loi pour qu'ils changent leur comportement afin de sortir des listes noires.

D'après cette chercheuse, les seules interactions connues entre les administrations étatiques et les entreprises technologiques concernent l'assurance de l'application des sanctions dans l'économie non étatique. En même temps, elle alerte sur la possibilité d'un système de crédit social beaucoup plus étendu qu'offre la mine d'informations sur les citoyens chinois dont disposent les entreprises technologiques que l'État pourrait réclamer quand et comme il voudrait, sans qu'il soit possible de leur refuser l'accès. Par ailleurs, elle

indique que la façon dont elles s'associent à l'État pour coproduire le système est généralement inconnue du public.

Aujourd'hui, il est difficile de cerner clairement les contours du dispositif final adopté qui est loin d'être homogène et standardisé. Il s'agit plutôt d'un cadre stratégique englobant un ensemble et une multitude d'initiatives locales.

Bien que le système soit relié à des technologies comme le big data et l'IA, nos recherches semblent indiquer qu'une telle mise en œuvre reste un objectif ambitieux vu l'hétérogénéité et le stockage décentralisé des données.[116],[117]

Les entretiens de Shazeda Ahmed avec des parties prenantes gouvernementales, technologiques et juridiques chinoises semblent révéler que *le système de crédit social chinois est plus limité dans sa collecte de données et fragmenté dans sa mise en œuvre sur le terrain que l'institution dystopique que ses critiques étrangers supposent qu'il est*.[118],[119]. Quel crédit accorder à ses parties prenantes dans un pays où l'information est contrôlée et verrouillée ? Là est la question…

[114] https://hai.stanford.edu/news/hai-fellow-shazeda-ahmed-understanding-chinas-social-credit-system

[115] https://www.rts.ch/info/monde/11137943-la-chine-veut-noter-tous-ses-habitants-et-installe-600-millions-de-cameras.html

[116] https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration

[117] https://logicmag.io/china/the-messy-truth-about-social-credit/

[118] https://fsi.stanford.edu/events/demystifying-china

[119] https://logicmag.io/china/the-messy-truth-about-social-credit/

Par ailleurs, nos recherches n'ont pas permis d'établir un lien entre le SCS et une éventuelle collecte massive des données via l'IdO grand public.

Figure 26: Capture d'écran de l'application WeChat Source

: The Messy Truth About Social Credit (logicmag.io)

La figure 25 montre une capture d'écran de l'application WeChat montrant des personnes et entreprises inscrites sur des listes noires sur une zone géographique donnée [120]

En conclusion, ce système de crédit social est un excellent cas d'école de captation et d'utilisation à grande échelle, par un régime, des données personnelles de ces citoyens dans le but de les contrôler et d'assoir son pouvoir. Dans la perspective d'un système homogène et centralisé régi par des technologies avancées telles que l'IA et le Big Data, il nous semble tout à fait vraisemblable que le régime chinois puisse recourir à l'IdO grand public comme source de collecte de données. Et nous ne voyons pas pourquoi il s'en priverait…

Ce qui est terrifiant dans cette affaire, c'est son potentiel de réplication et les voies que la technologie ouvre dans d'autres pays vers plus d'autoritarisme et d'asservissement des peuples.

V.2 STRATEGIE D'ISRAËL

[120] https://logicmag.io/china/the-messy-truth-about-social-credit/

Israël est reconnu comme un leader mondial dans le domaine de la cybersécurité des IdO, en grande partie grâce à une stratégie bien définie qui intègre divers aspects de la technologie et de la défense. Depuis sa création, Israël est en guerre, cette situation a induit un savoir et savoir-faire en termes de collecte de données personnelles et/ou du grand public et de leurs protections via toutes sorte de support. Aujourd'hui, les objets connectés sont rouages essentiels de la captation de données. Les orientations stratégiques d'Israël dans son ensemble sont appuyées et soutenues par les États-Unis qui a un droit de veto à l'ONU. Les influences entre ces deux pays ont des impacts sur les entreprises américaines, nous verrons le cas du projet NIMBUS.

V.2.1 Stratégie générale incluant les objets connectés et la captation de données

Les Startups et l'éducation scolaire sont intiment liées. Israël abrite un écosystème dynamique de cybersécurité avec plus de 470 startups actives, se classant au deuxième rang mondial pour les clusters de cybersécurité[121]. L'industrie israélienne de la cybersécurité est soutenue par un terreau fertile qui combine une armée formatrice, des entreprises prolifiques, et une stratégie d'État visant à développer des régions comme le désert du Néguev[122].

Les liens et relations entre les universités et les Start-Up sont pérennes et supervisés par des politiques gouvernementales. Le classement académique de 2023 des universités mondiales par l'université Jiao Tong de Shanghai, nous retrouvons 3 universités de

renommée mondiale dans le top : l'Université hébraïque de Jérusalem, le Technion et l'Institut Weizmann. Cette forte proximité entre le secteur économique et le monde universitaire se traduit par des programmes de transfert technologique. Chacun de ces instituts technologiques possède un bureau de transfert de technologie chargé de valoriser la recherche et de faire le lien avec l'industrie. Le monde académique est fortement incité à travailler avec les grands groupes, permettant à des entrepreneurs compétents de lancer des « spin off » sur la base de leurs brevets, en gardant les chercheurs au capital. Un spin off est une start-up ou une entreprise créée à partir des connaissances et technologies issues de la recherche, souvent d'un laboratoire universitaire ou scientifique. Les chercheurs universitaires sans être propriétaires des brevets qui restent en la possession des établissements et perçoivent une partie des royalties des licences de brevets. Les points cidessus sont extraits de la mission Digital Disruption Lab, en mars 2016 : « Présentation de l'écosystème numérique israélien »

[121] https://www.usine-digitale.fr/article/a-tel-aviv-la-cybersecurite-en-ordre-de-bataille-face-aux-defis-poses-par-l-intelligenceartificielle.N2150252

[122] https://www.usinenouvelle.com/article/plongee-au-coeur-de-l-industrie-israelienne-de-la cybersecurite.N2065132

Erez Maggor [123] titre : « Israël : toujours une « start-up nation » », ce titre est tiré de la publication : « Les politiques technologiques des puissances numériques » commandé par l'IFRI[124] en 2023

Cette étude montre qu'Israël revendique le titre de « start-up nation », et son économie high-tech florissante est souvent qualifiée de « nouvelle Silicon Valley». Elle se classe au septième rang dans l'index Bloomberg 2021 des « pays les plus innovants. Au total, le secteur de la haute technologie représente plus de 15 % du PIB total d'Israël et plus de 50 % de ses exportations. Il emploie 334 000 personnes, soit près de 10 % de l'ensemble de la population active, ce qui représente le taux le plus élevé de l'OCDE et plus du double de la moyenne des pays de l'OCDE.

TVL Partners est une entreprise à capital risque basée à Tel Aviv. Elle a réalisé un mapping[125] datant de 2015 et rassemblant les 60 sociétés israéliennes les plus innovantes dans l'univers des objets connectés. Depuis les attaques du 7 octobre 2023, il est assez difficile de trouver des informations en sources ouvertes.

[123] Erez Maggor est chercheur post-doctoral à la Martin Buber Society of Fellows de l'Université hébraïque de Jérusalem.

[124] IFRI : L'Institut Français des Relations Internationales est en France un centre de recherche et de débat indépendant consacré à l'analyse des questions internationales. Inspiré du modèle anglo-saxon, l'Ifri, think tank ou « laboratoire d'idées » français, s'est affirmé dans la durée, depuis sa création en 1979 par Thierry de Montbrial.

[125] https://www.objetconnecte.com/mapping-startups-israeliennes-iot/

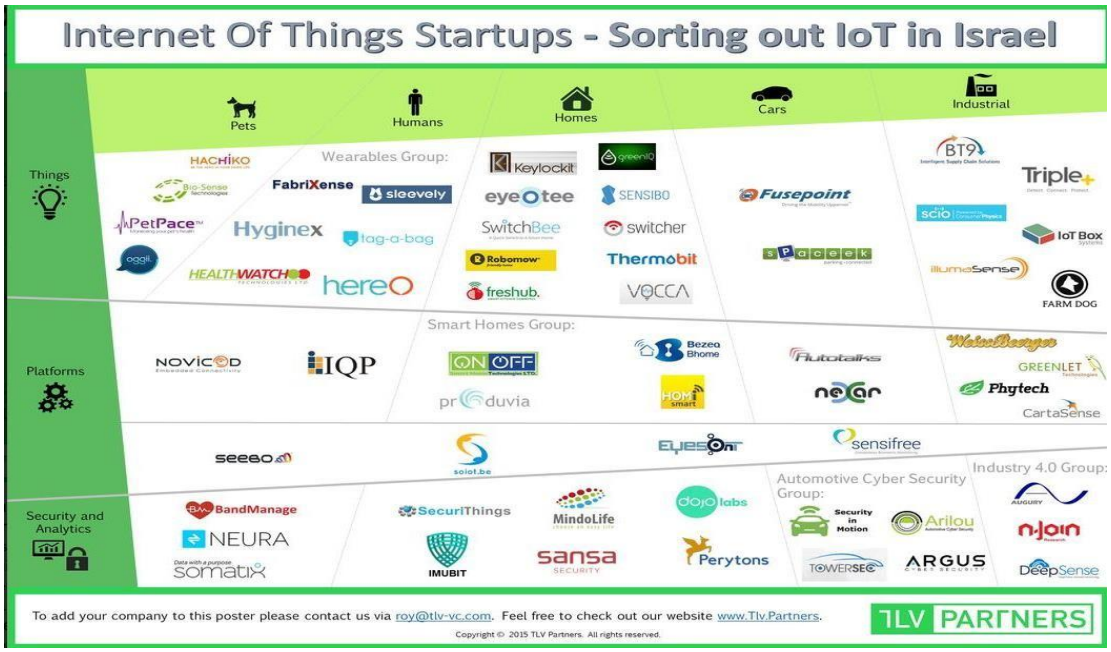


FIGURE 27: TVL PARTNERS 2015

Enfin l'événement majeur à Tel Aviv, le salon CyberTech Global a lieu chaque année. L'IdO est bien entendu un des sujets dominants de ce forum. Les conférences consacrées à la sécurité de la communication dans l'IdO sont très suivies. En 2019, Guy Bahiri, Directeur Technique de Splunk, a expliqué comment Splunk a développé une expertise dans la collecte et l'analyse des données, avec environ 50% des cas d'utilisation liés à la sécurité. La startup a fait ses preuves dans l'industrie et la maintenance prédictive des équipements de production.

L'écosystème d'innovation israélien, les programmes d'innovation gouvernementaux actuels, les principales réglementations, la politique en matière de données, l'infrastructure numérique et ses relations internationales convergent et participent au développement et l'expansion d'Israël dans cette conflictuelle. Nous démontrerons que cet écosystème d'innovation résulte de l'« État entrepreneurial » israélien. Les politiques publiques guidant l'orientation du développement technologique. La capacité d'Israël à conserver son statut de puissance numérique mondiale dépend à bien des égards de l'initiative et du soutien continus de l'État à l'égard du secteur privé.

Depuis sa création de l'état sioniste, elle a toujours su tisser des partenariats et collaborer avec son environnement proche et lointaine. Sur les 40 dernières années, son partenaire existentiel sont les États-Unis. Un paragraphe plus bas est dédié aux relations entre les deux pays. Israël a forgé des liens stratégiques avec d'autres pays, comme les Émirats

Arabes Unis, pour renforcer la cybersécurité à travers des accords de coopération[126]. Tous les pays à proximité ne sont pas spécifiquement des ennemis d'Israël. De plus, des

[126] https://www.usine-digitale.fr/article/a-tel-aviv-la-cybersecurite-en-ordre-de-bataille-face-aux-defis-poses-par-l-intelligenceartificielle.N2150252

partenariats avec des entreprises multinationales permettent d'intégrer des technologies innovantes et avancées pour sécuriser les infrastructures critiques.

Un aperçu des principaux aspects de ces collaborations économiques et technologiques.

Un hub d'innovation attirant de nombreux partenariats internationaux [127]:

- Le marché israélien, bien que relativement petit, est très dynamique avec un taux de chômage bas (4,3% en décembre 2022),
- Israël investit massivement dans la R&D, consacrant 5,4% de son budget à la recherche,
- Les secteurs clés de collaboration incluent les hautes technologies, la santé et la cybersécurité. Nous pouvons également citer la cleantech (la technologie propre »), ceux sont les techniques et les services industriels qui utilisent les ressources naturelles, l'énergie, l'eau, les matières premières dans une perspective d'amélioration importante de l'efficacité et de la productivité. Cette approche s'accompagne d'une réduction systématique de la toxicité induite et du volume de déchets, et assure une performance identique aux technologies existantes ou supérieure à celles-ci,
- Les exportations françaises vers Israël ont augmenté de 53% entre 2020 et 2022, atteignant 2,131 milliards d'euros.

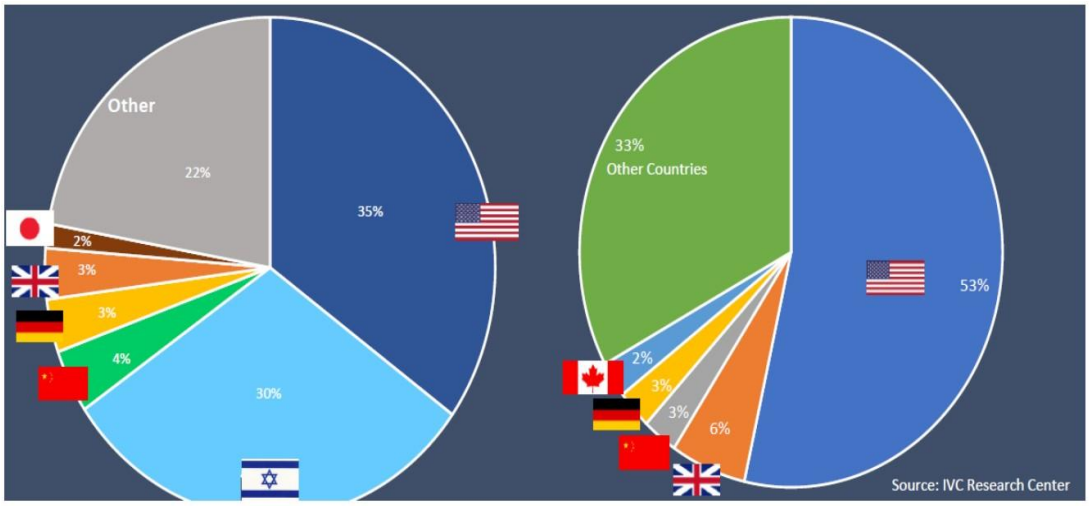


FIGURE 28: Part des investisseurs étrangers sur les 5 dernières années
https://www.tresor.economie.gouv.fr/Pays/IL/l -innovation-en-israel-newsletter-11-decembre-2018

Des programmes de soutien aux partenariats à travers plusieurs initiatives qui visent à promouvoir les collaborations avec les entreprises israéliennes :

- Masa Israel Journey [128] travaille avec des centaines de start-ups et entreprises pour enrichir la main-d'œuvre et l'écosystème entrepreneurial en Israël. Massa a été créée

[127] https://www.francaisaletranger.fr/2023/03/24/la-france-cherche-a-renforcer-ses-partenariats-economiques-avec-israel-dans-ledomaine-de-la-tech/
[128] https://www.masaisrael.org/fr/partners/

en tant qu'entreprise commune du gouvernement d'Israël et de l'Agence juive pour Israël et ses partenaires, les Fédérations juives d'Amérique du Nord et Keren Hayesod,

- Bpifrance[129] et l'Israel Innovation Authority ont lancé un appel à projets pour soutenir financièrement des partenariats en innovation entre entreprises françaises et israéliennes,
- Le programme européen Horizon 2020 [130]a permis de financer des projets collaboratifs comme LawTrain dans le domaine de la sécurité. Le projet LawTrain lancé le 1er mai 2015 et coordonné par l'Université de Bar-Ilan en Israël, vise à développer des technologies qui permettront l'uniformisation des méthodes d'interrogation de police dans le cadre de la lutte contre le trafic transnational de drogue. Il rassemble le ministère israélien de la Sécurité publique (qui chapeaute la police israélienne et le service israélien des prisons), le SPF Justice de Belgique et le ministère de l'Intérieur et la Guardia civil en Espagne.

Figure 29: ABITBOL ASSOCIES

Ces collaborations permettent aux pays partenaires de bénéficier de l'expertise israélienne dans des domaines de pointe comme la cybersécurité, l'intelligence artificielle et l'ingénierie, tout en offrant à Israël un accès élargi aux marchés internationaux.

Dans cette stratégie globale, Israël a fait un focus sur les IdO et les infrastructures critiques. Elle s'est imposée comme un acteur majeur dans le domaine de l'Internet des Objets (IdO) et de la protection des infrastructures critiques, en mettant l'accent sur la cybersécurité et l'innovation technologique.

À travers l'innovation, elle se positionne comme un centre important du développement de l'Internet des Objets[131]. Les entreprises israéliennes travaillent sur diverses applications de l'IdO, notamment :

- Les réseaux intelligents pour les services publics et les fournisseurs d'énergie,
- L'utilisation de capteurs compatibles IdO pour la collecte de données en temps réel,

[129] https://www.bpifrance.fr/nos-appels-a-projets-concours/partenariats-en-innovation-france-israel-nouvel-appel-a-projets

[130] https://www.abitbol-associes.com/fr/start-up-en-israel-comment-obtenir-un-financement-dans-le-cadre-du-nouveau-programmede-la-recherche-et-de-linnovation-de-lunion-europeenne-horizon-2020/

[131] https://fr.timesofisrael.com/linternet-des-objets-future-epine-dorsale-de-la-technologie-israelienne/

- L'intégration du Big Data et de l'intelligence artificielle pour améliorer la prise de décision.

La cybersécurité des infrastructures critiques est une priorité pour Israël. Quelques exemples d'initiatives :

- Déploiement de répéteurs GPS dans plus de 30 gares ferroviaires pour fournir un service géodépendant sécurisé[132],
- Développement de solutions de surveillance et de protection GPS pour les infrastructures ferroviaires[133],
- Mise en place de laboratoires permettant de simuler des cyberattaques sur différentes infrastructures critiques [134] , comme les centrales électriques ou les sites de désalinisation.

En conclusion, Israël a su capitaliser sur son expertise en cybersécurité pour devenir un leader dans la protection des infrastructures critiques à l'ère de l'Internet des Objets, en combinant innovation technologique, recherche académique et collaboration internationale.

V.2.2 Relation entre les État -Unis et l'État d'Israël

Les Etats-Unis ont commencé à s'intéresser au Moyen-Orient durant l'entre-deux guerres, découvrant l'importance stratégique de cette région riche en gisements de pétrole. Le 14 février 1945, le pacte de Quincy est signé entre l'Arabie Saoudite et les Etats-Unis permettant à la première de se voir assurer la sécurité et aux deuxièmes un accès au pétrole du royaume pendant 60 ans

C'est sur cette période que les relations entre les États-Unis et Israël se sont caractérisées et ont débuté par un soutien américain fort et durable envers l'État hébreu, fondé sur plusieurs facteurs.

Dans une alliance stratégique, les États-Unis considèrent Israël comme un allié majeur au Moyen-Orient depuis les années 1960[135]. Cette alliance s'est renforcée dans le contexte de la Guerre froide, lorsque Washington cherchait à contrer l'influence soviétique dans la région [136] . Aujourd'hui, Israël demeure un partenaire stratégique clé pour les intérêts américains dans cette zone géopolitique sensible.

[132] https://www.silicon.fr/press-release/infinidome-fournit-une-solution-de-surveillance-et-de-protection-gps-a-israel-railways

[133] https://www.silicon.fr/press-release/infinidome-fournit-une-solution-de-surveillance-et-de-protection-gps-a-israel-railways

[134] https://www.usine-digitale.fr/article/reportage-la-cyber-protection-des-infrastructures-critiques-au-c-ur-de-l-expertiseisraelienne.N2151092

[135] https://www.irenees.net/bdf_fiche-analyse-958_fr.html

[136] https://www.francetvinfo.fr/monde/proche-orient/israel-palestine/conflit-au-proche-orient-pourquoi-les-etats-unis-soutiennent-ilshistoriquement-israel_6246486.html

Le soutien militaire est conséquent, les États-Unis fournissent une assistance militaire massive [137]à Israël :

- Israël est le plus grand bénéficiaire de l'aide militaire américaine chaque année. De 2019 à 2028 l'aide militaire prévue sera à près de 4 milliards de dollars par an.[138]
- Les deux pays coopèrent étroitement en matière de recherche et développement militaire.
- Israël bénéficie du statut d'allié majeur hors OTAN depuis 1987, lui donnant accès privilégié à l'armement américain.

Des liens politiques et sociétaux profonds expliquent l'attachement américain à Israël :

- Une sensibilité historique et religieuse au destin d'Israël dans la société américaine[139].
- L'influence politique de la communauté juive américaine.
- Le rôle du lobby pro-israélien aux États-Unis, qui pèse sur la politique étrangère américaine.

Une relation complexe et un soutien de longue date ne sont pas exempte de tensions.

- Les États-Unis tentent parfois de modérer certaines actions israéliennes, comme récemment à Gaza[140].
- Certains remettent en question les bénéfices de ce soutien inconditionnel [141]pour les intérêts américains.
- Le projet Nimbus est essentiellement un projet conjoint entre Google Cloud, Amazon Web Services (AWS) et le gouvernement israélien. Le projet, lancé en 2021, vise à fournir des capacités de pointe en matière de cloud computing et d'IA aux Forces de défense israéliennes (FDI) et à différents organismes gouvernementaux israéliens. Néanmoins, le soutien à Israël reste une constante de la politique étrangère américaine, transcendant les clivages partisans.

V.2.3 Le Projet NIMBUS

Le projet Nimbus est une initiative majeure de cloud computing lancée par le gouvernement israélien en 2019. Les principaux éléments à retenir sur ce projet controversé. Les employés exhortent Google et Amazon à mettre fin à leurs contrats avec Israël.

Le projet Nimbus vise à fournir des services de cloud public au gouvernement israélien, au ministère de la Défense et à l'armée israélienne. En 2021, Google et Amazon ont remporté

[137] https://fr.wikipedia.org/wiki/Relations_militaires_entre_les_%C3%89tats-Unis_et_Isra%C3%ABl

[138] Piotr Smolar, « L'alliance militaire entre les Etats-Unis et Israël renforcée pour dix ans », Le Monde, 14 septembre 2016

[139] https://www.irenees.net/bdf_fiche-analyse-958_fr.html

[140] https://www.iris-france.org/180521-la-relation-etats-unis-israel-expliquez-moi/

[141] https://fr.wikipedia.org/wiki/Relations_militaires_entre_les_%C3%89tats-Unis_et_Isra%C3%ABl

les contrats pour ce projet d'une valeur de 1,2 milliard de dollars. Sur le site internet de : «LES CRISES » , il y a le titre le : » « Les liens cachés entre l'armée israélienne et

le projet Nimbus de Google et Amazon [142]». Le site IsraelValley trace le 3 novembre 2022 : « Le projet Nimbus d'Israël. Un investissement de $1,23 milliard[143] ».

Les caractéristiques principales :

- Construction de six centres de données en Israël pour un investissement d'au moins 1,23 milliard de dollars,
- Fourniture de services cloud, d'apprentissage automatique et d'analyse de données,
- Stockage sécurisé des données gouvernementales en Israël,
- Transition des services gouvernementaux vers le cloud pour améliorer l'efficacité.

Le projet Nimbus a suscité des controverses et de vives critiques en raison de son implication militaire :

- L'armée israélienne est un partenaire clé du projet depuis le début,
- Des employés de Google et Amazon ont protesté contre le projet, craignant qu'il ne soit utilisé pour faciliter les violations des droits des Palestiniens,
- Neuf employés de Google [144] ont été arrêtés lors de manifestations contre le projet Nimbus.

Des enjeux et des préoccupations, les opposants au projet s'inquiètent de l'utilisation potentielle de ces technologies pour :

- Renforcer l'occupation et les actions militaires israéliennes dans les territoires palestiniens,
- Faciliter la surveillance et le contrôle des Palestiniens,
- Collecter et analyser des données provenant de multiples sources, y compris des objets connectés telle que les caméras de rue et de drones.

Le projet Nimbus reste donc au cœur d'un débat éthique sur le rôle des géants de la technologie dans les conflits géopolitiques et les implications potentielles pour les droits humains.

V.2.4 Les points conclusifs

Israël est reconnu pour ses avancées significatives en cybersécurité et en création d'entreprise innovantes, notamment dans le domaine de l'Internet des Objets (IdO). Tout cela n'aurait pas été possible sans le soutien des Américains.

Voici quelques éléments clés de la stratégie israélienne en matière de cybersécurité IdO.

[142] https://www.arabnews.fr/node/154101/monde-arabe

[143] https://israelvalley.com/2022/11/03/le-projet-nimbus-disrael-un-investissement-de-123-milliard/

[144] https://www.aa.com.tr/fr/monde/neuf-employ%C3%A9s-de-google-en-garde-%C3%A0-vue-pour-avoir-protest%C3%A9-contre-leprojet-nimbus-entre-google-et-isra%C3%ABl/3194023

Le Centre d'Excellence CyberSpark, Israël a établi le centre à Beer Sheva, qui réunit les principaux acteurs de la cybersécurité israéliens et internationaux. Ce centre se concentre sur l'innovation et la collaboration dans le domaine de la cybersécurité, incluant l'IdO.

Des investissements massivement dans la cybersécurité, avec environ 1 milliard de dollars en investissements privés. Les entreprises israéliennes sont reconnues mondialement pour leur

expertise, notamment dans la collecte et l'analyse des données liées à la sécurité IdO. Microsoft serait sur le point de débourser 170 millions de dollars pour s'offrir CyberX. CyberX a développé un logiciel sans agent qui surveille en permanence et offre une visibilité sur les objets IoT et les systèmes de contrôle industriels non gérés dans les environnements informatiques et de technologie opérationnelle (OT).

Elle s'engage dans des accords de coopération internationale pour renforcer la cybersécurité, comme l'accord avec l'Australie pour la cybersécurité de l'aviation civile. Elle n'est pas centrée que sur les objets connectés, elle saisit toutes les opportunités technologiques

Israël et les États-Unis entretiennent des relations militaires très étroites en raison des intérêts économiques américains dans la région du Moyen-Orient (doctrine Kissinger) ainsi que du travail du lobby pro-israélien aux États-Unis qui influencent sensiblement la politique américaine dans cette région. Le lobby pro-israélien sert de courroie de transmission de la politique israélienne aux États-Unis, préparant les projets de lois soumis au vote du Congrès des États-Unis en fonction des priorités israéliennes, coordonnant et transmettant de l'information issue du gouvernement des États-Unis vers le gouvernement israélien tout en s'impliquant dans des opérations d'espionnage au profit des services secrets israéliens.

Les stratégies de cybersécurité pour l'IdO incluent l'identification des objectifs de sécurité pertinents et la mise en place de mesures techniques et organisationnelles pour les atteindre. Cela comprend la sécurisation des systèmes d'objets connectés et la protection contre les cybermenaces. À date, il est difficile de dire, comment les attaques du 7 octobre 2023 autour de la bande de Gaza ont impacté d'un point de technologique et politique.

En termes d'enjeux et de défis, l'IdO présente des risques accrus de cyberattaques en raison de la multiplication des points de vulnérabilité. Israël travaille sur des normes internationales pour améliorer la sécurité et la protection des utilisateurs. Il continue de jouer un rôle de leader dans l'élaboration de stratégies de cybersécurité innovantes et efficaces, en particulier dans le domaine en pleine expansion de l'IdO.

Ce qui distingue l'Internet des objets en Israël et en Inde, c'est sa maturité et son orientation. Israël se distingue à l'échelle mondiale en matière de cybersécurité et d'innovation IdO, grâce à son écosystème technologique sophistiqué. Il met l'accent sur la défense, la sécurité et l'agriculture de précision dans ses applications IdO, en accordant une attention particulière à la protection des données. D'autre part, l'Inde continue de progresser dans ce domaine, avec des projets importants tels que les smart cities et une utilisation plus étendue de l'IdO dans les infrastructures publiques et les services urbains, mais avec des obstacles liés à la cybersécurité. Il nous a semblé important d'examiner la stratégie de l'Inde car elle est en train de rivaliser avec des géants sur ce marché.

V.3 STRATEGIE DE L'INDE

L'Inde est un pays majeur avec ses diverses richesses culturelles, ethniques et religieuses. Elle est également l'un des pays émergents de l'Asie, rival de la Chine, alliée des pays occidentaux, maintenant des relations solides avec la Russie (notamment dans le cadre de l'importation du pétrole).

La stratégie proactive de l'Inde vise à devenir un leader mondial dans le domaine de l'Internet des objets. Elle vise principalement à favoriser l'innovation et le progrès technologique tout en renforçant la sécurité informatique. L'Inde cherche à améliorer les services publics et à soutenir son développement économique en mettant en place des projets de smart cities, en étendant les réseaux de capteurs et en modernisant les infrastructures connectées. Cependant, afin d'exploiter pleinement son potentiel, l'Inde doit faire face à des difficultés liées à la régulation, à la sécurité des données et à la gestion des cyberattaques.

L'Inde sait parfaitement quelle est sa position géopolitique dans l'Asie-Pacifique, elle sait se positionner de manière diplomatique auprès de ses voisins et des grandes puissances. Il convient cependant de souligner que l'Inde n'est pas réputée pour avoir participé à des guerres économiques agressives contre d'autres pays.

Avec la France, elle a une relation stratégique avec l'implantation de plusieurs entreprises françaises y compris celles du CAC 40.

En règle générale, l'Inde adopte une approche de diplomatie économique afin de créer des alliances commerciales et consolider sa position dans l'économie internationale. Le pays vise à susciter l'intérêt des investisseurs étrangers, à stimuler ses secteurs industriels et à favoriser le commerce international de manière pacifique et collaborative.

V.3.1 Dans l'univers du numérique

En ce qui concerne les services informatiques, l'Inde est devenue un leader mondial. Par exemple, certaines entreprises sont regroupées dans NASSCOM, une association nationale des sociétés de logiciels et de services, ce qui représente un développement majeur sur le plan technologique. En effet, cette fondation propose des solutions technologiques pour répondre aux besoins des entreprises, des citoyens. Un volet important sur le déploiement de l'IdO dans le pays afin de rendre les usagers plus autonomes.

L'inde attire de plus en plus des investisseurs étrangers et dépasse même la Chine sur le flux IDE « Investissement directs étrangers ». La fondation NASSCOM pourrait être une force de frappe importante autour de l'Internet des Objets.

L'Inde suscite l'intérêt des investisseurs étrangers et le gouvernement de Modi vise à améliorer le numérique pour qu'il soit accessible à tous les Indiens. Avec une économie en plein essor et une population très jeune, elle se distingue par l'attrait de sa main-d'œuvre qualifiée. Il s'agit

d'une puissance en plein essor qui pourrait s'emparer d'un marché majeur autour de l'Internet des objets.

V.3.2 L'IdO de l'Inde

L'Inde exporte des objets connectés, tels que des smartphones, des tablettes, des montres intelligentes et d'autres appareils électroniques. L'Inde est un acteur important sur le marché mondial des technologies de l'information et de la communication, et de nombreuses entreprises indiennes produisent des objets connectés pour être vendus tant sur le marché intérieur qu'à l'étranger.

« Le marché indien de l'Internet des objets (IoT) devrait atteindre 10,2 Mds USD d'ici 2024, avec un taux de croissance annuel moyen de 12,9 %. Le marché de l'IoT était évalué à 5,6 Mds USD en 2020, contre 1,3 Mds USD en 2016, soit une croissance de plus de 330 % en cinq ans. » (Team France Export , 2023)

Certains fabricants indiens d'appareils électroniques, tels que **Micromax**, **Lava, Tata Electronics, Karbonn et Intex** (MOKO TECHNOLOGY, s.d.), produisent des smartphones et des tablettes qui sont exportés vers d'autres pays, pour exemple la société Lava investit le Nigeria, le Ghana dans la vente de téléphone portable à petit prix. L'Inde est donc devenue un centre majeur pour la production de smartphones grâce à des initiatives telles que le programme "Make in India" visant à encourager la production locale.

Ainsi, l'Inde exporte non seulement des objets connectés fabriqués localement, mais elle est également un acteur important dans la chaîne d'approvisionnement mondiale pour la production et l'exportation de ces appareils.

« Le marché indien du SmartHome était évalué à 4,83 Mds USD en 2022. Les revenus devraient augmenter à un TCAC de 13,52 %, ce qui devrait donner un volume de marché de 8,08 Mds USD d'ici 2026. L'IoT a été largement perpétué par l'innovation des technologies intelligentes et la création de produits tels que Amazon Echo ou Google Home, qui ont joué un rôle important dans le développement de la domotique.
Le marché de la robotique en Inde a également connu une forte croissance ces dernières années. Les installations de robotique ont atteint 4 945 unités en 2021, soit une augmentation de 54 % par rapport à 2020 avec 3215 unités. Le marché devrait atteindre 801,4 Mds USD d'ici 2026 avec un TCAC de 14,2 % sur la période 2020-2025.
Les objets connectés, tels que les smartphones, les montres intelligentes et les appareils domestiques intelligents, sont de plus en plus populaires en Inde. En raison de la croissance rapide de la connectivité Internet dans le pays, de plus en plus de gens adoptent ces technologies pour simplifier leur vie quotidienne. » (Les Fondamentaux, s.d.)

Les objets connectés peuvent offrir de nombreux avantages aux habitants de l'Inde, tels que la possibilité de contrôler à distance leurs appareils domestiques, de surveiller leur santé et leur condition physique, ou encore de rester connectés avec leurs proches. Ces technologies peuvent également améliorer l'efficacité énergétique des foyers et contribuer à réduire les coûts de fonctionnement.

D'après Modi, son but est de transformer son pays en une nation puissante (Digital India), et il croit que c'est grâce à la technologie moderne qu'il réussira. Il est conscient des talents et de la main-d'œuvre qu'il possède dans le pays.

La puissance numérique de l'Inde repose sur une combinaison de personnel qualifié, d'un écosystème dynamique de startups, de politiques gouvernementales favorables, d'une infrastructure numérique en plein essor et d'un développement significatif de l'IoT dans le pays. En bref, en cas de cyberattaque, l'Inde peut se présenter comme un pays puissant capable de manipuler ses rivaux en volant leurs données personnelles.

Selon NASSCOM, l'Inde a déployé l'IdO sur son territoire et à grande échelle

« L'introduction de l'IoT en Inde a marqué le début d'une nouvelle révolution industrielle, également connue sous le nom d'Industrie 4.0. L'IoT joue un rôle de premier plan dans le contexte commercial et technologique en constante évolution de l'IoT, en plus du nouveau programme « Digital India » lancé par le gouvernement. Selon un récent rapport publié par Zinnov [2] en juin 2020, les investissements dans l'IoT en Inde ont atteint près de 5 milliards USD en 2019, et devraient atteindre 15 milliards USD en 2021.

L'Inde a déjà commencé à travailler sur les dernières tendances à venir. Vous trouverez cidessous les principales tendances IoT 2020 en Inde » (nasscom community, s.d.)*:*

Figure 30 : Tendances IdO 2020 en Inde

Source : Technologie IoT en Inde | nasscom | La communauté officielle de l'industrie informatique indienne (community-nasscom-in.translate.goog)

L'Inde joue un rôle essentiel dans l'économie numérique mondiale en raison de ces éléments. Toutefois, afin de préserver et consolider cette position, l'Inde devra poursuivre ses investissements dans l'éducation, l'innovation et l'infrastructure, tout en affrontant les défis liés à la cybersécurité et à la confidentialité des informations.

En résumé, l'Inde possède les compétences techniques et humaines nécessaires et il est possible de concevoir que le pays pourrait avoir une capacité de frappe considérable si nous devions envisager un espionnage massif grâce à l'IdO.

V.3.3 Cybersécurité et protection des données personnelles

Généralement, l'adoption croissante des objets connectés soulève également des questions de sécurité et de protection de la vie privée. Il est essentiel que les fabricants et les fournisseurs de services prennent aussi des mesures pour garantir la sécurité des données des utilisateurs et protéger leur vie privée.

L'Inde a aussi été très touchée par des attaques, par rancongiciel surtout pendant la pandémie, mais l'écosystème de l'Inde est très actif, les startups se sont mis vite en ordre de marche pour contrer le problème.

« Le marché indien des produits et services de cybersécurité a totalisé un chiffre d'affaires de 9,85 milliards de dollars en 2021, suivant un taux de croissance annuel moyen (TCAM) de près de 40 % au cours des deux dernières années, selon le rapport du Data Security Council of India intitulé « India Cybersecurity Industry Report – Services & Product Growth Story », ce qui signifie qu'il a presque doublé sur cette période (5,04 milliards de dollars en 2019) » (INCYBER News, s.d.; INCYBER News, s.d.)

Par ailleurs, la France et l'Inde et avec le soutien de l'ANSSI ont renforcé leurs relations sur le sujet du cyber sécurité, une feuille de route franco-indienne a été rédigée dans ce sens (Diplomatie.gouv.fr)

On peut conclure que l'Inde possède une capacité de soft power qui pourrait toujours être exploitée, en prenant des mesures pour protéger les données de ses citoyens contre les diverses menaces de cyberattaques.

V.3.4 Le RGPD Indien

Le Digital Personal Data Protection Act, 2023 (DPDPA) a été adopté le 11 août 2023. Le DPDPA Indien se concentre sur la souveraineté des données et l'équilibre entre la protection des données et le développement économique.

En résumé, le RGPD indien (DPDPA) est plus ou moins différent de la France, contrairement au RGPD, le DPDPA ne cherche pas à réglementer une opération de traitement ou une activité qui est entièrement manuelle ou non automatisée. Dans les parties impliquées, contrairement au RGPD, le DPDPA n'impose pas d'obligations directement au *data processor*, mais attend des *data fiduciary* qu'ils s'assurent de la conformité des *data processors* qu'elles engagent par le biais d'accords de traitement de données. Voir les données (DS Avocats)

L'Inde est le pays qui récence plusieurs entreprises multi nationales, des investisseurs, des startups et la protection des données devient un noyau important et un sujet controversé en fonction de qui vient investir dans le pays.

Notamment contre des géants de la technologie comme les GAFAM. En effet, des entités telles que Google souhaitent exporter & stocker les données des Indiens sur leurs territoires et le gouvernement veut maintenir les données de ses citoyens sur son sol.

Compte tenu de sa population et de l'explosion numérique dans le développement de l'IdO, l'Inde se doit de protéger les données de ces citoyens et doit y apporter les mesures de sécurité nécessaire.

« L'Inde sort ses griffes. Le gouvernement plancherait sur un projet de loi afin de compliquer l'expansion des géants américains de la tech sur son territoire. L'objectif : reprendre le contrôle des données de ses citoyens et favoriser l'écosystème local pour faire émerger ses propres mastodontes du numérique. Le projet de loi propose notamment de rendre obligatoire, pour les sociétés étrangères, le stockage des données personnelles des utilisateurs indiens - issues des réseaux sociaux, des moteurs de recherche ou encore des plateformes de e-commerce - sur son sol. Les données devront également être rendues accessibles aux autorités locales en cas d'enquête. » (LA TRIBUNE)

Pour autant, l'Inde a bien mis en place une politique de cybersécurité pour se protéger. Le pays a développé le National Cyber Security Policy en 2013, qui fournit un cadre pour protéger l'infrastructure nationale critique, promouvoir la sensibilisation à la cybersécurité, et encourager la collaboration entre le gouvernement, le secteur privé et les citoyens. De plus, l'Inde a créé des organismes comme le CERT-In ((WIKIPEDIA)).

Cependant, la mise à jour et l'application stricte des réglementations spécifiques à l'IdO restent nécessaires.

Enfin, **pour conclure**, à travers les différentes sources et rapports, nous pensons que les intérêts communs entre l'Inde et la France sont nombreux, et leur collaboration étroite est essentielle pour relever les défis mondiaux. Il n'y a aucune raison de considérer l'Inde comme une menace pour la France. Au contraire, les deux pays cherchent à renforcer leur coopération pour tirer parti de leurs expériences respectives.

Cela dit, l'Inde est en passe de devenir un leader mondial sur le marché de l'Internet des Objets. Bien que l'IdO permette aux Indiens de se connecter plus facilement, que ce soit dans le domaine de la communication ou de la maison connectée, il augmente aussi les risques. En effet, à mesure que les objets sont de plus en plus connectés à Internet, ils deviennent davantage exposés aux cyberattaques

L'Internet des objets est en perpétuelle mutation, et les cybercriminels cherchent constamment de nouvelles façons de l'exploiter. Alors que nous nous dirigeons vers un avenir où l'IdO occupera une place centrale, il est primordial de prendre en compte son importance croissante. Le RGPD en France et le DPDPA en Inde ne suffiront pas à eux seuls pour protéger les données personnelles de leurs citoyens. Des mesures de sécurité supplémentaires seront nécessaires pour renforcer la protection de ces données.

Aujourd'hui, il n'existe pas de stratégie commune spécifique entre les deux pays, en dehors de leur partenariat et de la feuille de route franco-indienne sur la cybersécurité et le numérique.

À ce stade, il n'y a aucune preuve publique et vérifiée d'utilisation de l'IdO par l'Inde pour mener des opérations d'espionnage à grande échelle. Toutefois, comme dans de nombreux

pays, les appareils IdO peuvent potentiellement être utilisés à des fins de surveillance, notamment dans des contextes de sécurité nationale. L'Inde accorde une attention particulière à la protection de ses infrastructures critiques contre les cybermenaces, plutôt qu'à l'utilisation de l'IdO à des fins d'espionnage.

VI. Stratégies pour un Internet des objets plus sûr : Recommandations et perspectives

VI. STRATEGIES POUR UN INTERNET DES OBJETS PLUS SUR : RECOMMANDATIONS ET PERSPECTIVES

Plusieurs rapports sur l'IdO ont été publiés au cours des dernières années, jusqu'en 2022, proposant diverses recommandations. Cependant, une grande partie de ces suggestions ne semble pas avoir été mise en œuvre. Nous avons donc choisi de reprendre et de prioriser celles qui nous paraissent les plus essentielles.

De plus, en nous appuyant sur nos recherches concernant les stratégies adoptées par des nations plus avancées dans le domaine de l'IdO, nous avons identifié d'autres recommandations qui nous semblent tout aussi pertinentes et cruciales.

Cette section se veut à la fois une synthèse et une consolidation de toutes les orientations de recommandations évoquées ou sous-entendues dans les sections précédentes. Bien que cela puisse sembler redondant, nous avons estimé qu'il était plus lisible et plus efficace de regrouper toutes les recommandations dans une partie dédiée.

Étant donné la complexité de l'écosystème de l'IdO, les recommandations visant à réduire les risques associés à ces dispositifs, ainsi qu'à protéger les données personnelles qu'ils manipulent, doivent en tenir compte. Elles doivent aborder divers enjeux et encourager une mise en œuvre simultanée d'actions sur plusieurs fronts : sensibilisation, technologie, organisation et régulation (normes, standards et réglementations).

Nous allons tenter d'envisager ces recommandations selon un quadriptyque : surveiller, analyser, protéger, influencer.

Nous n'avons pas de solutions toutes prêtes, mais nous proposons des pistes de réflexion à un niveau purement stratégique. Aux niveaux tactique et opérationnel, l'ENISA a, par exemple, produit une liste de plus d'une cinquantaine de recommandations et de bonnes pratiques pour le développement des appareils IdO domestiques[145].

Par ailleurs, il est possible que des solutions déjà existantes soient tenues confidentielles, ce qui nous empêche de les évaluer ou d'en tenir compte.

Recommandation n° 1 : Outils et structures d'observation dédiés à l'IdO

Dans une économie mondiale de libre-échange, à défaut de pouvoir contrôler le marché de l'IdO, il est crucial d'éviter de le subir. Nous pensons qu'il est essentiel de dresser un état des lieux et d'analyser notre niveau d'exposition et de vulnérabilité.
Pour cela, des outils d'observation dédiés à l'IdO, axés sur les technologies, les fournisseurs et les vulnérabilités, sont nécessaires et indispensables pour estimer notre surface d'exposition aux attaques et évaluer les efforts nécessaires pour réduire les risques inhérents aux appareils IdO.

Des outils privés en ligne, tels que Thingful, existent déjà et sont utilisés pour recueillir des données provenant de machines connectées et d'appareils IdO, mais Shodan est actuellement le meilleur en raison de la facilité d'utilisation de son interface web et de son interface de programmation d'applications (API). Il existe même une plateforme appelée SCUBA [146] (acronyme de 'scaphandre' en anglais), développée par l'équipe RESIST de

[145] Security and Resilience of Smart Home Environments.pdf
[146] SCUBA : des audits automatisés pour les objets connectés | Inria

l'Institut National de Recherche en Informatique et en Automatique (INRIA), qui est capable de réaliser des audits automatisés d'objets connectés.

Les outils sont donc nombreux, mais ce qui fait défaut, c'est une organisation capable de soutenir ces missions d'audit, de surveillance et de veille sur le long terme.
Il serait peut-être pertinent de confier cette réflexion, concernant l'organisation nécessaire, à la représentation nationale par le biais de la Commission Supérieure du Numérique et des Postes (CSNP).

Recommandation n° 2 : Renforcement du RGPD ou loi de cybersécurité nationale dédiée à l'IdO ?

À l'image du pendant chinois du RGPD, qui est d'ailleurs très récent, il serait pertinent de renforcer le RGPD afin de rendre obligatoire la localisation des données personnelles des citoyens européens et des résidents de leurs pays en Europe, sur des serveurs soumis à la législation européenne.

Toutefois, la question se pose de savoir si cette perspective est réellement envisageable ou s'il s'agit d'une utopie dans un monde dominé par les GAFAM et verrouillé par les lois extraterritoriales américaines. L'arsenal réglementaire européen semble avoir peu d'effet sur les géants de la Tech américains, qui continuent de capter nos données personnelles sans notre consentement. On pourrait en dire autant de la Chine avec ses BATX.

Comme évoqué précédemment dans la partie concernant le Cloud, tant que nos données seront hébergées sur les serveurs des géants technologiques américains, elles resteront vulnérables aux convoitises, légitimées par le Cloud Act.

Mais nous ne nous engagerons pas dans le débat du cloud souverain que certains de nos collègues de la MACYB02 [147] ont admirablement décortiqué et dont ils ont démontré la complexité. Nous ne pouvons que formuler le vœu qu'un jour une ou plusieurs initiatives européennes puissent voir le jour et nous affranchir des Google, Amazon et Microsoft. Nous pensons aux initiatives GAIA-X, EUCLIDE et à bien d'autres.

Une initiative réglementaire européenne pourrait-elle techniquement et juridiquement neutraliser le Cloud Act ? Les Européens sont-ils capables de construire un cloud souverain et d'imposer aux GAFAM et BATX de stocker nos données personnelles sur le territoire de l'UE lorsqu'ils y opèrent ?

Si les Chinois y sont parvenus, les Européens ont peut-être aussi une chance de réussir. Si la France a réussi à atténuer l'intrusion et l'agressivité de l'extraterritorialité des lois américaines grâce aux Lois Sapin, nos juristes pourraient obtenir un résultat similaire pour protéger nos données personnelles.

[147] Cloudspublics:Cybersécurité etenjeux.Peut-onleurfaire confianceetgarantirune souveraineté?, Ben Cacha, ANGAT NIVI, Augustin NGOMA, Carole DEGHMOUN, Décembre 2022

Dans le cadre du projet Nimbus, mentionné dans la section sur la stratégie, le petit État d'Israël nous donne une leçon en matière de protection des données personnelles et sensibles en imposant des exigences strictes à AWS et Google. La France et l'Europe devraient s'en inspirer.

Nous pourrions également évoquer et mettre en avant l'une des recommandations de France Stratégie dans son rapport de 2022[148], qui suggérait d'adapter le cadre réglementaire actuel afin de garantir un bon niveau de protection pour les publics vulnérables (personnes mineures, âgées, en perte d'autonomie, etc.).

Autant de questions qu'il serait pertinent de soumettre aux spécialistes, juristes et législateurs, afin d'explorer la faisabilité et les potentialités de ces mesures. Si les options réglementaires s'avèrent impossibles ou insuffisantes, il serait alors nécessaire d'investir dans la recherche et développement (R&D) ainsi que dans les aspects normatifs, comme le précisent les deux recommandations qui vont suivre.

Recommandation n° 3 : Encourager et promouvoir les travaux de recherche et leur donner une dimension européenne

Il est nécessaire de trouver un compromis entre la garantie d'une forte protection de la vie privée et la préservation de l'utilité des données issues de l'Internet des objets.
D'une part, nous devrions pouvoir exploiter massivement les données des utilisateurs d'appareils IdO lorsqu'il s'agit de sauver des vies, par exemple. D'autre part, le déploiement tous azimuts de l'IdO ouvre la porte à de potentielles graves dérives dans la captation des données personnelles et l'atteinte à la vie privée, comme nous l'avons décrit et développé dans la partie concernant les stratégies.

Un autre défi consiste à minimiser le rapport coût/bénéfice de ces mécanismes de confidentialité pour les appareils IdO, qui sont très souvent équipés de ressources limitées.

Nos chercheurs sont donc confrontés à une multitude de défis. Il est nécessaire de développer de nouvelles techniques de prétraitement des données à la source, directement sur les appareils IdO, avant même qu'elles ne parviennent aux clouds tiers, et d'obfusquer les données qui ne répondent pas à un 'intérêt légitime' précis. Par ailleurs, il faudrait concevoir de nouvelles primitives cryptographiques capables de résister à des attaques pré ou post-quantiques, tout en étant compatibles avec les capacités de traitement limitées des appareils IdO[149].

Des recherches sont également menées pour redonner au propriétaire des données un contrôle effectif sur le processus de chiffrement, d'une part, et sur le partage de ces données, d'autre part, indépendamment de leur localisation.

[148] le monde de l'internet des objets : des dynamiques à maîtriser, février 2022, sous la direction scientifique de Claude Kirchner.

[149] Internet des Objets: Défis sociétaux et domaines de recherche scientifique pour l'Internet des Objets (IoT) (hal.science)

Des solutions intéressantes pour atteindre ces objectifs ont été mises en œuvre par certains chercheurs grâce au chiffrement par attributs, ou *Attribute Based Encryption* (ABE). Ce dernier offre simultanément des fonctionnalités de chiffrement et de contrôle d'accès basé sur des attributs, en plus de sécuriser la transmission et le stockage des données. Il s'agit d'un schéma de chiffrement à clé publique de type un-à-plusieurs, où l'on chiffre avec une seule clé et où il est possible de générer, sur la base d'attributs descriptifs, plusieurs clés de déchiffrement, chacune dédiée à un utilisateur spécifique. À aucun moment, le fournisseur de services n'accède aux données en clair. De plus, aucune connaissance préalable de l'identité des destinataires n'est requise, et seules les entités possédant des attributs satisfaisant une politique d'accès aux données peuvent déchiffrer le texte[150].

À titre d'exemple, plusieurs équipes de l'INRIA (PRIVATICS, ARIC, COMETE) travaillent à l'adaptation des primitives préquantiques et postquantiques aux appareils IdO, à la conception de mécanismes améliorant la transparence pour les utilisateurs d'objets connectés et assurant leur consentement approprié. Elles se consacrent également à la conception et à l'analyse d'algorithmes de chiffrement entièrement homomorphes[151], et à leur utilisation pour des calculs protégeant la vie privée, ainsi qu'à la conception et à l'analyse de mécanismes de confidentialité différentielle [152] utilisés pour des calculs préservant la vie privée.

On pourrait également citer de nombreuses autres initiatives françaises et européennes, telles que le système d'exploitation RIOT ou l'adoption des identifiants uniques de l'AFNIC et ses travaux.

D'excellentes initiatives open source et libres, telles que OpenHAB et Home Assistant, permettent de fédérer une multitude d'objets connectés de la maison de divers constructeurs, au sein d'un même écosystème. Ces alternatives permettent de se soustraire à la dépendance au cloud en offrant un fonctionnement en local. Nous illustrons un cas d'usage en annexe X.

Il serait pertinent d'encourager et d'amplifier ces initiatives open source, tout en étudiant la possibilité de proposer au grand public des packages logiciels prêts à l'emploi et intuitifs, intégrant les mesures essentielles pour la sécurité de ces dispositifs ainsi que pour la protection des données personnelles qu'ils collectent.

Cela suppose que les fabricants coopèrent volontairement en ouvrant leur système pour l'intégration de tels packages ou bien qu'ils soient incités par des dispositifs réglementaires

[150] Thèse de doctorat : Proposition d'un modèle de sécurité pour la protection de données personnelles dans les systèmes basés sur l'internet des objets, Youcef Ould Yahia, Conservatoire national des arts et métiers (CNAM) à Paris, 2019

[151] Une classe avancée d'algorithmes de chiffrement qui permettent de réaliser des calculs sur des données chiffrées sans avoir besoin de les déchiffrer au préalable. L'un des principaux avantages est le traitement des données sensibles dans des environnements non sécurisés tout en maintenant leur confidentialité.

[152] Un ensemble de techniques qui permettent d'extraire des informations statistiques utiles à partir de bases de données contenant des données personnelles tout en garantissant la confidentialité des individus. Pour protéger les données sensibles, du "bruit" statistique est ajouté aux résultats, afin de rendre extrêmement difficile, l'identification d'un individu à partir des données publiées.

et des labels à suivre cette direction. Nous développons cet aspect de labellisation et de certification dans la recommandation n° 5.

Ces exemples donnent une idée du large éventail de ce qui se fait déjà, mais aussi de ce qui pourrait être accompli si nos laboratoires de recherche étaient dotés de moyens suffisants pour explorer de nouvelles voies, et si toutes ces initiatives étaient mieux coordonnées à un niveau européen.

Les meilleures compétences dans chaque domaine de recherche de l'écosystème IdO devraient être intégrées au sein des laboratoires de recherche les plus avancés de l'UE. Ces pôles d'excellence doivent contribuer à un programme européen global et coordonné afin d'optimiser les ressources et d'accélérer la recherche.

Nous appelons nos politiciens à créer les conditions nécessaires pour transformer une simple vision de marché commun en une véritable vision de destinée commune. Ce processus pourrait être mené progressivement, secteur par secteur, en s'appuyant sur les initiatives déjà engagées. Commençons par les secteurs les moins clivants, où la recherche et le développement, les sciences et les technologies semblent consensuelles. L'urgence de cette transformation ne peut être ignorée.

Il est désormais établi que ce sont la recherche et l'innovation qui favorisent la promotion des approches de sécurité par conception ('security by design') et de protection de la vie privée dès la conception ('privacy by design'). Mais cela ne suffit pas, comme nous le verrons un peu plus loin.

Recommandation n° 4 : Préparer et soutenir la représentation française et européenne dans les institutions internationales de normalisation et de gouvernance de l'Internet (UIT, 3GPP, W3C, IETF, IGF)[153]

Certains experts reconnus, tels que Gérôme Billois, associé et directeur de la practice cybersécurité chez Wavestone, que nous avons eu l'opportunité d'interviewer, estiment que l'IdO reflète la même fracture que l'on observe dans l'ensemble du numérique : *les ÉtatsUnis conçoivent le matériel et les services, la Chine et l'Asie les fabriquent, et l'Europe les utilise*[154]. Toutefois, nous pensons que la situation est plus complexe et qu'elle a évolué en faveur de la Chine, au détriment des États-Unis et de l'Europe. Contrairement à ce qui est souvent décrit, l'Europe n'est pas simplement un marché de consommateurs.

En réalité, l'Europe dispose de laboratoires de recherche à la pointe de l'innovation et possède les compétences nécessaires pour jouer un rôle actif au sein des organismes de normalisation internationaux. Comme l'a si bien dit M. Zhang Xiaogang, ancien directeur de l'Organisation internationale de normalisation (ISO) et de l'Association chinoise du fer et de

[153] Union Internationale des Télécommunications, 3rd Generation Partnership Project, World Wide Web Consortium, Internet Engineering Task Force, Internet Governance Forum

[154] Interview de Gérôme Billois - auteur, associé et directeur de la practice cybersécurité chez Wavestone-, 04/07/2024

l'acier (CISA) : *'Celui qui contrôlera la norme, contrôlera la technologie et le marché*.' C'est bien là que réside l'enjeu.
Les Européens devraient s'inspirer de la Chine en redéployant leurs compétences au sein des organismes de normalisation, afin de maintenir et de consolider leurs positions, tout en influençant en faveur des architectures basées sur la 'privacy by design' et la 'security by design'. De plus, à l'instar des Américains et des Chinois, l'Europe devrait privilégier des représentations mixtes (diplomates, scientifiques, parties prenantes) au sein de ces organisations.

Enfin, il est crucial de mettre en place des incitations financières pour encourager les entreprises, les laboratoires de recherche, les organismes de normalisation nationaux européens, ainsi que toutes les parties prenantes compétentes, à proliférer au sein des organismes de normalisation internationaux et à imposer les normes européennes

Recommandation n° 5 : Adoption de certifications, évaluations de la conformité et labels[155]

Il faudra distinguer certification, évaluation de la conformité et labels car les 3 concepts n'ont pas la même signification même s'ils ont le point commun d'être des outils efficaces pour instaurer la confiance, accroître la transparence et promouvoir la concurrence.

L'évaluation de conformité est un dispositif permettant de vérifier et de mesurer le niveau de respect des produits ou des organisations des exigences spécifiques, définies par des directives et des normes techniques. Elle peut être auto-évaluée ou évaluée par un tiers. La certification est un dispositif permettant d'évaluer avec plus de certitude, par le biais d'une tierce évaluation indépendante, l'atteinte par des produits ou des organisations d'un certain niveau de sécurité numérique.

Les avis des experts divergent sur l'interdépendance entre certification et évaluation de conformité, notamment sur le fait que l'une doive s'appuyer sur l'autre pour être crédible. L'évaluation de conformité par certification pourrait être intéressante pour des utilisateurs avertis et familiers avec les concepts normatifs et techniques. En revanche, c'est beaucoup moins impactant pour le grand public qui nécessiterait plutôt des labels avec un étiquetage simple et universel.

Par ailleurs, du côté des fournisseurs et des constructeurs, l'évaluation de conformité et la certification sont associés à des coûts significatifs. Par conséquent, comme nous avons de cesse de le répéter, il faudra trouver le juste équilibre et recourir à ces dispositifs de manière proportionnée au risque. Cette contrainte a été prise en compte par le Cybersecurity Act de l'Union européenne qui consacre le principe de reconnaissance transfrontalière afin que les entreprises n'aient à passer qu'un seul processus pour obtenir une certification valable pour tous les pays membres. Le premier schéma de certification européen a été adopté par la Commission Européenne en janvier 2024 et a été largement abordé dans la partie réglementation et législation de ce mémoire.

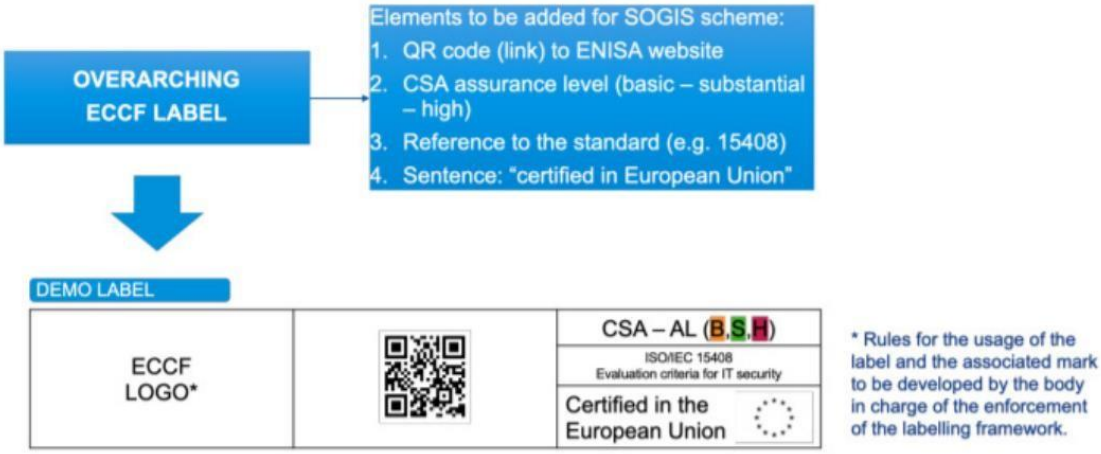
[155] Enhancing the digital security of products_cd9f9ebc-en.pdf, pages 41 à 45.

Pour ce qui est des labels, la principale différence avec les évaluations de conformité réside dans l'accessibilité des informations fournies et sont développés pour accroître la transparence pour les utilisateurs grand public. Ils peuvent être affichés sur l'emballage du produit, sur le site Web du producteur ou sur le smartphone du client après avoir scanné l'identification du produit (code-barres ou code QR). Nous illustrerons par des exemples, un peu plus bas dans le document ainsi qu'en annexe, certains modèles d'étiquetage et les informations qui y sont incluses. Ils peuvent être attribués par des autorités publiques ou des organisations dirigées par l'industrie et inclure ou pas la certification comme critère pour son attribution.

Comme les évaluations de conformité, ils peuvent être volontaires ou obligatoires, et reposer sur une auto-évaluation ou une certification par un tiers. Certains pensent que les labels seront utiles pour aider les consommateurs à choisir entre des produits présentant un niveau raisonnable de sécurité numérique, mais seraient insuffisants pour imposer ce niveau minimum pour tous les produits.

Plusieurs pays ont devancé l'UE en lançant leur propre schéma d'étiquetage pour la sécurité numérique des produits. Il s'agit de la Finlande, l'Allemagne, le Japon, Singapour et la Chine que nous avions évoquée sur la partie stratégie de ce mémoire.

Nous ne savons pas encore ce qui a été retenu par l'**UE** comme label et s'il consisterait uniquement en l'apposition du label CE pour certifier du bon niveau de sécurité numérique d'un produit. Ce qui serait vraiment dommageable car constituerait un label pas très explicite et opaque. En 2020, l'ENISA projetait un label comme celui de la figure ci-dessous, qui devait comprendre un logo facilement reconnaissable, trois niveaux de garantie (de base, substantiel et élevé), des références aux normes pertinentes, ainsi qu'un code QR qui pourrait fournir des informations supplémentaires lors de la numérisation. Il serait normal et pertinent que l'ENISA s'inspire des expériences des pays cités plus haut dans l'élaboration de celui de l'UE.



Note: ECCF stands for European Cybersecurity Certification Framework.
Source: (ENISA, 2020[50]).

Figure 31 : Projet de label de cybersécurité de l'UE

Pour ce qui est de **la Finlande**, en novembre 2019, l'agence finlandaise des transports et des communications (Traficom) a lancé **le premier label de "sécurité de l'information" au monde**, **spécifique aux appareils IdO**. Il sera attribué aux produits IdO répondant à certains critères de certification, basés sur la spécification technique de l'ETSI sur la cybersécurité pour les objets connectés destinés aux consommateurs.

Un site web dédié au label répertorie les produits l'ayant reçu et publié des informations à leur sujet. **Ce qui est intéressant, c'est l'idée de cette liste, qui sert de référence pour identifier les fournisseurs et les produits de confiance**. Le schéma d'étiquetage repose sur plusieurs critères, dont les certifications attribuées au produit ou au fabricant (par exemple, la certification STAR[156] par la Cloud Security Alliance), la période de support, la capacité de mise à jour, la politique de divulgation des vulnérabilités, le chiffrement et la protection de la vie privée.

Figure 32: Label finlandais de sécurité de l'information dédié à l'IdO

Source : https://www.kyberturvallisuuskeskus.fi/en/news/information-security-requirements-smart-devicesare-companies-ready

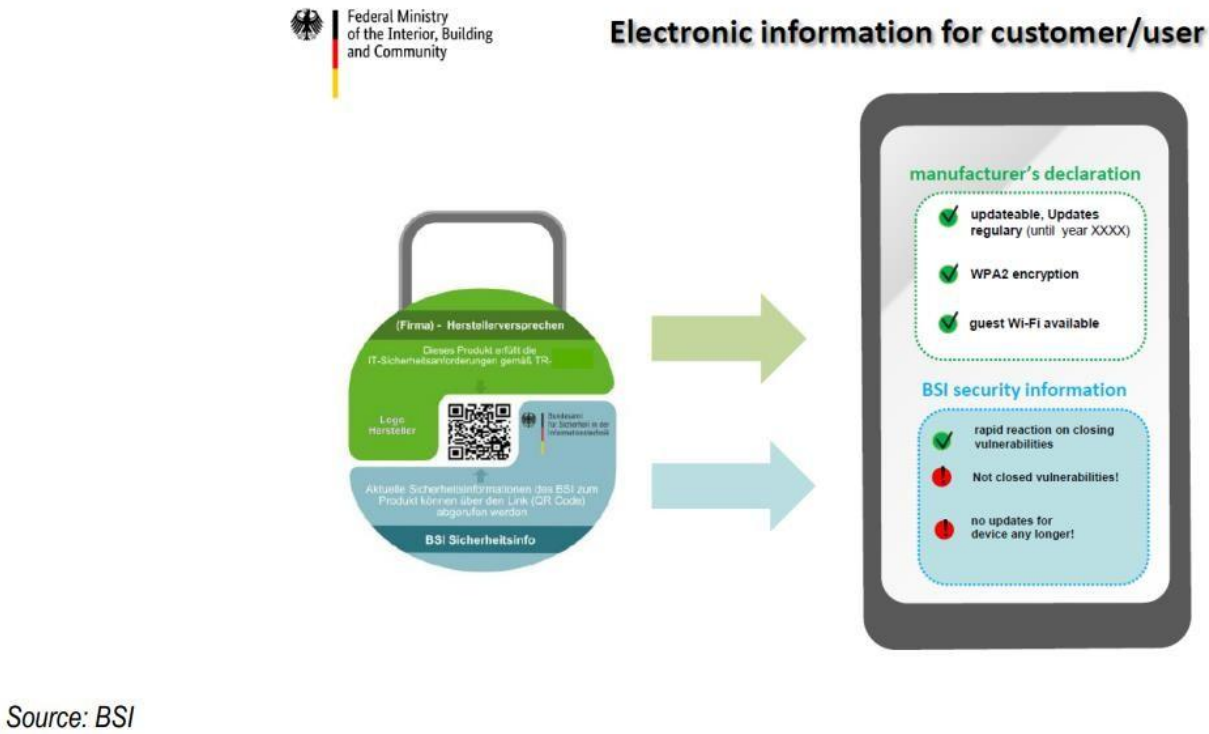
[156] Security, Trust, Assurance, and Risk

Une coopération étroite et solide existe entre les autorités de cybersécurité de Finlande et de **Singapour**, leurs labels sont basés sur la même norme [157] et se reconnaissent mutuellement. Les détails du schéma d'étiquetage de cybersécurité (CLS [158]) pour les consommateurs de Singapour seront fournis en annexe 4. Il en sera de même pour le Japon. On va terminer ce tour d'horizon par l'**Allemagne** dont l'agence en charge de la sécurité numérique (BSI[159]) en partenariat avec l'industrie, a lancé en 2020, un schéma d'étiquetage volontaire, "Sécurité informatique" pour tous les produits informatiques.

Il est venu compléter les dispositifs existants des fabricants de produits qui n'étaient pas standardisés et qui manquaient de clarté, de pertinence et de transparence.

Le label prend la forme d'un code QR présent sur l'emballage du produit dont le scan présente deux ensembles d'informations au client : l'auto-déclaration du fabricant et les informations de sécurité du BSI (Figure ci-dessous) comme les failles de sécurité ou d'autres

informations pertinentes pour la sécurité, tandis que la déclaration du fabricant garantit que le produit possède certaines caractéristiques de sécurité informatique.



Source: BSI

Figure 33 : Projet de label IT en Allemagne

Nous préconisons le recours volontaire aux trois dispositifs avec des incitations proportionnelles au niveau d'engagement et de transparence des parties prenantes (accès

[157] ETSI EN 303 645

[158] Cybersecurity Labelling Scheme

[159] Bundesamt für Sicherheit in der Informationstechnik (office fédéral allemand pour la sécurité de l'information)

privilégié aux marchés publics, exemption de certains risques de responsabilité par les assurances, etc.).

L'obligation pourrait produire l'effet inverse de l'objectif recherché, créant ainsi un problème d'« *insécurité par conformité* » en devenant un obstacle à la mise en œuvre des mises à jour de sécurité.

Recommandation n° 6 : Sensibiliser les citoyens aux risques des objets connectés

Comme l'a indiqué M. Stéphane FERRER, responsable informatique, DPO indépendant et spécialiste RGPD, lors de notre entretien au sujet du RGPD et de l'IdO[160], nous avons la chance en France de disposer d'un organisme tel que la CNIL, qui produit de nombreux supports pour sensibiliser les consommateurs aux risques du numérique en général, et à ceux de l'IdO en particulier, malgré des ressources humaines limitées. Bien que nous partagions cet avis, nous pensons qu'il reste des efforts à fournir pour que la communication atteigne effectivement sa cible.

L'État devrait fournir à la CNIL les moyens nécessaires pour renforcer ses équipes et mener des campagnes de vulgarisation dans les médias de grande audience.

Pour leur sécurité et la protection de leurs données personnelles, il est essentiel d'inciter les citoyens à se poser la question du réel besoin avant d'acheter un objet connecté, et à choisir, le cas échéant, un modèle répondant aux labels de sécurité et de confiance établis et reconnus par les autorités européennes ou nationales.
Pour illustrer notre propos, prenons l'exemple d'une ampoule connectée. En fonction de la technologie de contrôle utilisée, les données peuvent emprunter divers chemins et impliquer différents acteurs. Voir les divers scénarios en annexe 3.

Dans tous les cas, la cible reste l'ampoule et l'ordre est d'allumer cette ampoule. Ce qui diffère, c'est le moyen de contrôle utilisé avec les conséquences évoquées ci-dessus. Ces scénarios mettent en évidence que Google, et dans une moindre mesure, Amazon, sont très largement impliqués. Ce n'est évidemment pas une surprise et cela confirme ce que nous avions développé dans la partie relative à la stratégie des États-Unis pour la captation des données personnelles. Ces géants technologiques déploient tous les moyens pour se positionner à l'intersection de tous ces flux de données.

Cet exemple met également en lumière la menace pour notre souveraineté numérique. Les flux de données ne quittent pas seulement la maison, mais aussi la France, l'Union européenne, pour traverser l'Atlantique. Pour illustrer l'absurdité de la situation, c'est comme si je devais demander l'autorisation à une entreprise privée située outre-Atlantique pour allumer une ampoule alors que je suis à 2 mètres d'elle. C'est pourquoi il est primordial de sensibiliser les citoyens à la portée de leurs choix et à la nécessité d'acheter un objet connecté.

---

[160] Entretien avec M. Stéphane FERRER, responsable informatique, DPO indépendant et spécialiste RGPD, le 23/08/2024

Nous conclurons ce point sur la vulgarisation et la sensibilisation en évoquant à nouveau le modèle finlandais et une mesure plutôt opérationnelle. Nous avons été agréablement surpris de découvrir sur le site de l'agence finlandaise des transports et des communications (Traficom), une météo cyber mensuelle [161]. Celle-ci fournit des informations sur les principaux incidents et évènement de sécurité de l'information du mois. Destinée à ceux qui travaillent sur les questions de sécurité de l'information à différents niveaux au sein des organisations, elle offre un aperçu rapide des événements récents et à venir dans le domaine de la cybersécurité.

Vous pourriez dire qu'il n'y a rien d'exceptionnel à cela et que des rapports équivalents existent dans d'autres pays, notamment en France.
Cependant, cela nous a inspiré l'idée d'une météo cyber destinée au grand public, visant à vulgariser la cybersécurité et à sensibiliser aux risques du numérique en général, et de l'IdO en particulier. Cette météo pourrait être présentée à la fin d'un journal télévisé, comme une météo classique, à une fréquence hebdomadaire ou mensuelle. Après la météo classique et la météo des plages, pourquoi pas la **météo cyber** ?

Recommandation n° 7 : Étendre le périmètre du projet de cyber bouclier européen

Renforcer notre cybersécurité contribue à mieux protéger nos données personnelles et notre vie privée.

La Commission européenne a adopté, le18 avril 2024, le Cyber Solidarity Act, projet de réglementation européenne visant à mutualiser les ressources, les moyens et les compétences cyber des 27 états afin de doter l'Europe d'un cyberbouclier. L'objectif est de *"détecter rapidement et efficacement les cybermenaces majeures"* et d'y répondre de manière solidaire.

Cette infrastructure paneuropéenne sera composée de centres d'opérations de sécurité (SOC) nationaux et transfrontaliers dans l'ensemble de l'UE, dotés des technologies de pointe, telles que l'intelligence artificielle (IA) et l'analyse avancée des données, pour détecter et partager des alertes sur les cybermenaces et les incidents transfrontaliers.
Il est également prévu la création d'un *"mécanisme d'urgence cybernétique"* qui comprendra des actions de préparation et de tests, notamment dans des secteurs hautement critiques (santé, transport, énergie, etc.) afin d'améliorer les capacités de réponse aux incidents dans l'UE. Dans cet esprit de solidarité et de mutualisation, il est également prévu la création d'une réserve de cybersécurité de l'UE composée de prestataires de confiance prêts à intervenir, à la demande d'un État membre ou des institutions, organes et agences de l'Union, en cas d'incident de cybersécurité significatif ou à grande échelle.

Cette réglementation a été envisagée dans un contexte d'augmentation des risques notamment liés au conflit en cours en Ukraine.

[161] En voici un exemple, EN_kybersaa_heinakuu2024.pdf (kyberturvallisuuskeskus.fi)

Nous sommes évidemment ravis de cette initiative et nous lui souhaitons tout le succès qu'elle mérite. Elle s'inscrit parfaitement dans la vision que nous évoquions précédemment, concernant la transformation du marché unique en une communauté d'intérêts beaucoup plus large.

À terme, nous pensons que cette infrastructure devrait viser les mêmes objectifs que le cyber dôme israélien. Autrement dit, elle devrait construire une architecture de cyberdéfense commune et approfondie, couvrant l'ensemble du cyberespace européen et pas seulement les secteurs hautement critiques.

En conclusion et pour clore cette partie, nous sommes pleinement conscients des difficultés et des obstacles liés à la mise en œuvre de certaines recommandations. Néanmoins, ces actions sont essentielles si nous voulons rivaliser avec les États-Unis et la Chine sur la scène mondiale.

Si les Européens continuent à agir en ordre dispersé, ils mettent en péril leur souveraineté et leur indépendance technologiques et numériques, risquant de devenir de simples alliés subordonnés des États-Unis dans leur guerre économique et technologique contre la Chine. Retrouver notre souveraineté, tant individuelle que nationale, exigera certainement des sacrifices. Pour les individus, cela pourrait signifier accepter temporairement une certaine dégradation des usages pratiques de l'IdO au profit d'une meilleure sécurité et d'une protection accrue de la vie privée et des données personnelles. Pour les États, cela impliquera des investissements massifs dans la recherche, le développement, la maintenance et la réglementation, avec une attention particulière à la sécurisation des données de leurs citoyens.

Ces efforts, s'ils sont menés dans le cadre d'une démarche européenne unifiée et coordonnée, auront sans aucun doute des effets considérables et rapides.
Avec l'IdO, demain c'est déjà aujourd'hui et il faut toujours avoir une longueur d'avance pour ne pas être dépassé. C'est déjà aujourd'hui car l'IA, la BlockChain et le calculateur quantique sont déjà là pour apporter plus de défis et de complexité à l'environnement numérique. La protection des données personnelles, au cœur de la souveraineté numérique, doit être au centre de ces avancées technologiques afin de garantir un avenir numérique sûr et respectueux des libertés individuelles.

VII.Conclusion

VII. CONCLUSION

Gerd Leonhard, futurologue et auteur suisse, dans le documentaire « So much about digital »[162], déclarait déjà en 2018 que « Les données sont plus importantes que le pétrole, le gaz ou l'énergie nucléaire. Les données sont plus lucratives. ».

L'enjeu central de ce rapport reste la protection de nos données personnelles. L'IdO constitue un canal supplémentaire de captation massive, notamment pour des fins de contrôle et de surveillance.

Malgré le ralentissement post-crise du Covid, dû à la pénurie de puces électroniques et à l'augmentation des prix dans l'industrie des semi-conducteurs, les projections de croissance à deux chiffres pour le secteur de l'IdO montrent que la tendance va continuer à s'accentuer.

La prolifération de ces objets connectés grand public, souvent vulnérables, ne fera que s'amplifier, augmentant ainsi de manière significative notre surface d'attaque. Ce caractère vulnérable nous a été confirmé par nos diverses recherches et la raison principale semble économique mais pas uniquement. C'est à se demander même si, dans certains cas, ce ne serait pas prémédité. Certains pays n'accordent pas la même attention à la sécurité des objets connectés destinés à l'exportation qu'à ceux destinés à leur marché domestique.

[162] Documentaire réalisé en 2018 par Peppo Wagner et diffusé sur plusieurs plateformes de streaming comme Netflix. Il pose la question de l'impact de la digitalisation massive de notre société.

La prospection de l'environnement réglementaire et législatif encadrant cet écosystème met en évidence l'insuffisance des dispositifs actuels pour adresser les spécificités de l'écosystème IdO et répondre au défi de l'extraterritorialité de certaines législations comme celle des EtatsUnis.

En effet, le monde entier nous envie notre RGPD et s'en inspire mais force est de constater qu'il est insuffisant. Des pays tels que la Chine et Israël ayant adopté des réglementations similaires inspirées du RGPD ont dû les renforcer afin de mieux protéger les données personnelles de leurs citoyens et leur vie privée.

De plus, nous avons la loi sur la cybersécurité de l'UE ainsi que le tout récent Cybersecurity Resilience Act (CRA) qui viennent renforcer cet arsenal juridique. La France et l'Europe sont à l'avant-garde de la réglementation régissant leur cyberespace mais nécessitent d'apporter un focus par sous-système technologique pour traiter les spécificités.

Dans notre modeste contribution, nous avons voulu lever le voile sur l'hypocrisie de ceux qui prétendent être nos alliés et ceux plus connus pour ne pas l'être et qui ont peu de respect pour les données personnelles et la vie privée. Nous nous sommes intéressés à leur stratégie de développement de l'IdO et à leur approche du traitement des données personnelles et la manière dont ils se prémunissent contre les risques liés à cet écosystème.

Nous avons découvert des idéologies d'un nouveau genre, le capitalisme et le communisme de surveillance, qui considèrent nos informations sensibles comme une ressource précieuse et convoitée. Bien qu'aux antipodes, leur objectif est le même : capter massivement cette matière première. Non pas dans le but de nous proposer de meilleurs services mais dans le but d'influencer et de contrôler nos opinions et nos comportements de consommateurs.

Nous avons également voulu exhumer un certain nombre de rapports [163] d'une qualité remarquable afin de remettre en lumière certaines de leurs recommandations en nous en inspirant.

Pour sécuriser l'écosystème de l'IdO et respecter les données personnelles et la vie privée, une combinaison de mesures technologiques, réglementaires et organisationnelles est indispensable. Nos lectures, nos recherches et nos divers échanges avec des experts de qualité du domaine, nous ont inspirés sept recommandations que nous avons jugées importantes et même essentielles afin d'atteindre cet objectif.

Il est essentiel de souligner les défis technologiques, notamment l'intelligence artificielle (IA), dont la maturation contribuera largement à la croissance de l'IdO tout en complexifiant davantage cet écosystème. Même si nous pensons que l'IA et l'IdO vont se nourrir mutuellement et se renforcer.

La création de solutions d'IA simplifiées, l'infusion de l'IA dans les applications historiques et les progrès notables en matière de puces IA participeront, elles aussi, à la croissance de l'intelligence artificielle des objets (AIoT).

Nous allons terminer en revenant au point de départ de cette conclusion en citant les propos de Gerd Leonhard, futurologue et auteur suisse, dans le documentaire « So much about digital

[163] Rapports de France Stratégie, de l'AFNIC ainsi que le livre blanc de l'INRIA dédié à l'IdO.

» concernant le développement technologique, « Il faut qu'on imagine un cadre pour l'utilisation de la technologie, comme pour le nucléaire. Il y a eu 2 bombes, puis on a dit qu'on ne voulait pas avoir 5000 autres bombes, alors on s'est mis d'accord. Il faut faire la même chose pour l'IA, l'ingénierie génétique, l'IdO, la connectivité. On doit dire : ça c'est bien pour l'homme, et ça, ça n'est pas bien. Donc, utiliser ce qui est bien et éviter ou réduire ce qui est mauvais. **C'est à la politique et à la société de le dire** ».

Dans le même reportage, Martina Mara, spécialiste autrichienne de renom en psychorobotique, nous invite à arrêter d'idéaliser la technologie (image de l'humanoïde au chevet de la mamie et du papy) et plutôt la présenter comme une aide, un outil et un complément.

Le législateur, les pouvoirs publics et les scientifiques devront s'assurer que la technologie reste un outil au service de l'humain, et non un instrument d'asservissement au profit d'intérêts lucratifs ou hégémoniques. Il est impératif qu'un cadre éthique rigoureux soit rapidement mis en place afin de garantir un équilibre entre innovation technologique et protection des droits fondamentaux.

VIII.Références bibliographiques

VIII. REFERENCES BIBLIOGRAPHIQUES

Alex Drozhzhin. «Xiaomi Mi Robot vacuum cleaner hacked.» *Kaspersky Daily.* 04 01 2018. https://www.kaspersky.com/blog/xiaomi-mi-robot-hacked/20632/ (accès le 08 2024).

All., IoT For. *"U.S. Cyber Trust Mark: All You Need to Know." IoT For All. .* 5 septembre 2023. https://www.iotforall.com/u-s-cyber-trust-mark-all-you-need-to-know (accès le avril 2024).

Anaïs Cherif. «Face aux Gafa, l'Inde veut reprendre le contrôle de ses données.» *LA TRIBUNE.* 14 08 2018. https://www.latribune.fr/technos-medias/face-aux-gafa-l-inde-veut-reprendre-lecontrole-de-ses-donnees-787696.html (accès le 07 2024).

Analytics, IdO. *« État de l'IdO 2020 : 12 milliards de connexions IdO » .* 21 décembre 2020 . https://www.ido-analytics.com/etat-de-lido-2020-12-milliards-de-connexions-ido/ (accès le mai 2024).

ANSSI. *Recommandations relatives à la sécurité des systèmes d'objets connectés.* Paris, 2021.

Arlane Beky. «La NSA veut exploiter l'Internet des objets, santé incluse.» *Silicon.* 02 03 2021. https://www.silicon.fr/nsa-exploiter-internet-objets-sante-150066.html (accès le 07 2024).

Baccelli, Emmanuel. *Internet des Objets: Défis sociétaux et domaines de recherche scientifique pour l'Internet des Objets (IoT).* Livre Blanc, Paris: INRIA, 10/12/2021.

BITAG. «Recommandations sur la sécurité et la confidentialité de l'Internet des objets (IoT).» 2016.

Bouchareb, Ali. *Développement d'une architecture flexible pour la gestion et la sécurité.* 2023.

Carlos, Barraza. *« 12 avantages et inconvénients de l'Internet des objets » .* 8 septembre 2023. https://barrazacarlos.com/12-avantages-et-inconvenients-de-linternet-des-objets/ (accès le mai 2024).

Caroline Briner. «La Chine veut noter tous ses habitants et installe 600 millions de caméras.» *Radio Télévision Suisse (RTS).* 14 03 2020. https://www.rts.ch/info/monde/11137943-la-chine-veutnoter-tous-ses-habitants-et-installe-600-millions-de-cameras.html (accès le 08 2024).

Cheng, Kenneth. *Hackers stole data of PM Lee and 1.5 million patients in 'major cyberattack' on SingHealth.* 21 07 2018. https://www.todayonline.com/singapore/hackers-stole-data-pm-leeand-15-million-patients-major-cyberattack-singhealth (accès le 09 2024).

Christophe Auffray. «Montres connectées : les parents les boudent, les enfants vont les adorer.» *ZDNET.* 27 06 2018. https://www.zdnet.fr/actualites/montres-connectees-les-parents-lesboudent-les-enfants-vont-les-adorer-39870312.htm (accès le 08 2024).

Commission, European. *"Cyber Resilience Act." Digital Strategy. .* 16 septembre 2023. https://digitalstrategy.ec.europa.eu/fr/policies/cyber-resilience-act. (accès le mai 2024).

Commission., European. *"New EU Cybersecurity Rules Ensure More Secure Hardware and Software Products " Digital Strategy.* 25 août 2023. https://digital-strategy.ec.europa.eu/en/news/neweu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products (accès le avril 2024).

Connectés, Objets. *« Confidentialité et sécurité : les enjeux majeurs des réglementations de l'IdO » .*

25 août 2023 . https://www.objetconnecte.com/confidentialite-securite-enjeuxreglementations-ido/ (accès le mai 2024).

Dennis Giese. *Security analysis of the XIAOMI IoT ecosystem, https://dontvacuum.me/thesis/Security_Analysis_of_the_Xiaomi_IoT_Ecosystem.pdf.* Master Thesis, Technische Universität Darmstadt: Department of Computer Science, Secure Mobile Networking Lab, 2019.

«Diplomatie.gouv.fr.» s.d. https://www.diplomatie.gouv.fr/IMG/pdf/iv.2_feuille_de_route_numerique_fr_2__cle053556.pdf.

Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF). *"Objets connectés." Économie.gouv.fr. .* 30 août 2023 . https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/objetsconnectes. (accès le avril 2024).

Dr. Cédric LÉVY-BENCHETON (ENISA), Ms. Eleni DARRA (ENISA), Mr. Guillaume TÉTU (Trusted labs),Dr. Guillaume DUFAY (Trusted Labs), Dr. Mouhannad ALATTAR (Trusted Labs). *Security and Resilience of Smart Home Environments - Good practices and recommendations .* ENISA, Décembre 2015.

Emily de La Bruyère, Doug Strub et Jonathon Marek. *Ambitions numériques de la Chine : Une stratégie mondiale visant à supplanter l'ordre libéral.* Rapport spécial du NBR n° 97, Seattle, Washington: The National Bureau of Asian Research (NBR), 2022.

E-Space. 2023. "Pourquoi la connectivité par satellite est essentielle pour les appareils de l'internet des objets. . 5 juillet 2023. https://fr.e-space.com/article/why-satellite-connectivity-is-essentialfor-intern (accès le septembre 2024).

Européenne, Commission. *« La prochaine génération de l'Internet des objets | Bâtir l'avenir numérique de l'Europe » .* 1 septembre 2023 . https://europa.eu/next-generation-iot (accès le mai 2024).

FCC., Federal Communications Commission. *Public Safety and Cybersecurity .* 15 septembre 2023. https://docs.fcc.gov/public/attachments/DOC-401201A1.pdf. (accès le avril 2024).

So much about digital. Réalisé par Peppo Wagner. Interprété par Martina Mara Gerd Leonhard. 2018.

Gérôme Billois - -, interviewer par Auteurs de ce mémoire. *Auteur, Associé et directeur de la practice cybersécurité chez Wavestone* (04 07 2024).

Gouv.fr, Cyber Malvaillance. «Sécurité des objets connectés (IoT).» Sensibilisation sécurité IoT, Paris, 2021.

Guido Noto La Diega, Ian Walden. *Contracting for the «'Internet of Things' :Looking into the Nest ».* London: research paper, Queen Mary University of London, School of Law, 2016.

HADDAB, Yassine. *Introduction à l'internet des objets (IoT - IdO).* 2015.

Hemmer, Adrien. *Méthodes de détection pour la sécurité des systèmes IoT hétérogènes.* 2023.

House., The White. *"Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers.".* 18 juillet 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harrisadministration-announces-cybersecurity-labeling-program-for-smart-devices-to-protectamerican-consumers/ (accès le mai 2024).

IdO : Les prédictions pour 2024. 13 septembre 2023 . https://www.objetconnecte.com/IdOpredictions-2024/ (accès le juin 2024).

Inc., Statista. *Assistants vocaux les plus importants en 2020 .* 22 septembre 2020 . https://fr.statista.com/infographie/22400/assistants-vocaux-les-plus-importants-en-2020/ (accès le juin 2024).

Inc.., Statista. *Les objets connectés.* 13 septembre 2023. https://fr.statista.com/themes/2972/lesobjets-connectes/#topicOverview (accès le juin 2024).

«Indian Computer Emergency Response Team.» *WIKIPEDIA .* 18 08 2024. https://en.wikipedia.org/wiki/Indian_Computer_Emergency_Response_Team (accès le 08 2024).

Informatique, Le Monde. *« L'IoT, ce maillon faible dans la cybersécurité bientôt plus réglementée ».* 12 septembre 2023 . https://www.lemondeinformatique.fr/actualites/lire-l-iot-ce-maillon-faibledans-la-cybersecurite-bientot-plus-reglementee-86383.html (accès le mai 2024).

INRA. *Un réseau communautaire et open source pour l'internet des objets.* 2009.

Insights, Polytechnique. *« Objets connectés : 50 milliards d'émetteurs de CO2 » .* 7 septembre 2023 . https://www.polytechnique-insights.com/dossiers/planete/comment-reduire-lempreintecarbone-du-numerique/objets-connectes-50-milliards-demetteurs-de-co2/ (accès le mai 2024).

Jeffrey Roman. *Anthem Breach Tally: 78.8 Million Affected.* 24 02 2015. https://www.bankinfosecurity.com/anthem-update-a-7946 (accès le 09 2024).

Johanna Costigan, Graham Webster. «14th Five-Year Plan for National Informatization.» *DIGICHINA.* 01 2022. https://digichina.stanford.edu/wp-content/uploads/2022/01/DigiChina-14th-FiveYear-Plan-for-National-Informatization.pdf (accès le 07 2024).

John Chen, Emily Walz, Brian Lafferty, Joe McReynolds, Kieran Green,. «China's Internet of Things.» *SOSi Special Programs Division.* 2018. https://www.uscc.gov/sites/default/files/Research/SOSi_China%27s%20Internet%20of%20Things.pdf (accès le 06 2024).

John Lee. «THE CONNECTION OF EVERYTHING : China and the Internet of Things.» *MERICS CHINA MONITOR.* 24 06 2021. https://merics.org/sites/default/files/2023-02/MericsChinaMonitor70InternetOfThings2.pdf (https://merics.org/en/report/connectioneverything-china-and-internet-things) (accès le 08 2024).

Jonathan A. Obar et Anne Oeldorf-Hirsch. «TPRC 44 : The 44th research conference on Communication, Information and Internet Poilicy, VA : Social REsearch Network, .» *« The biggest Lie on the internet : Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services », in Facebook/Social Media 2.* Arlington,: TPRC 44, 2016.

Katja Drinhausen. *China's Social Credit System in 2021: From fragmentation towards integration; MERICS.* 09 05 2022. https://merics.org/en/report/chinas-social-credit-system-2021fragmentation-towards-integration (accès le 08 2024).

Kirchner, sous la direction scientifique de Claude. *le monde de l'internet des objets : des dynamiques à maîtriser.* Paris: France Stratégie, février 2022.

La traçabilité des produits et la technologie RFID chez DECATHLON. s.d.

https://engagements.decathlon.fr/la-tracabilite-des-produits-et-la-technologie-rfid-chezdecathlon (accès le Juin 2024).

«Le Marché des Objets connectés, Smart Home, Robotique en Inde.» *Business France.* 14 06 2024. https://www.teamfrance-export.fr/fiche-marche/tech/objets-connectes-smart-homerobotique/IN (accès le 07 2024).

Légifrance. *« Section 1 : De l'atteinte à la vie privée (Articles 226-1 à 226-7) » .* 1 janvier 2023. https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006140050/ (accès le mai 2024).

M. Stéphane FERRER, interviewer par Auteurs de ce mémoire. *Responsable informatique, DPO indépendant et spécialiste RGPD* (23 08 2024).

Marie Turcan. «Monsieur Cuisine Connect : micro caché, Android non sécurisé… les dessous du robot cuiseur de Lidl.» *Numerama.* 13 06 2019. https://www.numerama.com/tech/525214monsieur-cuisine-connect-micro-cache-android-non-securise-les-dessous-du-robot-cuisinede-lidl.html (accès le 08 2024).

Mary Duan, Shazeda Ahmed,. *HAI Stanford University Human-Centered Artificial Intelligence; .* 31 08 2020. https://hai.stanford.edu/news/hai-fellow-shazeda-ahmed-understanding-chinas-socialcredit-system (accès le 08 2024).

MédiasDSCI. *Nasscom Community; Technologie IoT en Inde.* 10 11 2020. https://community-nasscomin.translate.goog/communities/emerging-tech/iot-ai/iot-technology-inindia.html?_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=rq#:~:text=The%20introduction%20of%20IoT%20in,program%20launched%20by%20the%20Government (accès le 08 2024).

Merabet, Fatma. *Solutions de sécurité pour l'internet des objets dans le cadre de l'assistance.* 2021.

Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique. *"Marchés des objets connectés à destination du grand public." Entreprises.gouv.fr. .* 25 août 2023. . https://www.entreprises.gouv.fr/fr/presse/etude (accès le avril 2024).

Newswire, PR. *La Convention mondiale de l'Internet des objets 2023 .* 15 septembre 2023. https://www.prnewswire.com/news-releases/la-convention-mondiale-de-lint (accès le mai 2024).

OECD. *Enhancing the digital security of nproducts - A POLICY DISCUSSION.* OECD DIGITAL ECONOMY PAPERS, No. 306, OECD Publishing, Février 2021.

Parisien, Le. *« Tout comprendre à l'affaire Snowden » .* 6 septembre 2023 . https://www.leparisien.fr/international/tout-comprendre-a-laffaire-snowden-06-09-2023 (accès le 2024 mai, 2024).

recherche), DTU (base de données de. *« Modèles économiques des botnets, tentatives de démantèlement et marché du darkweb : une enquête » .* 10 octobre 2023 . https://www.dtu.dk/research/research-databases/botnet-economics/ (accès le mai 2024).

«Réglementation des données – Inde.» *DS Avocats.* 08 02 2024. https://www.dsavocats.com/reglementation-des-donneesinde/#:~:text=Le%20RGPD%20et%20le%20DPDPA&text=Il%20a%20une%20port%C3%A9e%2 0nationale,droit%20%C3%A0%20la%20vie%20priv%C3%A9e. (accès le 08 2024).

Rémi Lou. «Attention à votre robot-aspirateur, il pourrait vous espionner !» *Journal Du Geek (JDG).* 24 11 2020. https://www.journaldugeek.com/2020/11/24/attention-robot-aspirateurespionner/ (accès le 08 2024).

ROCA, Vincent. «Cas d'étude : analyse d'une ampoule connectée...» *MOOC "Protection de la vie privée dans le monde numérique' / Module 5 : Internet des objets et vie privée.* Paris: INRIA, 03 12 2020.

Rogier Creemers et Paul triolo, DIGICHINA. *Analyzing China's 2021–2025 Informatization Plan: A DigiChina Forum.* 24 01 2022. https://digichina.stanford.edu/work/analyzing-chinas-20212025-informatization-plan-a-digichina-forum/ (accès le 07 2024).

Ryan Chan. *MOKO TECHNOLOGY; Haut 10 Fabricants d'électronique en Inde.* 07 03 2023. https://www.mokotechnology.com/fr/electronics-manufacturers-in-india/ (accès le 07 2024).

Shana Lynch. «Former NSA Head Michael Hayden: The Agency "Cannot Survive Without Being More Transparent".» *Graduate School of Stanford Business.* 07 11 2014. https://www.gsb.stanford.edu/insights/former-nsa-head-michael-hayden-agency-cannotsurvive-without-being-more-transparent (accès le 07 2024).

Shazeda Ahmed. *The Messy Truth About Social Credit; Logic's.* 01 05 2019. https://logicmag.io/china/the-messy-truth-about-social-credit/ (accès le 08 2024).

Shazeda Ahmed, Xinru Ma, Julien de Troullioud de Lanversin. *Demystifying China.* 16 04 2020. https://fsi.stanford.edu/events/demystifying-china (accès le 08 2024).

Shoshana ZUBOFF. *L'âge du capitalisme de surveillance.* Zulma Essais, 2022.

SINGAPORE, CSA. *CSA SINGAPORE.* 2024. https://www.csa.gov.sg/our-programmes/certification-andlabelling-schemes/cybersecurity-labelling-scheme/for-consumers (accès le 08 2024).

Team France Export . 00 00 2023. https://www.teamfrance-export.fr/fiche-marche/tech/objetsconnectes-smart-home-robotique/IN.

The White, House. *Technologies for American Innovation and National Security.* 07 02 2022. https://www.whitehouse.gov/ostp/news-updates/2022/02/07/technologies-for-americaninnovation-and-national-security/ (accès le 07 2024).

TRAFICOM. «La sécurité de l'information maintenant !» *TRAFICOM.* 07 2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/EN_kybersaa_heinakuu 2024.pdf (accès le 08 2024).

UIT, PRIDA. *Les fondamentaux de l'IoT.* TUNIS, 2020.

Vidéo de sensibilisation CNIL. «La montre connectée pour enfants : quels enjeux pour leur vie privée ?» *CNIL.* 2023. https://video.cnil.fr/w/iZaAZAxGHUApbJLCSV97pN (accès le 08 2024).

Vignau, Benjamin. «La sécurité dans l'internet des objets: des configurations par défaut aux dénis.» 2022.

Wikipedia. *« Courtier en données » .* 5 septembre 2023 . https://fr.wikipedia.org/wiki/Courtier_en_donn%C3%A9es (accès le mai 2024).

Yahia, Youcef Ould. *Proposition d'un modèle de sécurité pour la protection de données personnelles dans les systèmes basés sur l'internet des objets.* Thèse de doctorat, Paris: Conservatoire national des arts et métiers (CNAM), 2019.

ZDN. *Quel réseau demain pour les objets connectés ? .* 19 janvier 2023. https://www.zdnet.fr/blogs/green-si/quel-reseau-demain-pour-les-objets-connectes39964316.htm (accès le mai 2024).

IX.Annexes

IX. ANNEXES

IX.1 Annexe 1 : Cas réels de cyberattaques et violations de la vie privée

Logiciel malveillant Mirai

Contexte	Le logiciel malveillant Mirai est apparu pour la première fois en 2016. Il visait principalement les appareils de l'Internet des objets (IdO) tels que les caméras de surveillance et les routeurs domestiques. Mirai transforme ces appareils en bots contrôlés à distance pour former un botnet, utilisé pour mener des attaques par déni de service distribué (DDoS).
Mécanisme de l'attaque	Mirai fonctionne en scannant en permanence Internet à la recherche d'appareils IdO vulnérables. Il exploite les identifiants et mots de passe par défaut de ces appareils pour s'y connecter. Une fois connecté, il installe le logiciel malveillant, transformant l'appareil en un "zombie" contrôlé à distance. Ces appareils continuent de fonctionner normalement, mais ils peuvent subir des ralentissements de la bande passante.
Répercussions et préoccupations	Les répercussions de Mirai sont importantes pour les appareils IdO grand public. Utilisé dans certaines des plus grandes attaques DDoS jamais enregistrées, Mirai a notamment ciblé le fournisseur DNS Dyn, perturbant l'accès à des sites web majeurs comme GitHub, Twitter, et Netflix. Les préoccupations majeures incluent la sécurité des appareils IdO souvent mal protégés et la capacité des botnets à mener des attaques à grande échelle, paralysant des portions importantes d'Internet. La publication du code source de Mirai a permis à d'autres cybercriminels de créer des variantes, augmentant ainsi les risques de nouvelles attaques.

Cas des Smart TV de Vizio[164]

Contexte	Vizio, un fabricant de télévisions connectées (Smart TV), a été impliqué dans un scandale en 2017, accusé de collecter des données sur les habitudes de visionnage de ses utilisateurs sans leur consentement.
Mécanisme de la collecte des données	Vizio avait intégré un logiciel de surveillance dans ses télévisions connectées, capable de suivre en détail les habitudes des utilisateurs grâce à la technologie de reconnaissance automatique de contenu (ACR). Ce logiciel collectait des données précises sur les programmes, chaînes, horaires de visionnage, et même sur les appareils connectés. Ces informations étaient ensuite vendues à des tiers, comme des annonceurs, pour un ciblage publicitaire plus précis. Cependant, Vizio n'avait pas informé correctement les utilisateurs ni obtenu leur consentement explicite, et les options de désactivation étaient difficiles à trouver.
Répercussions et préoccupations	En 2017, la Federal Trade Commission (FTC) des États-Unis et le procureur général du New Jersey ont poursuivi Vizio pour pratiques commerciales trompeuses et violation de la vie privée des consommateurs. Vizio a accepté de payer une amende de 2,2 millions de dollars, de supprimer les données collectées sans consentement, et de modifier ses pratiques pour assurer une meilleure transparence à l'avenir. Ce scandale a sensibilisé le public et les régulateurs aux risques liés à la collecte de données par les objets connectés.

Cas des poupées Cayla et i-Que[165]

[164] https://www.usine-digitale.fr/article/vizio-condamne-pour-avoir-espionne-11-millions-d-acheteurs-de-ses-smart-tv.N498214
[165] https://www.radiofrance.fr/franceinter/cayla-et-i-que-les-jouets-qui-peuvent-toujours-espionner-vos-enfants-7271165

Contexte	Les jouets intelligents comme la poupée Cayla et le robot i-Que sont conçus pour interagir avec les enfants via des applications connectées. Ces jouets peuvent répondre à des questions, raconter des histoires et jouer à des jeux en utilisant des technologies de reconnaissance vocale et de connexion à Internet.
Mécanisme de la collecte des données	Les jouets Cayla et i-Que sont dotés de microphones qui enregistrent les conversations des enfants, avec les enregistrements envoyés à des serveurs tiers pour analyse et réponse via une application connectée. Ces jouets peuvent collecter des informations personnelles, telles que les noms, goûts et préférences des enfants, ainsi que d'autres données sensibles. Les données sont traitées et stockées par Nuance Communications, une entreprise spécialisée dans la reconnaissance vocale, et il a été révélé qu'elles pouvaient être utilisées à des fins commerciales.
Répercussions et préoccupations	Les jouets intelligents comme Cayla et i-Que sont capables d'enregistrer des conversations privées et collecter des informations personnelles sans un consentement adéquat. De plus, des chercheurs en sécurité ont révélé que ces jouets permettent de communiquer avec les enfants via le jouet, créant ainsi des risques importants. En 2017, des organisations telles que l'Electronic Privacy Information Center (EPIC) et le Center for Digital Democracy (CDD) ont porté plainte auprès de la Federal Trade Commission (FTC) contre Genesis Toys et Nuance Communications pour violation des lois sur la protection de la vie privée des enfants. En Allemagne, la vente de cette poupée a été interdite.

Cas de Strava [166]

Contexte	Strava est une application de fitness qui permet aux utilisateurs de suivre et partager leurs activités physiques. En 2018, il a été découvert que sa révélait des informations sensibles sur les emplacements de bases militaires et les mouvements de troupes, mettant en lumière des risques de sécurité liés à la divulgation publique de données.
Mécanisme de la collecte des données	Les montres connectées et appareils de fitness utilisés par les militaires enregistraient des données GPS de leurs déplacements et entraînements, synchronisées avec l'application Strava. Strava publiait une carte thermique mondiale montrant les zones de haute activité sous forme de tracés lumineux. Des chercheurs ont utilisé cette carte pour identifier des bases militaires secrètes et des itinéraires de patrouille, en raison des tracés distincts correspondant aux mouvements réguliers des militaires.
Répercussions et préoccupations	La divulgation des emplacements et itinéraires des bases militaires par Strava a mis en danger les opérations militaires et la sécurité des soldats, en permettant aux groupes hostiles de planifier des attaques. En réponse, plusieurs gouvernements, dont le Pentagone, ont émis des directives pour restreindre l'utilisation des dispositifs de fitness et des applications de géolocalisation par le personnel militaire, et ont limité la collecte et le partage de données dans les zones sensibles. Strava a révisé ses politiques de confidentialité, renforcé ses paramètres de sécurité, et fourni des guides pour aider les utilisateurs à protéger leurs informations personnelles.

IX.2 Annexe 2 : Sélection de partenariats sino-européens dans le domaine de l'IdO (Traduit De L'anglais) [167]

Institutions partenaires	Domaine de collaboration
Société allemande pour la coopération internationale Giz) – Académie chinoise des technologies de l'information et de la communication (CAICT)	Coopération sino-allemande sur l'Industrie 4.0 : renforcer la coopération industrielle dans fabrication intelligente
SAP – Huawei	Partenariat cloud
SAP – Nanjing	- Utilisation de SAP IoT pour analyser le mouvement des modèles de trafic en temps réel -

[166] https://www.radiofrance.fr/franceinter/podcasts/sous-les-radars/le-bruit-du-monde-sous-les-radars-du-mercredi-22juin-2022-4502231

[167] MericsChinaMonitor70InternetOfThings2.pdf, page 6

- Dassault Systèmes – Huawei	- Plateforme 3DEXPERIENCE de Dassault Systèmes fournie via Huawei Cloud
- Siemens – Alibaba	- Le système d'exploitation MindSphere de Siemens fourni via Alibaba Cloud
- Bosch – Huawei	- Services Bosch IoT Suite fournis via - Huawei-Cloud
- Ministère de la Science et de la Technologie de Chine – - Fonds d'innovation Danemark	- Collaboration en recherche et innovation sur - Développement durable urbain (IA & IoT désignés comme priorité)
- Irootech – Putzmeister, de société réassurance munichoise, - Connexion Télénor	- La plateforme RootCloud IIOT d'Irotech fournie sur les marchés européen
- Lenovo – Schneider Electric	- Des solutions de fabrication durables et intelligentes pour le secteur manufacturier chinois
- ABB – Huawei	- Solutions numériques ABB Ability fournies via - Huawei-Cloud
- 1NCE – China Telecom	- Partenariat pour le lancement commercial de la carte SIM itinérante NBIoT de China Telecom -

IX.3 Annexe 3 : Impact du dispositif de contrôle sur la destination des données (Divers chemins et différents acteurs).

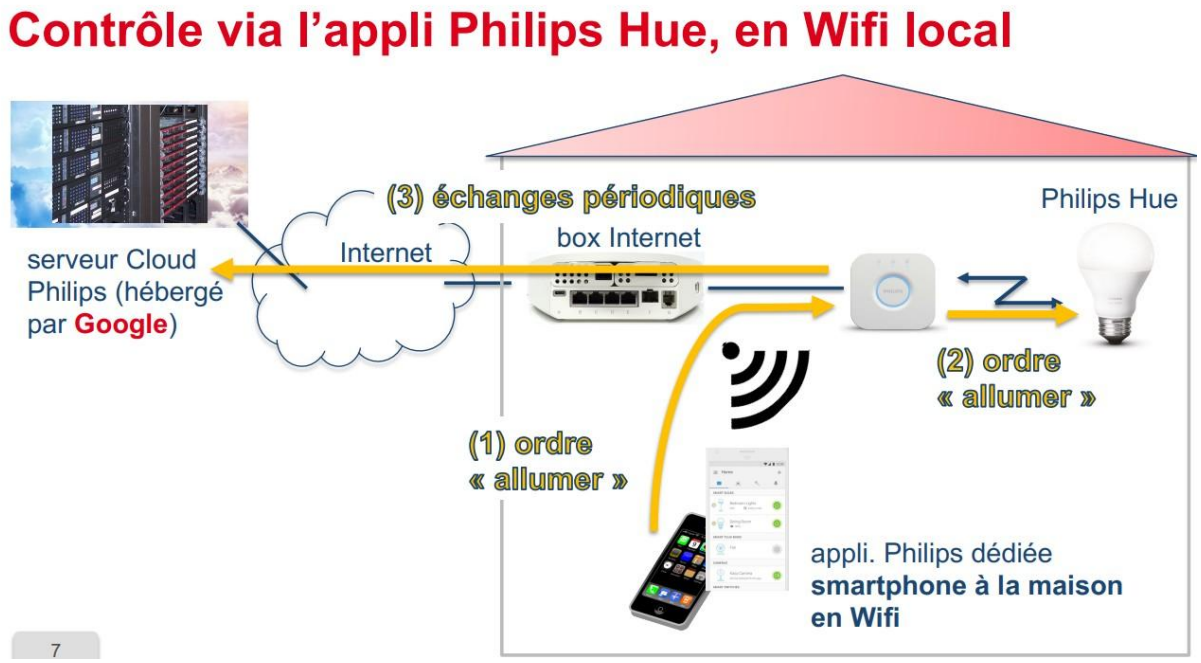


Fig. 1 – Ampoule connectée commandée via l'application Philips Hue avec un smartphone en wifi local

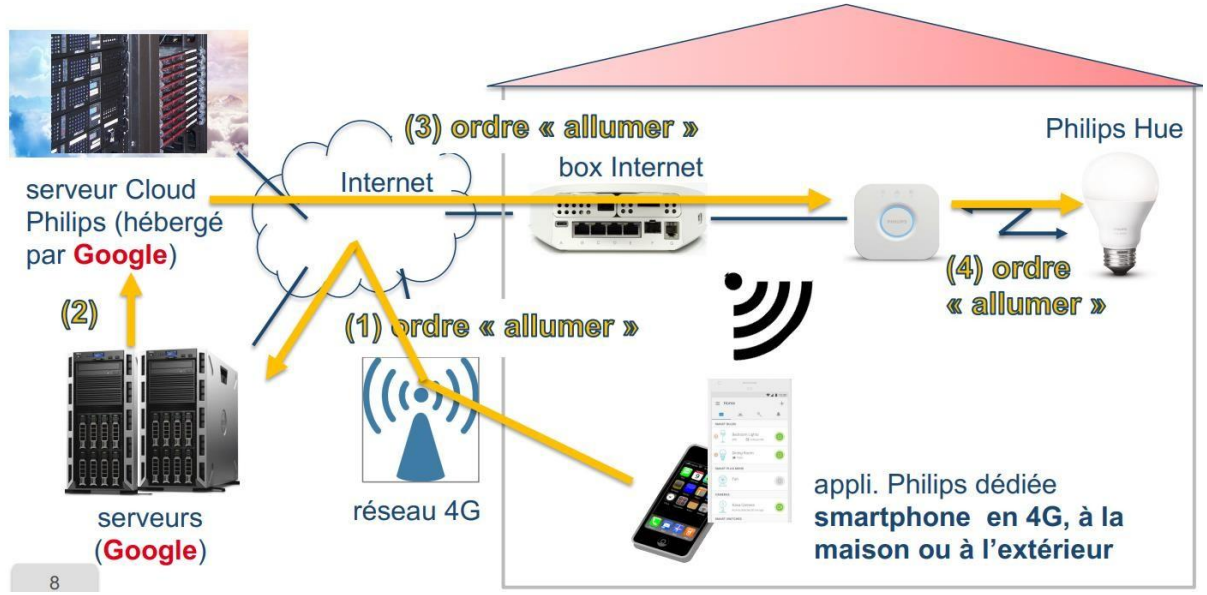


Fig. 2 – Ampoule connectée commandée via l'application Philips Hue avec un smartphone en 4G

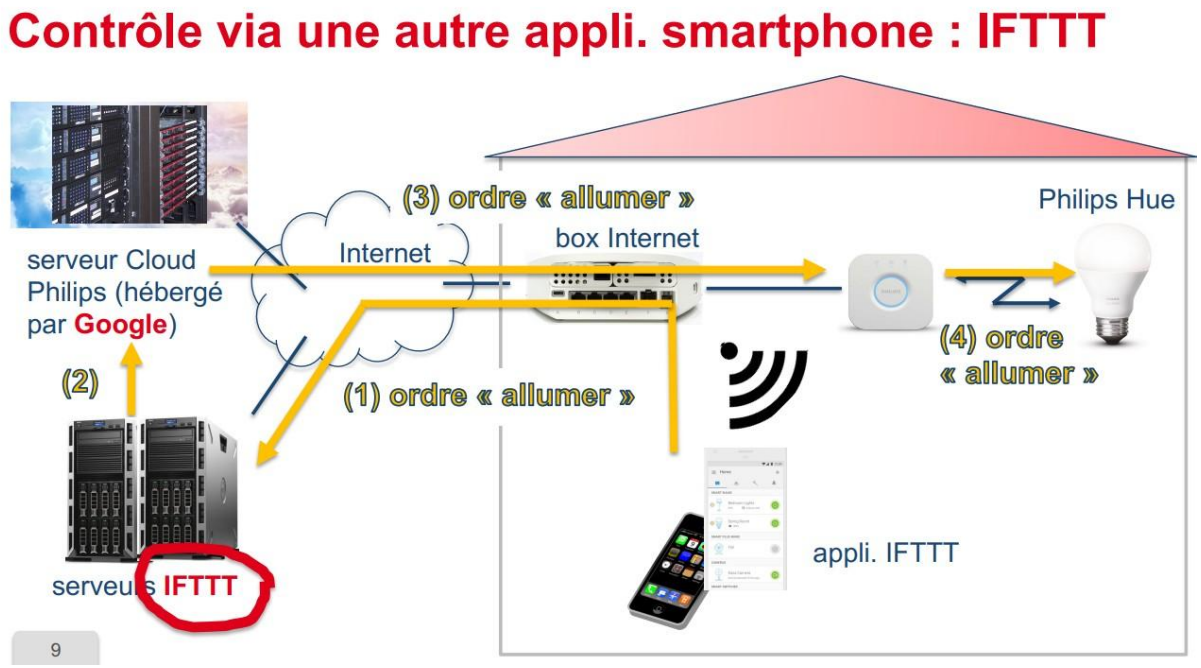


Fig. 3 – Ampoule connectée commandée via l'application IFTTT avec un smartphone en wifi local

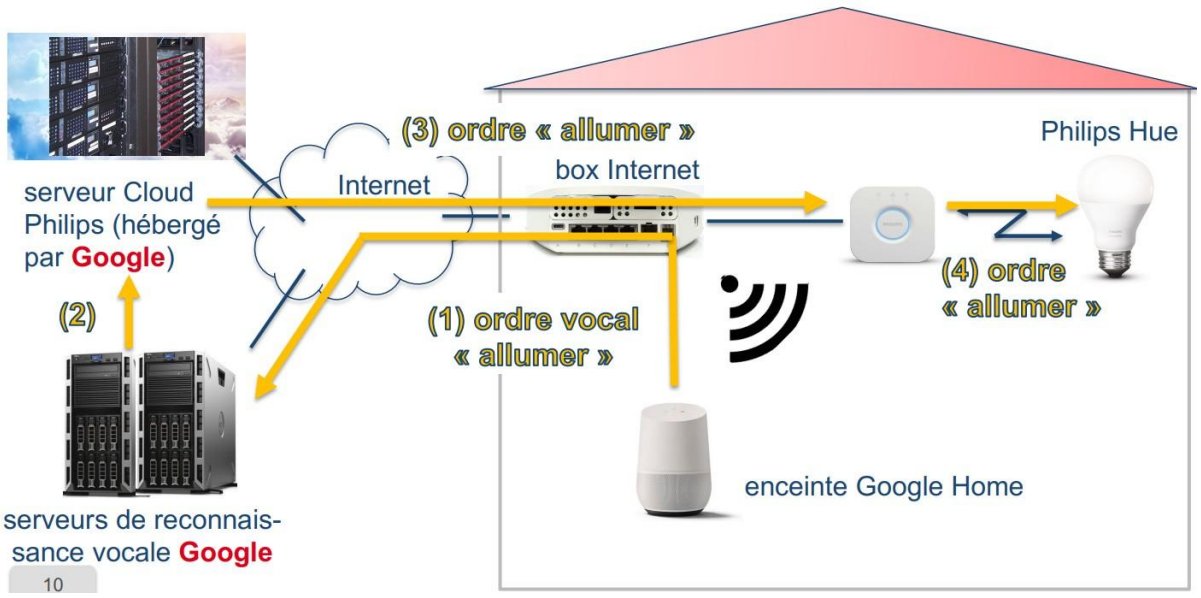


Fig. 4 – Ampoule connectée commandée via enceinte Google Home en wifi local

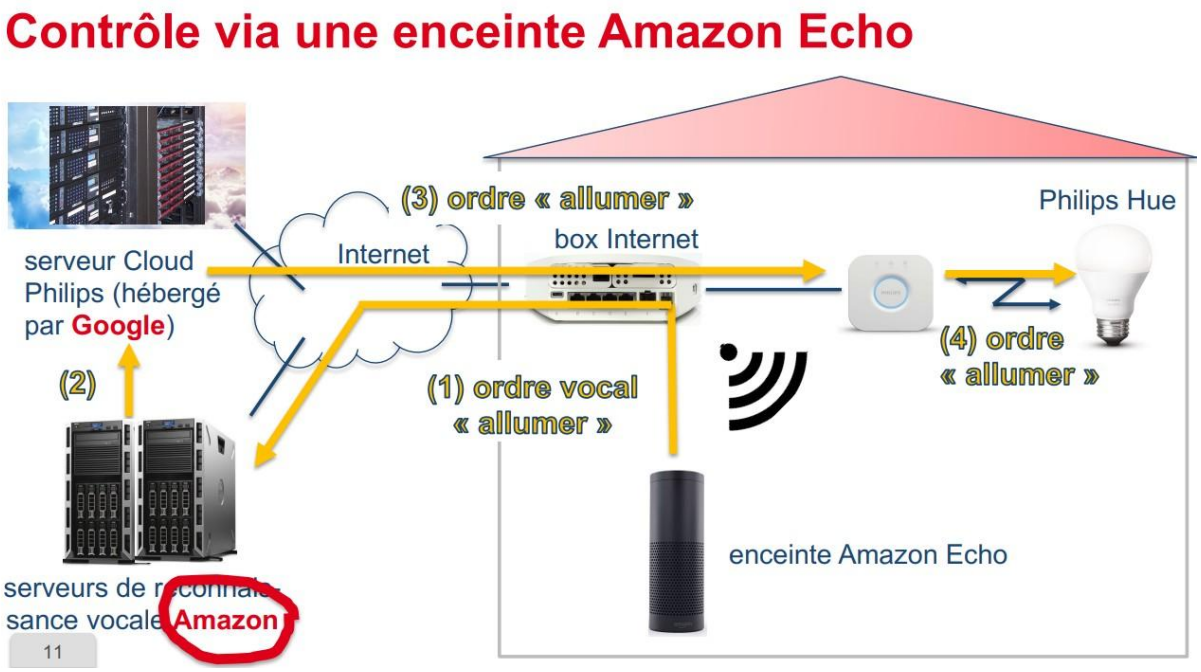


Fig. 5 – Ampoule connectée commandée via enceinte Amazon Echo en wifi local

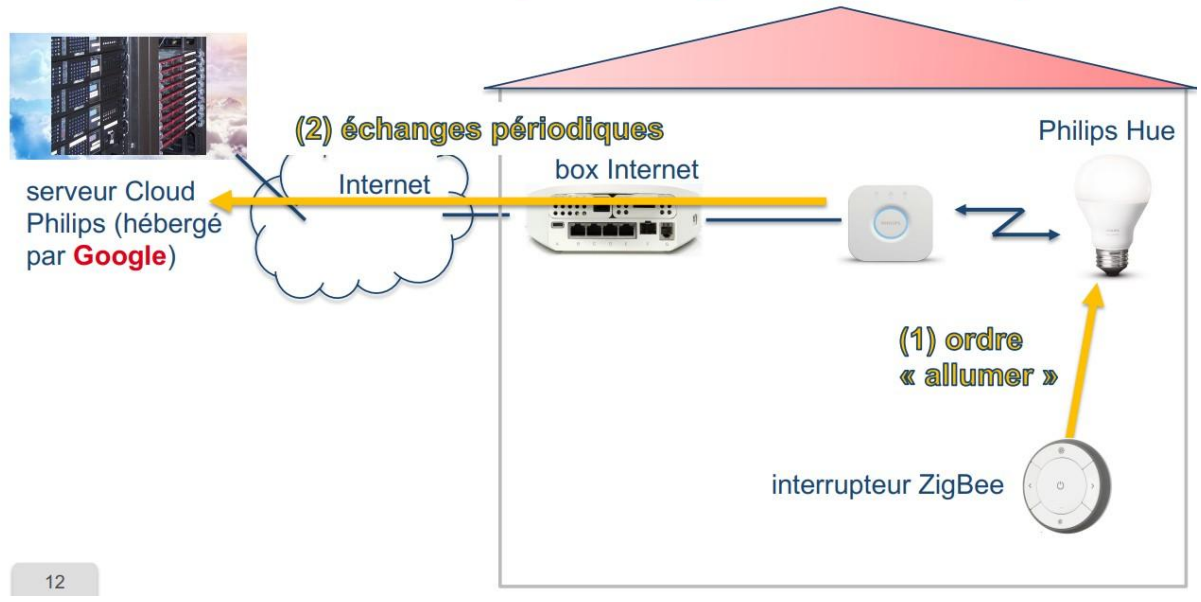


Fig. 6 – Ampoule connectée commandée via interrupteur IKEA en ZigBee

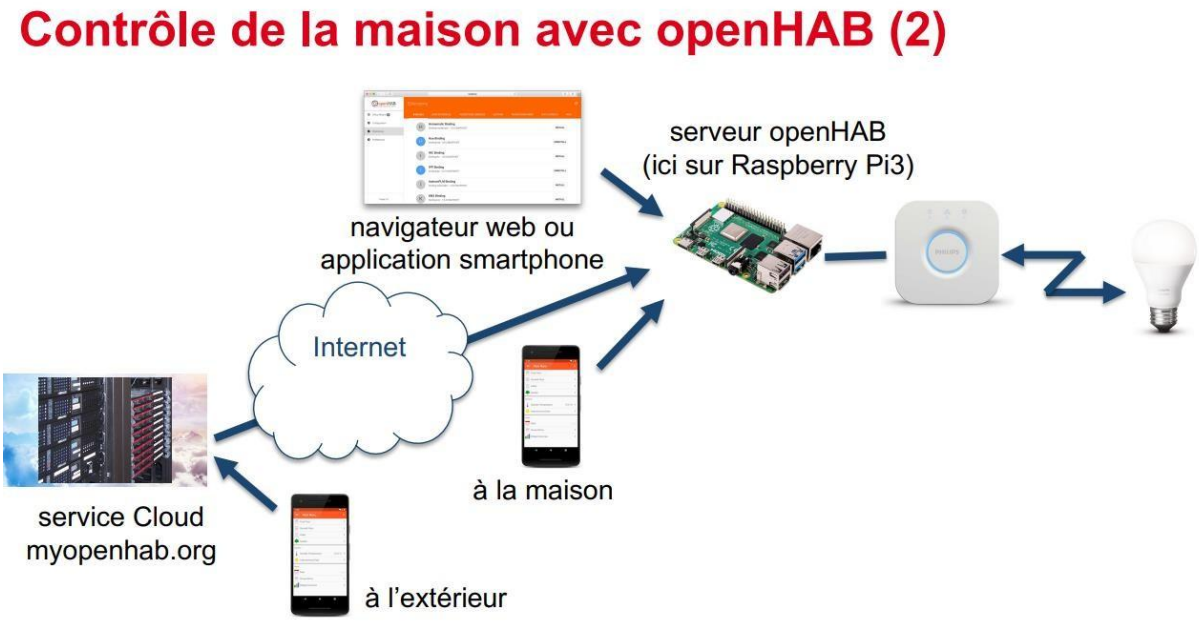


Fig. 7 – Alternative : openHAB, une initiative open-source et libre, est un outil qui fédère tous les objets connectés de la maison, quel que soit le fabricant. Par défaut, il offre un contrôle purement local centré autour d'un mini-serveur local exécutant le logiciel openHAB. En option, un contrôle à distance est possible via le cloud myopenhab.org, hébergé en Europe.

Des outils de contrôle open-source et libres : openHAB, Home Assistant pour un contrôle local de la maison.

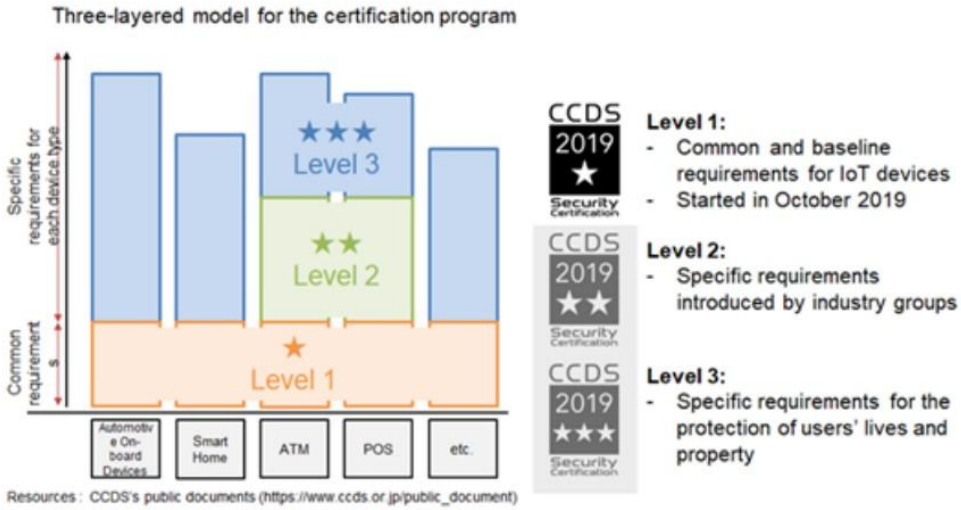
IX.4 Annexe 4 : Exemples de labels de confiance IdO – Japon et Singapour.

JAPON[168]

Au Japon, le Conseil de sécurité des dispositifs connectés pour les consommateurs (Connected Consumer Device Security Council, CCDS), une association professionnelle visant à améliorer la sécurité des dispositifs destinés aux consommateurs, y compris les appareils IdO, a lancé un programme d'étiquetage volontaire pour ce type d'appareils en

[168] Enhancing the digital security of products_cd9f9ebc-en.pdf, pages 41 à 45

octobre 2019. Cette certification repose sur un modèle à trois niveaux, en fonction du degré des mesures de sécurité implémentées, comme illustré dans la figure ci-dessous.



Note: Levels 2 and 3 have been launched in October 2020.
Source: Japanese government, MIC.

Figure 1 : Schéma d'étiquetage du Japon pour les produits IdO

La certification de niveau 1 est basée sur les exigences réglementaires minimales pour la sécurité des IdO, à savoir une fonction de contrôle d'accès ; une fonctionnalité incitant les utilisateurs à changer les identifiants/mots de passe par défaut ; une fonctionnalité de mise à jour du firmware pour les futures corrections de sécurité.
La certification de niveau 2 sera développée dans des secteurs spécifiques (par exemple, la banque, l'industrie), tandis que la certification de niveau 3 sera développée pour la sécurité des produits nécessitant une sécurité renforcée, couvrant à la fois des aspects techniques et des considérations critiques pour la sécurité des utilisateurs.

SINGAPOUR [169] :

Pour compléter ce qui avait été évoqué dans la recommandation 5, schéma d'étiquetage de cybersécurité (CLS [170]) pour les consommateurs de Singapour se base sur 4 niveaux de certifications symbolisés par le nombre d'étoiles tel qu'illustré par la figure ci-dessous. Le détail des exigences de chaque niveau est explicité dans le tableau plus bas.

Figure 2. Schéma d'étiquetage de Singapour pour les produits IdO

[169] Pour les consommateurs (csa.gov.sg)
[170] Cybersecurity Labelling Scheme

Tableau des niveaux et exigences du schéma d'étiquetage - Singapour

Niveau	Exigences
Niveau 1	Le produit a satisfait aux exigences de sécurité de base, telles que la garantie de mots de passe par défaut uniques et la fourniture de mises à jour logicielles.
Niveau 2	Le produit a satisfait à toutes les exigences de sécurité obligatoires des normes internationales et a satisfait aux exigences de niveau 1.
Niveau 3	Le produit a été développé selon les principes de la sécurité dès la conception, a fait l'objet d'une évaluation des binaires logiciels par des laboratoires de test tiers approuvés et a satisfait aux exigences de niveau 2.
Niveau 4	Le produit a subi des tests d'intrusion structurés par des laboratoires de test tiers agréés et a satisfait aux exigences de niveau 3.