FRANCE STRATÉGIE
ÉVALUER. ANTICIPER. DÉBATTRE. PROPOSER.

RAPPORT

FÉV.
2022

Le monde de l'Internet des objets : des dynamiques à maîtriser

LE MONDE DE L'INTERNET DES OBJETS : DES DYNAMIQUES À MAÎTRISER

Sous la direction scientifique de

Claude Kirchner

Directeur du Comité national pilote d'éthique du numérique
et directeur de recherche émérite d'Inria

Rapporteurs

Anne Faure

Mohamed Harfi

Antoine Naboulet

Éva Tranier

FRANCE STRATÉGIE

FÉVRIER 2022

AVANT-PROPOS

Déjà largement présent dans notre vie quotidienne et pourtant encore difficile à appréhender, l'Internet des objets (l'IdO) implique une évolution profonde de l'Internet que nous connaissons. Il ne s'agit plus de relier des tablettes, des ordinateurs, des téléphones entre eux, mais de rendre communiquant tout élément du monde physique, abolissant en quelque sorte les frontières entre objets physiques et monde virtuel. C'est le caractère à la fois émergent, avec une croissance très rapide, et multidimensionnel de l'IdO – diversité des objets concernés, des cas d'application possibles, des technologies associées – qui rend difficile la compréhension des transformations sociales et des impacts environnementaux que provoque le développement massif de l'IdO.

La lettre de mission adressée par la ministre de la Transition écologique[1], Mme Barbara Pompili et le secrétaire d'État au numérique M. Cédric O nous a fixé pour objectifs d'apporter des clés de compréhension et d'analyse sur les technologies de l'Internet des objets, et d'en évaluer les principaux impacts sur l'environnement et sur la vie quotidienne des Français, tant par leur impact social sur le développement des usages que sur les questions qu'elles soulèvent notamment en matière de protection de la vie privée.

Les travaux présentés ci-après soulignent d'abord l'extrême difficulté à cerner un sujet aussi vaste et aussi complexe, pour un objet dont il n'existe aujourd'hui aucune définition arrêtée, aucun outil statistique de mesure, ni cadre juridique déterminé.

C'est pourquoi il était nécessaire que France Stratégie s'appuie sur un large spectre de compétences extérieures, en réunissant un comité *ad hoc* de quatorze experts issus du monde académique, mais aussi de représentants de la société civile, du monde politique ou de membres d'institutions spécialisées[2]. Je tiens à remercier particulièrement les nombreuses contributions de chacun des membres du comité, qui s'est réuni chaque semaine pour des réunions de travail, pendant quatre mois.

[1] Voir annexe 1.

[2] Voir annexe 2.

Le travail du comité n'aurait pas été possible sans l'implication diligente de M. Claude Kirchner, directeur du Comité national pilote d'éthique du numérique et directeur de recherche émérite d'Inria, qui a présidé le comité et animé ses travaux en assurant avec rigueur le pilotage scientifique de la mission. Je l'en remercie vivement.

Ce rapport est aussi le fruit d'une trentaine d'auditions[1] qui se sont tenues entre la mi-septembre et la mi-décembre 2021. Je remercie les intervenants pour leur disponibilité et la qualité de leurs interventions.

France Stratégie a également bénéficié de l'appui des cabinets Boston Consulting Group (BCG) et Ernst & Young-Parthenon (EY-Parthenon), dans le cadre d'une prestation financée par la Direction générale des entreprises du ministère de l'Économie, des Finances et de la Relance (Service Économie numérique) et des contributions du réseau des services économiques (Direction générale du Trésor).

Les travaux du cabinet BCG/EY-Parthenon nous ont permis notamment d'approfondir notre approche des cas d'usage et de compléter notre analyse du cadre juridique du déploiement de l'IdO, dans une perspective internationale.

La Direction générale du Trésor a conduit une enquête comparative auprès de huit pays, Inde, Israël, Chine, Chili, Japon, Nigéria, Finlande et Estonie. Ces derniers ont été sélectionnés avec le comité d'experts sur la base de critères[2] tenant compte de la maturité technologique et numérique du pays, de ses caractéristiques socioéconomiques et de la nature du cadre institutionnel et politique, afin d'appréhender les différentes approches pour encadrer ces technologies. Ce travail nous a permis d'illustrer notre réflexion par un éclairage international original.

Ce rapport présente une première analyse des enjeux déjà présents et à venir mais il dit aussi l'hétérogénéité des connaissances et des données disponibles, ce qui s'agissant d'un domaine aussi vaste n'est pas surprenant. C'est pourquoi il souligne les nombreux champs qui restent à investiguer et les nombreux outils d'observation à mettre en œuvre, mais il permet également de proposer les premières orientations des travaux et actions à poursuivre.

Quelques axes forts en ressortent.

- Les conditions d'exploitation et de valorisation des données collectées par des objets connectés sont au cœur du développement de ces technologies et un enjeu majeur. Pourtant de nombreuses questions restent en suspens selon que ces données relèvent du statut de données personnelles (recueillies dans la sphère privée, professionnelle

[1] Voir annexe 3.

[2] Voir annexe 7.

ou publique) ou qu'elles relèvent du champ des données à caractère non personnel (échangées entre machines). Si les premières font l'objet d'un cadre juridique qui a fait ses preuves – le RGPD, règlement général sur la protection des données –, celui-ci devra néanmoins s'adapter aux enjeux spécifiques de l'IdO et un cadre de régulation *ad hoc* doit être défini pour les données à caractère non personnel.

- Des aspirations contradictoires existent sur la circulation des données collectées : entre d'un côté l'aspiration à un espace large de circulation et d'usage des données de toute nature qui constitue la condition nécessaire au développement de nouveaux services et à la création de bénéfices liés à ces services, et de l'autre le souhait d'encadrer le partage de ces données pour rester suffisamment protecteur de la vie privée, de la propriété industrielle ou intellectuelle. En outre, l'absence d'un cadre adapté, sécurisé et propice au partage des données donne un avantage certain aux grandes plateformes hégémoniques, qui fixent leurs règles du jeu, en capturant les données et leur valeur pour leur seul bénéfice.

- Les enjeux de sécurité liés au développement rapide de l'IdO sont massifs, et massivement sous-estimés. Les identifier, prévenir les risques, définir les protections à mettre en place et les actions nécessaires à la remédiation des situations de crise qui ne manqueront pas de se produire doit être un objectif de premier plan.

- L'empreinte environnementale liée aux usages de l'IdO va croître rapidement. Mais elle peut rester modeste à long terme, dans la part de la consommation d'énergie globale du numérique, si les solutions technologiques les moins gourmandes en énergie (pour les réseaux télécommunication notamment) sont retenues et si la sensibilisation des usagers à plus de sobriété numérique s'engage.

- Enfin, pour disposer d'une vision complète des différents enjeux et élaborer les différentes réformes évoquées ci-dessus, il faut, en France et en Europe, un investissement important de recherche, pour établir des faits et des connaissances techniques robustes et rester pertinent malgré la rapidité des évolutions technologiques.

Gilles de Margerie
Commissaire général de France Stratégie

SOMMAIRE

SYNTHÈSE

Des apports remarquables, des impacts omniprésents, des enjeux complexes

Les objets du rapport

L'Internet des objets désigne la mise en réseau, au moyen d'Internet, d'objets physiques. Ce peut être une ampoule électrique, un panneau de signalisation, un bracelet, une brosse à dent, un pacemaker, une poupée, un thermostat, un pluviomètre, un détecteur de CO_2, une caméra, un vélo, un vêtement ou encore un ensemble de capteurs actionneurs sur une chaîne de production industrielle… Passerelle entre le monde physique et le monde virtuel, cette mise en réseau numérique globale a des impacts profonds sur tous les secteurs de l'activité humaine : notre habitat, nos véhicules, notre environnement de travail, nos usines, nos villes, notre agriculture, notre système de santé. D'abord simple solution technologique, l'Internet des objets – IdO en français ou IoT en anglais pour « *Internet of Things* » – est devenu l'un des éléments clés de la transformation numérique et de l'Internet que nous connaissons. En 2021, la Conférence des Nations unies sur le commerce et le développement[1] l'a distingué parmi les onze technologies dites de rupture[2].

L'Internet des objets est porteur de promesses, comme l'illustre la soixantaine de cas d'usage répertoriés pour ce rapport – dont douze cas emblématiques présentés en détail –, parce qu'ils améliorent la maîtrise de notre environnement ou parce qu'ils contribuent à une meilleure qualité de vie. Les applications en matière de santé et de sécurité sont prometteuses. Dans les secteurs industriels et agricoles, des hausses de la qualité et de la productivité sont mises en avant par les acteurs. Enfin, les technologies de l'IdO pourront accompagner la transition énergétique et la lutte contre le réchauffement climatique en améliorant la gestion et l'accès aux ressources essentielles (énergie, eau, air).

[1] CNUCED (2021), *Technology and Innovation Report 2021. Catching Technological Waves: Innovation with Equity*, Conférence des Nations unies sur le commerce et le développement.

[2] Les dix autres technologies sont l'intelligence artificielle, le Big Data, la *blockchain*, la 5G, l'impression 3D, la robotique, les drones, l'édition génomique, les nanotechnologies et le photovoltaïque solaire.

Le déploiement massif de l'IdO est aussi porteur d'interrogations et de nombreuses inconnues. Les impacts de ce phénomène émergent et multidimensionnel – diversité des objets connectés, des technologies mobilisées, des acteurs impliqués – sont encore difficiles à appréhender. Quelles sont les perspectives de développement réelles ? Quels seront les usages, avec quel niveau et quelle rapidité d'adoption ? Ces technologies auront-elles les effets escomptés en matière environnementale, au profit de la lutte contre le réchauffement climatique ? Le cadre juridique actuel est-il adapté, notamment en termes de protection des données et d'usage de l'intelligence artificielle ? Quels seront les bénéfices réels pour les citoyens et les entreprises ? Quelles seront les technologies et les standards qui s'imposeront et qui seront les promoteurs et les bénéficiaires de ces technologies et des valeurs ainsi créées ?

« L'effet cocktail », c'est-à-dire la présence généralisée d'objets connectés dans les sphères privées et publiques de la vie quotidienne et leurs interconnexions multiples, pose sous un jour nouveau les problématiques sociales et éthiques du numérique (surveillance, sécurité, protection de la vie privée). En matière environnementale, la massification d'objets communicants, l'intensification de l'utilisation des réseaux et la création de nouvelles infrastructures de stockage et de traitement pour exploiter les volumes particulièrement importants de données produites conduisent inévitablement à une augmentation de la consommation énergétique et à une empreinte environnementale accrue du numérique. Dans quelle mesure les bénéfices environnementaux de l'IdO pourront-ils compenser voire dépasser les coûts liés à la production des objets, à leur consommation énergétique et au traitement des déchets qu'il occasionnera ?

Dans la lettre de mission adressée à France Stratégie[1], la ministre de la Transition écologique, Mme Barbara Pompili, et le secrétaire d'État chargé de la transition numérique et des réseaux de télécommunication M. Cédric O, ont souhaité disposer d'une étude portant « sur les principaux impacts de l'Internet des objets, et notamment à partir de la 5G, sur l'environnement (…), sur la vie quotidienne des Français, tant par leur impact social (…) que par les enjeux sociétaux qu'ils soulèvent ». Cette étude réalisée « sur la base des connaissances existantes » s'appuie « sur un comité d'experts, spécifiquement créé, dont la composition devra garantir la pluralité des points de vue ».

Les éléments figurant dans ce rapport résultent de l'analyse de multiples sources bibliographiques et d'informations issues des contributions de quatorze experts de tous horizons – représentants de la société civile, politiques, académiques, institutionnels – qui ont accompagné la réflexion et la préparation de ce document. Une trentaine d'auditions ont permis d'enrichir ce matériau. Sont également présentés des éléments sur le contexte international en Europe et aux États-Unis, complétés par une enquête comparative

[1] Voir annexe 1.

réalisée par la Direction générale du Trésor qui porte sur huit pays (Chine, Chili, Estonie, Finlande, Inde, Israël, Japon et Nigéria)[1]. Enfin, certains volets du rapport ont été préparés avec l'appui des cabinets de conseil Boston Consulting Group et EY-Parthenon, qui nous ont fait bénéficier de leur expertise dans ce domaine.

Ce rapport a pour objet d'apporter des clés de compréhension de l'IdO, domaine dont il est encore difficile de mesurer l'ampleur et d'appréhender tous les enjeux pour l'action publique. **La première partie s'attache à COMPRENDRE l'Internet des objets** et à expliciter les principales notions, notamment en proposant une définition raisonnée, en décrivant les technologies mobilisées et en dressant un panorama des principaux indicateurs économiques du secteur qui est encore quasi inexistant dans la statistique publique. **La deuxième partie se propose d'ANALYSER les enjeux sociaux et environnementaux** que soulève de façon singulière l'IdO. **La troisième partie présente des pistes pour AGIR** et pour accompagner le développement de l'Internet des objets dans le respect d'un certain nombre d'exigences sociales et environnementales.

Si le rapport apporte un éclairage sur les évolutions économiques à partir de quelques indicateurs, il n'aborde pas les enjeux économiques (position et compétitivité des acteurs français, modèles des opérateurs, répartition de la chaîne de valeur, concurrence), conformément à la lettre de mission. Même si ces sujets n'entraient pas dans le périmètre de la mission confiée à France Stratégie, le rapport souligne la nécessité de mener des études complémentaires qui permettront d'éclairer la construction d'une vision stratégique (économie de la donnée, chaînes de valeur des acteurs, définition des marchés pertinents, etc.).

Une réalité complexe à quantifier

Connecter des objets entre eux et à l'Internet est devenu facile, les usages possibles sont multiples et la croissance du nombre d'objets connectés est extrêmement rapide. L'IdO est partout, mais **il n'existe pas encore de définition globalement acceptée au niveau mondial**, du fait de la diversité des objets à considérer. Ce rapport propose une définition englobante et dynamique soulignant notamment les interactions possibles entre les objets et leur environnement. Comme pour de nombreuses définitions actuellement utilisées et dans une vision additive de l'IdO, nous choisissons de considérer seulement les objets qui n'étaient pas déjà constituants d'Internet :

« *L'internet des objets est un ensemble d'objets connectés et de technologies de réseaux qui, à l'exclusion des stations de travail, des tablettes, des téléphones portables et des smartphones, se conjuguent en associant :*

[1] Les critères qui ont présidé au choix de ces pays sont présentés en annexe 7.

- *des objets physiques qui possèdent des capteurs connectés, éventuellement dotés de capacités de calcul et qui sont en mesure d'interagir avec leur environnement ;*
- *des réseaux de communication numériques filaires ou non filaires qui permettent de communiquer les données issues de ces objets ;*
- *des espaces de stockage distants pour les données recueillies ;*
- *des applications de traitement des données qui engagent des processus décisionnels à même de rétroagir sur des objets physiques inanimés ou vivants.*

Un objet ou un ensemble d'objets de l'IdO est appelé un dispositif IdO. »

Comme c'est le cas pour d'autres vagues de transformation dans le domaine numérique, les projections concernant le nombre d'objets connectés ou le chiffre d'affaires de l'IdO fournies par différentes institutions (publiques ou privées) ne portent pas sur les mêmes périmètres. Elles sont peu robustes et probablement surestimées. Nous avons constaté l'**absence aujourd'hui d'outils statistiques fiables** permettant de mesurer la volumétrie et l'ampleur de la croissance du nombre d'objets concernés, la part des réseaux utilisés pour ces nouveaux usages ou même le volume de données générées par les applications IdO.

Le nombre d'objets connectés estimés pour l'année 2020 selon les sources consultées varie dans une fourchette allant de 18 milliards à 78 milliards au niveau mondial. L'Ademe et l'Arcep estiment **leur nombre à 1,8 milliard en Europe dont 244 millions pour la France**[1]. Malgré ces écarts importants, si l'on considère les tendances sur les six dernières années, quelle que soit la source, qu'il s'agisse de prévisions ou d'estimations du réalisé, toutes concordent sur le constat d'une très forte croissance des objets connectés, dont le nombre aurait doublé en six ans. Pour établir ses projections relatives à la consommation énergétique du numérique, l'Agence internationale de l'énergie (AIE) estime que **le stock du nombre d'objets connectés va plus que doubler de 2020 à 2030, passant de 20 milliards** (soit la borne basse de la fourchette mentionnée *supra*) **à environ 45 milliards**[2]. En termes de marché, la CNUCED[3] estime que ce marché s'élevait à 130 milliards de dollars en 2018 et qu'il devrait être multiplié par plus de dix d'ici 2025 pour atteindre 1 500 milliards de dollars. Selon ces mêmes estimations, la France et le Royaume-Uni représentent 3 % chacun du marché mondial, soit 45 milliards de dollars, une part légèrement inférieure à leurs parts dans le PIB mondial.

[1] Ademe et Arcep (2022), *Évaluation de l'impact environnemental du numérique en France et analyse prospective*, janvier. Ademe : Agence de la transition écologique. Arcep : Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.

[2] AIE (2019), *Total Energy Model for Connected Devices*, IEA 4E EDNA, programme de coopération technique de l'Agence internationale de l'énergie, juin.

[3] CNUCED (2021), *Technology and Innovation Report 2021*, *op. cit.*

En France, l'intensité de l'usage de l'IdO – c'est-à-dire la fréquence de recours à des applications de l'IdO – **est relativement limitée et très variable selon les secteurs**. L'enquête Insee TIC entreprises 2020[1] montre qu'en moyenne 10 % des entreprises de dix salariés ou plus utilisaient l'Internet des objets. Cette proportion est trois fois plus élevée (29 %) pour les entreprises de 250 salariés ou plus, qui prennent en charge un nombre plus important d'équipements et de produits. Elle varie aussi selon les secteurs, avec des valeurs supérieures à la moyenne dans les transports (16 %), les TIC (12 %) et l'industrie (11 %) et des valeurs inférieures à la moyenne dans le commerce de gros, le commerce et la réparation automobile, ainsi que dans l'hébergement et la restauration (une proportion autour de 7 %). Pour ces derniers secteurs, une des explications avancées par l'Insee résiderait dans la plus faible proportion de grandes sociétés (7 % des entreprises y emploient 50 personnes ou plus, contre 15 % dans l'ensemble des secteurs).

Des impacts environnementaux avérés mais difficiles à objectiver

En matière d'impact environnemental, les estimations de gains et de bénéfices comme les estimations de coûts – consommation énergétique et empreinte carbone – doivent aussi être considérées avec précaution. Alors que de nombreux acteurs du marché ont intérêt à surestimer les perspectives de bénéfices, la recherche académique et les publications institutionnelles les plus robustes portent elles avant tout sur les estimations des coûts. Toutefois, au vu de ces différentes estimations, si les bénéfices de l'IdO sont mesurables individuellement au sein d'une entreprise dans une chaîne de production, l'impact global est plus difficile à évaluer. Mais il est d'ores et déjà avéré que **l'IdO contribuera à l'augmentation de l'empreinte carbone globale du numérique.** Pour la seule consommation énergétique, cela pourrait représenter **plus de 200 TWh** de consommation supplémentaire à **l'horizon 2025 au niveau mondial**, sur une consommation globale du numérique qui devrait se situer entre 5 700 et 7 300 TWh par an[2]. En France, les travaux récents de l'Ademe et de l'Arcep ont permis d'estimer la consommation électrique annuelle du numérique à plus 48 TWh/an, soit 10 % de la consommation électrique annuelle française[3]. Sur la base d'un nombre d'objets connectés installés en France de 244 millions, consommant en moyenne 30 kWh/an[4], la

[1] Insee (2020), « Les TIC et le commerce électronique dans les entreprises en 2020. Enquête Technologies de l'information et de la communication (TIC) auprès des entreprises », *Insee Résultats*, avril.

[2] Citizing, KPMG et Virtus management (2020), *Étude relative à l'évaluation des politiques publiques pour réduire l'empreinte environnementale du numérique*, étude réalisée à la demande de la commission de l'aménagement du territoire et du développement durable du Sénat, juin ; Hugues Ferreboeuf, audition du 28 octobre 2021.

[3] Ademe et Arcep (2022), *Évaluation de l'impact environnemental du numérique en France…*, *op. cit.*

[4] Sur la base d'une estimation d'une consommation électrique moyenne d'un objet connecté de 30 kWh fournie par le cabinet BCG, toutefois, l'étude Ademe et Arcep (2022) fourni des valeurs plus basses : 1 smartphone = 3,9 kWh/an (usage individuel), 1 tablette = 18,6 kWh/an, 1 enceinte connectée = 23 kWh/an.

consommation électrique des objets connectés serait d'environ 7,2 TWh/an, soit 15 % de la consommation des biens et services numériques.

Quant à l'empreinte carbone du numérique en France, elle est estimée actuellement à près de 17 $MtCO_2eq$[1] dont 460 000 tCO_2eq pour le seul IdO. À l'horizon 2040, elle pourrait s'élever à plus de 6 $MtCO_2eq$[2], sur les 24 $MtCO_2eq$ pour le numérique dans sa globalité[3].

Réduire l'impact environnemental de l'IdO implique des choix technologiques et des usages guidés par le critère de sobriété

Les technologies de communication jouent un rôle déterminant dans l'IdO. Certaines applications peuvent avoir besoin de bande passante importante, comme la réalité virtuelle, d'autres nécessitent une durabilité longue, par exemple les capteurs environnementaux, qui ne peuvent pas être rechargés fréquemment. De façon générale, le choix d'une technologie réseaux pour la mise en œuvre d'un service IdO se décline autour de cinq dimensions : la connectivité, la bande passante, le délai, la fiabilité et la sécurité des communications. Or l'empreinte environnementale est très différente selon les réseaux mobilisés. **Privilégier des choix de technologies de réseaux de communication peu consommatrices de ressources devrait permettre de réduire l'empreinte environnementale de l'IdO.**

Les caractéristiques techniques des réseaux existants – débit, consommation énergétique, couverture, latence – permettent de répondre aux différents cas applicatifs et de couvrir un large spectre d'usages possibles. Les réseaux 5G ne constituent qu'une solution parmi d'autres. Si leur efficacité énergétique est plus élevée que celles des réseaux prédécesseurs (2G, 3G, 4G), elle est toute relative au regard d'autres solutions plus adaptées à de nombreux cas d'usages de l'IdO (objets connectés du quotidien, smart compteurs, capteurs environnementaux, etc.).

Les données au cœur des enjeux sociaux individuels et collectifs de l'IdO s'invitent dans l'organisation des collectifs de travail

Le développement de l'IdO implique la présence de capteurs qui collectent, parfois à notre insu, une variété et un nombre important de données. Certes, la collecte et le traitement des données personnelles sont soumis au respect du droit fondamental des individus et à la protection de leur vie privée, prévus au titre du Règlement général sur la protection des

[1] Ademe et Arcep (2022), *op. cit.*

[2] Citizing, KPMG et Virtus management (2020), *Étude relative à l'évaluation des politiques publiques pour réduire l'empreinte environnementale du numérique*, *op. cit.* ; Hugues Ferreboeuf, audition du 28 octobre 2021.

[3] Citizing, KPMG et Virtus management (2020), *op. cit.*

données (RGPD). Mais cette collecte massive et systématique par des capteurs ou objets souvent invisibles pose de nouvelles questions, par exemple sur les **conditions d'exercice des droits de l'usager** (droit d'accès, de rectification ou d'effacement, opposition au traitement, etc.) ou sur les **modalités d'obtention de son consentement**. Par ailleurs, les questions relatives au **statut de données à caractère non personnel** (ne relevant pas de la catégorie des données personnelles) se posent avec acuité. Ces données sont générées à partir des millions de capteurs disposés dans les espaces professionnels, les espaces publics et les collectivités, notamment avec le développement de « services intelligents » (gestion des déchets, des réseaux de distribution des fluides, du trafic, entretien de la voierie, etc.). Pourtant, le statut juridique de cette catégorie de données est incertain et les possibilités de partage et de création de valeur à partir de leur exploitation sont encore trop limitées. Ces sujets doivent devenir un sujet de réflexion collective et, demain peut-être, de réglementation.

Entre espaces privés et espaces publics, le déploiement de l'IdO dans les espaces professionnels est encore relativement peu étudié. Si l'IdO concerne aujourd'hui surtout les travailleurs des secteurs qui s'en sont emparés le plus rapidement (transports et logistique, TIC, certaines industries, etc.), il touchera à terme tous les milieux professionnels. Le déploiement de l'IdO offre des potentialités importantes pour **modifier et optimiser les organisations de travail**, pour superviser la qualité des produits et les processus. Il peut contribuer à **améliorer les conditions de travail** – par exemple par la détection continue de l'environnement des travailleurs pour anticiper des risques physiques ou psychologiques ou pour adapter en temps réel cet environnement (luminosité, température, etc.). Il participe, comme de nombreuses mutations numériques, à la redéfinition de certains métiers et des compétences associées, avec un effet global sur l'emploi qui reste à ce jour difficile à appréhender. Mais l'IdO peut aussi s'accompagner d'une intensification du travail, affectant tant la responsabilité que l'autonomie des travailleurs, et surtout exposer les salariés à une surveillance renforcée de leur travail. Ce sont des enjeux importants qui ne doivent pas être omis **dans les agendas des partenaires sociaux et du dialogue social**, et qui nécessitent une appréhension fine des pouvoirs publics.

Des cadres juridiques fragmentés et en construction

Il n'existe pas de réglementation spécifique à l'IdO. Le cadre juridique des objets connectés couvre aujourd'hui une grande diversité des champs du droit et de la régulation : protection des données personnelles, cybersécurité, droit de la concurrence, de la consommation, des télécommunications, de l'environnement, de la santé, etc. En France, le cadre juridique de l'IdO s'appuie aussi sur la réglementation européenne existante ou en cours d'élaboration (cybersécurité, sécurité des produits, etc.). Il est complexe à appréhender, pour les entreprises notamment, et de nombreuses questions juridiques restent en suspens comme la détermination des responsabilités en cas de produits défectueux ou de

dommage provoqué par les objets connectés. Les expériences étrangères montrent que les pays qui se sont dotés d'un cadre juridique spécifique disposent également d'une stratégie globale pour l'IdO (par exemple les États-Unis).

Les éléments collectés et analysés à l'occasion de cette mission confirment la nécessité de conduire une **analyse juridique approfondie, notamment sur les dispositions actuelles du droit de la consommation et de la cybersécurité selon les spécificités présentées par les objets connectés.** En outre, l'IdO étant par nature à la frontière de nombreux domaines de l'action publique, le champ des compétences des autorités administratives ou des agences en charge de ces domaines d'application pourrait être amené à être précisé au vu des questions spécifiques posées.

Les risques de cyberattaque accrus par l'IdO

L'Internet des objets va considérablement étendre les failles potentielles et la surface d'attaque disponible pour des actes de malveillance ou des vols de données. La maturité des technologies mobilisées est encore inégale, ce qui ajoute une source de vulnérabilité. Poursuivre la recherche mais aussi intensifier le travail au sein des enceintes internationales pour favoriser des standards européens sont des leviers pour mieux maîtriser ces risques. En outre, **les objets connectés peuvent devenir les tremplins d'actions très dommageables, en raison de leur capacité à produire des effets « physiques » et systémiques susceptibles de toucher les collectivités ou les infrastructures stratégiques.** Ces risques systémiques sont insuffisamment pris en compte.

Exigences environnementales, droits des utilisateurs, souveraineté technologique : une stratégie européenne de l'IdO doit émerger

Les enjeux que soulèvent l'élaboration et l'adoption des standards, ainsi que l'évolution des protocoles (notamment IP, identification des objets sur le réseau, etc.), sont déjà très largement débattus au niveau international où des acteurs étatiques et privés tentent d'imposer leurs standards et leurs technologies. Ces standards auront des répercussions sur la nature des services proposés mais aussi sur la protection et la sécurité des utilisateurs, qu'il s'agisse de particuliers, de personnes morales ou de collectivités, et plus globalement sur le fonctionnement d'Internet et de son économie.

L'Europe et la France ont des atouts à faire valoir – des entreprises, des acteurs, des solutions technologiques, des équipes de recherche – qui devraient permettre de développer une véritable filière de l'IdO au profit des entreprises du numérique mais bien au-delà d'ouvrir une voie originale par rapport aux modèles américains et chinois.

Les cinq principaux constats issus de l'analyse

À l'issue de nos travaux, nous dressons cinq principaux constats qui montrent que l'Internet des objets est bien plus qu'une simple évolution technologique.

- **L'IdO a déjà et va avoir un impact croissant sur la société, les citoyens et les entreprises**. Il va transformer nos rapports au numérique et en particulier les interactions humain-machine. Son omniprésence et sa relative invisibilité vont avoir des conséquences sur la vie privée ainsi que sur le travail et son organisation. L'ampleur et la diversité du phénomène sont telles qu'il est difficile d'en évaluer de manière robuste l'évolution, ne serait-ce qu'à cinq ans. Il faut disposer de moyens d'observation plus précis pour améliorer la compréhension des enjeux – techniques, éthiques, environnementaux ou économiques –, par la puissance publique et par la société en général.
- **L'IdO va constituer une composante importante de l'impact environnemental du numérique**. La massification des usages et des infrastructures (réseaux, *edge*, cloud, équipements) conduit à une augmentation significative de la consommation énergétique et de l'empreinte carbone – hausse à mettre en regard des bénéfices potentiels sur la maîtrise des autres dépenses énergétiques et des engagements de l'accord de Paris. Nous proposons plusieurs recommandations pour réduire cet impact en tenant compte de l'ensemble des dimensions de l'IdO, du choix des réseaux au recyclage des équipements.
- **L'IdO accroît les surfaces de vulnérabilité et présente des risques renouvelés en matière de cybersécurité**. Aux risques déjà connus de vols de données ou d'actes de malveillance s'ajoutent des risques d'attaques systémiques à très grande échelle. Nos propositions visent à améliorer la coordination de l'action publique dans ce domaine.
- **Les développements de l'IdO se jouent largement hors de nos frontières**. Les technologies impliquées sont de maturité inégale, avec des incertitudes techniques qui restent à lever. **Les défis ne sont pas seulement techniques mais aussi géo-politiques.** La France comme l'Europe disposent d'atouts pour jouer un rôle dans cette compétition. Nos propositions soulignent l'importance de la recherche et d'une présence plus active dans les instances de gouvernance de l'Internet mondial.
- **L'IdO 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. Pour la protection des données personnelles, le cadre juridique actuel fondé sur le RGPD couvre la majorité des situations d'utilisation de l'IdO. Mais certaines applications ne permettent pas la mise en œuvre d'un consentement libre et éclairé et il reste des incertitudes sur le statut des données non personnelles produites dans le cadre d'applications IdO, ainsi que sur la protection des consommateurs. Nos propositions visent à assurer une meilleure protection de la vie privée et des droits fondamentaux des utilisateurs mais aussi à lever des incertitudes sur le statut des données non personnelles tout en proposant de favoriser leur valorisation.

Synthèse des recommandations

Le rapport propose plusieurs pistes d'action qui, en raison de l'ampleur du champ étudié et des délais de réalisation de l'étude, sont des premières pistes qui restent à instruire en détail. Ces recommandations visent à éclairer le législateur, les citoyens et les entreprises, pour leur permettre de s'approprier nos travaux et d'en saisir les principaux enjeux. Elles ont aussi vocation à anticiper les sujets sur lesquels une action publique pourrait être nécessaire. Nos recommandations s'organisent autour de cinq axes.

Donner les moyens de développer une vision stratégique de l'Internet des objets : observer, mesurer, comprendre, protéger

1 – **Disposer d'un outil d'observation dédié** portant sur les technologies, le niveau de déploiement, les acteurs et les usages, pour favoriser l'émergence d'une vision stratégique de l'IdO tant pour la puissance publique que pour les acteurs du marché.

2 – **Intégrer systématiquement au sein du nouvel Observatoire des impacts environnementaux du numérique, prévu au titre de la loi REEN du 15 novembre 2021, un volet IdO** en prenant en compte l'ensemble des dispositifs impliqués dans son fonctionnement (capteurs, réseaux, usage et stockage) sur tout le cycle de vie des équipements.

3 – **Faciliter la connaissance des réglementations**, normes, certifications, et animer une veille sur les évolutions des cas d'usage et des législations étrangères pour l'information des entreprises.

4 – **Mieux évaluer les risques systémiques de cyberattaques spécifiques à l'Internet des objets** (impacts, coûts, mesures de résilience) et mieux articuler les compétences des organismes en charge de la prévention et de la lutte contre ces menaces, notamment dans le cadre de la stratégie cyber définie au niveau européen.

Développer la recherche et intensifier la présence française dans les instances de gouvernance de l'Internet

5 – **Encourager et promouvoir les travaux de recherche** notamment ceux qui favorisent **l'interopérabilité et la portabilité** des solutions IdO, tout en soutenant les initiatives des acteurs français et européens (organismes de recherche, entreprises) quand elles existent (système d'exploitation tel que RIOT, adoption d'identifiants uniques et travaux de l'AFNIC, par exemple).

6 – **Préparer et soutenir la représentation française** dans les institutions internationales et européennes et dans les instances de normalisation et de gouvernance de l'Internet (UIT,

3GPP, W3C, IETF, IGF)[1] en privilégiant (comme les Américains et les Chinois) des représentations mixtes (diplomates, scientifiques, parties prenantes).

7 – **Permettre la mise en place d'expérimentations** à grande échelle visant à valider des propositions techniques et à évaluer leur impact environnemental et social.

8 – **Encourager la coopération internationale, en particulier sur le partage des données** environnementales recueillies par les objets connectés, notamment celles relatives aux risques climatiques.

Permettre le développement d'un IdO éthique et respectueux des utilisateurs

9 – **Informer le citoyen sur la protection de ses données personnelles,** de sa vie privée et de ses libertés et droits fondamentaux ainsi que sur la protection de sa sécurité et de la confidentialité de ses données par une information disponible sur les produits, ou par des campagnes d'information publiques associant les différentes parties prenantes.

10 – L'utilisation de l'IdO dans les interventions médicales doit faire l'objet d'une **déclaration explicite aux professionnels de santé et aux patients.** Explorer la possibilité d'étendre cette démarche à d'autres cas d'usage considérés comme critiques.

11 **– Consolider** la mise en œuvre d'une information claire et, lorsque cela est nécessaire, **d'un consentement « libre, spécifique, éclairé et univoque »** pour les services de l'IdO, dans le respect du RGPD.

12 **– Informer les usagers de la présence de capteurs** et de la possibilité de traçage de leurs objets connectés personnels, notamment dans les espaces publics qu'ils fréquentent (rues, espaces commerciaux, lieux de loisirs, etc.), à l'image des dispositions relatives à la vidéosurveillance. Introduire un droit à l'arrêt ou à la déconnexion d'un dispositif IdO.

13 **– Adapter le cadre réglementaire actuel pour permettre un bon niveau de protection des publics vulnérables** (avec une attention particulière pour les personnes mineures, âgées, en perte d'autonomie, etc.).

14 **– Expertiser les enjeux spécifiques de l'IdO sur le lieu de travail** (santé et sécurité, emploi et conditions de travail, droits des données et surveillance du travail) à différents niveaux (règlementation, dialogue social, pratiques de entreprises) notamment dans le cadre des travaux menés par l'observatoire **LaborIA**. Ces travaux doivent s'accompagner d'une réflexion juridique à l'intersection du droit du travail, du droit civil et du numérique.

15 **– Confier au Comité national pilote d'éthique du numérique** l'organisation d'une réflexion associant la CNIL, le Défenseur des droits et la Commission nationale

[1] Voir le glossaire en annexe 4.

consultative des droits de l'homme sur les enjeux éthiques et la protection des libertés et droits fondamentaux relative à la conception et à la mise en œuvre des usages de l'IdO.

16 **– Étendre le champ de compétence de la Commission nationale du débat public (CNDP)** aux questions et aux enjeux du numérique, conformément à la recommandation de cette commission du 21 février 2021, sur les projets de révision de l'article R 121-2, afin notamment de lui donner les outils lui permettant d'intervenir sur l'ensemble des questions relatives à l'environnement.

Soutenir le développement d'un IdO sobre et responsable

17 **– Mieux organiser les filières de recyclage pour qu'elles s'adaptent aux objets connectés,** y compris les produits hors filière électronique et électrique qui deviendront connectés (textiles, électroménagers, petits équipements), depuis les filières de tri jusqu'au recyclage, dans la perspective notamment de la révision de la directive européenne sur les DEEE (déchets des équipements électroniques et électriques).

18 **– Inclure les dispositifs IdO dans le référentiel général d'écoconception des services numériques,** prévu au titre de la loi REEN du 15 novembre 2021.

19 **– Intégrer dans la gestion du spectre radioélectrique des dispositifs d'incitation à des choix d'implémentation frugaux** (énergétique, données, ressources, algorithmes).

20 **– Mettre à disposition des acheteurs publics et des prescripteurs, en particulier auprès des collectivités, des outils d'aide à la décision** (bonnes pratiques, simulateurs indépendants) pour mesurer l'efficacité et les bénéfices environnementaux du déploiement d'une solution IdO (coûts/bénéfices, proportionnalité, finalité, transparence, etc.) afin de nourrir les stratégies territoriales pour un numérique responsable prévues au titre de la loi REEN du 15 novembre 2021. Cette disposition pourrait également être appliquée dans le cadre de la mise en œuvre de l'article 36 de la loi n° 2021-1104 du 22 août 2021 portant sur la lutte contre le dérèglement climatique et le renforcement de la résilience face à ses effets.

21 **– Intégrer dans les certifications ou labels existants à l'attention du grand public des mentions spécifiques relatives aux objets connectés** et aux services associés permettant de s'informer sur l'impact de leurs usages mais aussi sur le niveau de confiance de ces dispositifs (fiabilité, privacy by design, transparence, proportionnalité, éthique, etc.) ou encore sur les risques cyber.

22 **– Intégrer explicitement les objets connectés grand public dans la liste des produits concernés par l'indice de réparabilité** prévu au titre de l'article 16 de la loi n° 2020-105 du 10 février 2020 relative à la lutte contre le gaspillage et à l'économie circulaire, dite loi AGEC.

Concevoir un IdO de confiance pour les entreprises, les citoyens et les acteurs publics

23 **– Créer les conditions favorables au partage maîtrisé et à la valorisation des données** qui vont être massivement recueillies par les dispositifs IdO, en favorisant l'émergence d'acteurs en capacité d'offrir aux entreprises et aux personnes publiques des garanties sur la sécurité des échanges, leur confidentialité et l'intégrité des données échangées.

24 **– Définir un statut de données sensibles** au-delà des données personnelles ou médicales pour les données industrielles ou celles qui, recueillies dans le cadre de déploiement massif de dispositifs d'observation (caméras, capteurs) pourraient présenter des risques stratégiques ou de sécurité nationale (certaines données d'urbanisme ou d'équipement des collectivités ou dans le domaine de l'agriculture).

25 **– Veiller à préserver des pratiques concurrentielles sur les différents maillons du marché de l'IdO**, y compris pour les dispositifs palliant l'absence d'interopérabilité (assistants conversationnels notamment).

26 **– Procéder aux analyses juridiques permettant notamment de définir l'échelle des responsabilités sur la chaîne des usages** afin de clarifier les niveaux de responsabilité entre les différents intervenants dans la mise en œuvre d'une solution IdO (les fabricants de capteurs, les opérateurs de réseaux et de plateformes, les entreprises qui commercialisent le service).

27 **– Analyser l'opportunité d'une loi cyber globale** compte tenu de l'étendue du champ des usages de l'IdO et du caractère interministériel des administrations concernées à l'occasion de l'adoption du Cyber Security Act européen.

28 **– Accompagner les acheteurs publics** (collectivités, hôpitaux, universités, etc.) dans la mise en œuvre et l'achat de solutions incluant des objets connectés, en mettant à leur disposition des ressources (guide d'achat, bonnes pratiques) réalisées en collaboration avec l'ANSSI, la CNIL, l'Ademe et l'ANSES.

29 **– Cartographier les compétences respectives des régulateurs publics susceptibles de couvrir le champ de l'IdO** (télécom, données, concurrence, droit des consommateurs, etc.) afin d'identifier les lacunes existantes (par exemple, compétences Arcep sur d'autres acteurs que télécom pour le recueil des données relatives à l'Observatoire des impacts environnementaux du numérique) mais aussi de mesurer les moyens à mettre à leur disposition pour l'exercice de leur mission.

30 **– Procéder pour l'IdO à une analyse juridique fondée sur une approche d'analyse des risques,** complémentaire de la démarche engagée à l'occasion de la proposition européenne d'Artificial Intelligence Act qui définit les typologies de risques (inacceptable, élevé, limité et minimal). Cette approche permettrait d'élaborer des protocoles de conformité pour les entreprises et les collectivités.

INTRODUCTION

« L'Internet des choses », « l'Internet de toutes choses[1] » ou encore le « système nerveux planétaire[2] »… Les expressions ne manquent pas pour qualifier le phénomène. La plus courante, l'Internet des objets (IdO) s'est imposée dans le vocabulaire français (en anglais *Internet of Things* ou *IoT*). Elle désigne la mise en réseau, au moyen d'Internet, d'objets physiques comme une ampoule électrique, un bracelet, une brosse à dent, un pacemaker, une poupée, un thermostat, un pluviomètre, un détecteur de $C0_2$, une caméra, un vélo, une voiture, un vêtement, etc. S'agit-il d'une simple évolution technologique ou d'une transformation plus profonde de notre environnement ? Pour l'European Research Cluster on the Internet of Things[3], l'IdO présente des caractéristiques nouvelles désignées sous l'acronyme des **5A** : ***A**nything, **A**nyone, **A**nytime, **A**ny place, **A**ny service, **A**ny network*[4].

Avec l'Internet des objets, nous sommes entrés dans une nouvelle étape historique de l'évolution des entités connectées décrite par Tim Berners-Lee en 2006[5]. Après Internet, le réseau des machines informatiques en 1974 ; après le Web, l'Internet des documents en 1990 et après le réseau des personnes via les réseaux sociaux dès 2004 ; voici venu le temps de l'Internet des objets, l'Internet des entités cyber-physiques, instance contemporaine de la cybernétique de Norbert Wiener[6]. Ce développement majeur pose de façon renouvelée la question du contrôle, dans ses multiples dimensions. Maîtrise facilitée de notre environnement, meilleures prévisions, anticipations, mesures qui participeront au pilotage et à la maintenance de nombreuses applications nécessaires au bon fonctionnement d'une société toujours plus complexe. Mais aussi contrôles que ces technologies

[1] Inria (2021a), *Internet des objets. Défis sociétaux et domaine de recherche scientifique pour l'Internet des Objets (IoT)*, Livre blanc, n° 5, Institut national de recherche en sciences et technologies du numérique, décembre.

[2] Forbes (2012), « How the Internet of Things will change almost everything », par E. Savitz, 17 décembre.

[3] Voir la présentation sur le site de l'IERC.

[4] « N'importe quoi, n'importe qui, n'importe quand, n'importe où, sur n'importe quel terminal et n'importe quel réseau. »

[5] Voir en particulier Berners-Lee T. (2006), « Linked Data », juillet.

[6] Wiener N. (1962), *Cybernétique et société. L'usage humain des êtres humains*, Paris, Éditions des Deux rives.

volontiers invasives pourraient exercer sur nos vies, impliquant une vigilance accrue de l'utilisateur sur les conditions d'exercice de ses droits, ainsi que la maîtrise et l'encadrement du phénomène par les pouvoirs publics. Les impacts de cette interconnexion numérique globale vont être considérables, comme le résume le Livre blanc publié en décembre 2021 par l'Inria.

> « De la même manière qu'Internet a profondément bouleversé notre société, l'Internet des objets (…) impactera tous les secteurs de l'activité humaine : notre habitat, nos véhicules, notre environnement de travail, nos usines, nos villes, notre agriculture, nos systèmes de santé… De même, tous les niveaux de la société (individus, entreprises, États) sont d'ores et déjà concernés, de l'urbain au rural, ainsi que la nature[1]. »

C'est dans ce contexte que ce rapport est réalisé, à la demande de la ministre de la Transition écologique et du secrétaire d'État chargé de la transition numérique et des communications électroniques, afin d'analyser les principaux impacts sociaux et environnementaux de l'Internet des objets.

L'Internet des objets est porteur de promesses : il peut améliorer le contrôle et la maîtrise de notre environnement et contribuer à une meilleure qualité de vie grâce à de nouveaux services dans le domaine des transports, de la logistique, de la distribution, dans la gestion des villes et des espaces urbains. Les applications en matière de santé et de sécurité sont également prometteuses. Dans les domaines industriel et agricole, des perspectives d'accroissement de la qualité et de la productivité sont mises en avant par les acteurs. Enfin, les technologies de l'IdO pourront accompagner la transition énergétique et la lutte contre le réchauffement climatique en améliorant la gestion et l'accès aux ressources les plus essentielles (énergie, eau, air). Nous avons voulu dans ce rapport, par une approche fondée sur les usages, illustrer concrètement les potentialités de ces technologies, jauger leur maturité et lorsque c'est possible, étayer quantitativement ces promesses.

L'Internet des objets généralise les passerelles entre le monde numérique et le monde physique. Si le degré de maturité des cas d'usage que nous avons observés est encore inégal, l'IdO est déjà présent dans de nombreux secteurs d'activité. Son adoption généralisée dans les sphères privées et publiques de la vie quotidienne pose sous un jour nouveau les problématiques sociales et éthiques que le numérique a fait émerger dans le débat public : « l'Internet des objets met au carré toutes les difficultés identifiées initialement avec le numérique : *privacy*, domination industrielle, libertés individuelles, surveillance, démocratie, etc.[2] »

[1] Inria (2021a), *Internet des objets…*, *op. cit.*, p. 3.

[2] Henri Verdier, audition du 18 novembre 2021.

L'Internet des objets est aussi porteur de nouvelles questions, aux dimensions sociales inédites. Alors que nous disposions jusqu'ici d'un accès explicite à notre environnement numérique, via des interactions et des interfaces facilement identifiables (écran, clavier), avec la capacité de choisir les moments de nos connexions, l'IdO bouscule notre rapport aux interactions traditionnelles entre humains et machines. Les objets connectés disposent rarement d'un écran ou d'un clavier, mais proposent d'autres modes d'interaction en utilisant le son comme la voix, la vidéo, la reconnaissance de présence ou de mouvements, ou encore des données biométriques.

Une autre caractéristique propre à l'Internet des objets est la transformation de notre rapport à l'espace et au temps. Les dispositifs seront à la fois omniprésents[1] et souvent invisibles dans notre sphère privée comme dans les espaces publics ou sur nos lieux de travail. Il en découle la difficulté, voire l'impossibilité, pour une personne de choisir d'être ou non dans le champ de l'IdO, d'être ou non connectée. Surgissent ainsi des propriétés nouvelles et spécifiques qui viennent se heurter notamment à la notion de consentement[2].

Compte tenu de l'ampleur du développement attendu[3], les impacts environnementaux de la mise en place de l'IdO doivent être évalués. Chaque composante de ce nouvel Internet – les objets, les réseaux, les centres de mémorisation et de traitement des informations – consomme des ressources matérielles et énergétiques, produit pour certaines des ondes électromagnétiques et génère des déchets. Ces mêmes dispositifs peuvent être utilisés pour mieux contrôler ces impacts sur l'environnement. Ce rapport analyse les différentes variables d'une balance bénéfices/risques dont les éléments de formalisation objectifs ne sont pas simples à déterminer et à évaluer. Parmi les points d'attention, l'utilisation appropriée des réseaux cellulaires 4G et 5G est abordée, ainsi que l'analyse des questions de maintenance, de marché de seconde main et de recyclage.

Enfin, il existe encore de nombreuses inconnues sur ce que l'on pourrait appeler « l'effet cocktail » de l'Internet des objets, qui offre des possibilités d'interconnexion entre réseaux encore inexplorées et dont on ne mesure ni l'ampleur ni les conséquences. Il est particulièrement difficile d'anticiper les effets qu'auront la multiplication de ces dispositifs communicants, leur interconnexion et leurs potentialités d'échanges, de mémorisation et de traitement d'informations. Les conséquences tant techniques que sociales, économiques et environnementales peuvent être très fortement structurantes. Aujourd'hui difficilement prévisibles, elles n'en nécessitent pas moins dès à présent une réflexion sur

[1] Le terme anglais « *pervasive* » est souvent utilisé dans la littérature pour définir cette notion d'omniprésence.

[2] Cunche M., Le Métayer D. et Morel V. (2019), « A generic information and consent framework for the IoT », Trustcom 2019, 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Rotorua, Nouvelle-Zélande, août.

[3] Les chiffres diffèrent mais on pourrait arriver à 180 milliards d'objets connectés au niveau mondial en 2028, selon le cabinet d'analyse spécialisé IoT Analytics (voir notre chapitre 3 sur ce chiffrage).

leurs enjeux potentiels et sur leur respect des valeurs fondamentales que collectivement nous souhaitons mettre en œuvre et défendre. Il s'agit de se donner les moyens de contrôler l'usage de cette technologie, tant à titre individuel que collectif.

Une complexité d'un autre ordre vient s'ajouter à ce tableau déjà très riche. Il est en effet difficile de définir l'ensemble des acteurs impliqués dans cette technologie et de percevoir, à ce stade, qui seront les bénéficiaires de la valeur produite. Les auteurs du premier *Code du droit du numérique* soulignent la complexité de l'économie de l'Internet des objets.

> « Dans la chaîne économique, allant de la production à l'utilisation d'un objet connecté, il y a d'abord en amont : le fabricant qui produit l'objet ; souvent avec le concours d'un partenaire technologique qui lui s'occupe de la "connectivité" » de l'objet (capacité à se connecter), notamment en concevant et/ou choisissant les capteurs ; le tout – bien souvent – sous le contrôle d'un maître d'œuvre sous la marque duquel le produit sera commercé (…) Interviendra ensuite un prestataire de service qui opérera à partir des données collectées et transmises par l'objet lors de son usage (…) Enfin l'objet sera commercialisé auprès des clients finaux (consommateurs ou professionnel) par l'intermédiaire d'un distributeur (le vendeur)[1]. »

Comme cela a pu être le cas par le passé pour bon nombre d'innovations profondes, il est vraisemblable que le déploiement de l'Internet des objets s'effectuera de façon décentralisée, par le marché, et qu'il devra s'opérer dans un cadre de régulation évolutif. Ses multiples usages possibles, mais aussi l'impact environnemental que les dispositifs IdO peuvent avoir dans un contexte d'urgence climatique qui n'est plus celui des précédentes vagues d'innovations, interrogent la pertinence du cadre actuel de régulation et l'opportunité de son évolution – questions qui seront aussi abordées dans ce rapport.

Il existe donc de nombreuses incertitudes sur ce que sera l'Internet des objets à l'horizon 2030 : quelles sont les perspectives de développement et de maturité technologique ? Comment anticiper les usages et leur adoption ? Quelles seront les technologies et les standards les plus utilisés ? Quels seront les acteurs majeurs de ces marchés ? Quels seront les bénéfices réels pour les citoyens et les entreprises ? Ces technologies auront-elles les effets escomptés en matière environnementale, au profit de la lutte contre le réchauffement climatique et en limitant leurs externalités négatives ?

Les objectifs de ce rapport sont d'abord de clarifier à l'attention d'un public de non spécialistes ce que recouvre l'Internet des objets, en présentant dans une forme pédagogique les principaux concepts de l'IdO, tout en exposant une vision globale des enjeux sociaux et environnementaux qui en découlent.

[1] Mattatia F., Berthault D. et Degos L. (2021), *Code du numérique*. *Édition 2022*, Paris, Lexis-Nexis, coll. « Code bleu », 1re éd.

Ce rapport n'a pas vocation à traiter des enjeux économiques, des perspectives de compétitivité et de productivité qui sont les moteurs du développement de l'IdO. Au cours des auditions et dans les travaux réalisés en appui du rapport, ces points ont pourtant été régulièrement abordés. Les atouts de la France et de l'Europe sont nombreux, même s'il existe des risques importants inhérents à l'état global de l'économie numérique globalisée (domination industrielle, *privacy*, souveraineté, etc.[1]). Si nous avons pu approcher ponctuellement ces thématiques, il ne s'agit pas du sujet principal de la mission qui nous a été confiée. Notre démarche s'est appuyée sur l'observation de cas d'usage qui nous ont permis de conduire une première analyse, laquelle s'est enrichie de l'apport de plus de trente auditions[2] conduites entre les mois de septembre et décembre 2021.

Nous avons d'abord cherché à COMPRENDRE l'Internet des objets en nous soumettant à l'exercice d'une définition raisonnée, en décrivant les principales technologies mobilisées et en dressant un panorama des principaux indicateurs économiques du secteur.

La deuxième partie du rapport propose d'ANALYSER les enjeux sociaux, environnementaux et réglementaires au travers de cas d'usage emblématiques.

Enfin nous présentons dans une troisième et dernière partie des pistes pour AGIR. Le déploiement de l'Internet des objets est d'ores et déjà une réalité et nous proposons ici des mesures qui permettront d'accompagner son développement dans le respect des exigences sociales et environnementales.

[1] Voir aussi à ce sujet Toledano J. (2020), *GAFA. Reprenons le pouvoir !*, Paris, Odile Jacob.

[2] Voir la liste des personnes auditionnées en annexe 3.

PREMIÈRE PARTIE

COMPRENDRE LES CONCEPTS, LES TECHNOLOGIES ET L'ÉCONOMIE

CHAPITRE 1

UNE DÉFINITION MOUVANTE

1. Un peu d'histoire

Au départ simple solution technologique, l'Internet des objets (IdO) ou en anglais « *Internet of Things* » (IoT) est devenu un des éléments clés de la transformation numérique et de l'Internet que nous connaissons. Certains acteurs y voient la dernière évolution majeure des technologies de l'Internet. Dans les années 1970, le réseau des réseaux a permis de connecter les machines entre elles, puis dans les années 1990 et 2000, il a rendu possible l'échange d'informations, via les services de messagerie, le World Wide Web et les réseaux sociaux. C'est désormais le développement de l'IdO qui transforme en profondeur le monde de l'Internet.

Depuis l'origine de l'Internet, nous avons appris à communiquer via des objets dédiés, ordinateur, tablette, smartphone, terminal bancaire, etc. Mais l'IdO constitue une nouvelle étape, puisqu'il rend communicants des objets du quotidien dont la fonction première n'est pas de communiquer : vêtements, montres, appareils électro-ménagers, véhicules, etc. Ces objets deviennent « intelligents » et acquièrent la capacité de collecter des données, de les traiter, de les échanger et de les acheminer vers d'autres machines, pour *in fine* s'adapter voire agir sur ces machines ou sur leur environnement.

Cette évolution constitue une révolution anthropologique qui ouvre des possibilités inédites de dialogue entre des entités du monde physique. Synthèse du rapprochement entre le monde physique et le monde numérique, l'Internet des objets offre aussi la possibilité aux objets, aux personnes et, au-delà, à toute entité physique identifiable sur un réseau de télécommunication, de communiquer sans aucune interaction d'humain-à-humain ou d'humain-à-machine.

Les promesses de l'Internet des objets sont donc immenses, tant à l'échelle de notre vie quotidienne et domestique que dans le monde des entreprises, de l'industrie et plus largement dans l'ensemble de la sphère sociale.

Tableau 1 – Dates clés de l'Internet

Années 1960 Internet est né	**1989-2000** Une première révolution	**Début des années 2000** Internet devient universel	**Aujourd'hui** L'Internet des objets : la nouvelle étape
			
L'Internet connecte les ordinateurs entre eux et transmet des messages simples avec une capacité d'échange de données limitée.	Les technologies Web permettent de lier des documents. Le WWW est né (Web 1.0).	L'Internet est désormais une plateforme de communication universelle. Il transporte tout le contenu vocal, vidéo ou informationnel, les médias sociaux permettant le contenu généré par l'utilisateur (Web 2.0).	L'IoT est la prochaine étape vers la numérisation où tous les objets peuvent être interconnectés entre eux ou avec des personnes via des réseaux de communication, dans et entre les espaces privés, publics et industriels, et rendre compte de leur état et/ou de l'état de leur environnement.
			L'IoT est un élément clé du développement de l'Internet, car il se caractérise par la collecte massifiée des données connectées et analysées.

Source : France Stratégie - BCG et EY-Parthenon

2. Une définition strictement technique ne suffit pas à cerner le concept

Pourtant l'Internet des objets n'est pas si facile à définir. De fait il existe autant de définitions que de locuteurs et de points de vue : législateurs, usagers, fabricants, opérateurs de réseaux, utilisateurs, intégrateurs de services, etc. Dans une étude de 2018[1], l'OCDE a analysé les différentes définitions de l'IdO au niveau international en vue d'établir une base commune pour les travaux du Comité de la politique de l'économie numérique (CPEN). Il en ressort une grande variété d'approches : par type d'objets, par domaine d'application, par fonction. Cette même étude a proposé une taxonomie pour la mesure de l'IdO[2]. Une autre étude à paraître de l'OCDE[3] établit une comparaison des définitions retenues de l'IdO par les

[1] OCDE (2018), *IoT Measurement and Applications*, OECD Digital Economy Papers, n° 271, Paris, Publications de l'OCDE.

[2] *Ibid*., voir plus loin le Graphique 4.

[3] OCDE (2022, à paraître), *Measuring the Internet of Things*, Working Party on Measurement and Analysis of the Digital Economy, Draft report d'octobre 2021.

différents organismes statistiques de pays membres dans le cadre des enquêtes publiques sur l'utilisation des technologies de l'information et de la communication (TIC).

Quelles sont les divergences de point de vue qui rendent si difficile cette définition partagée[1] ? Le premier point d'achoppement porte sur le périmètre concerné. De quels objets connectés parle-t-on lorsque qu'on parle d'Internet des objets ?

En fait, les expressions « objets connectés » et « Internet des objets » sont souvent utilisées à tort l'une pour l'autre, car elles ne recouvrent pas les mêmes notions. Un objet connecté ne donne aucune précision quant à la nature et aux effets de la connexion, il est simplement connecté à un réseau informatique dont on ignore a priori la structure et la finalité. Le terme « Internet des objets » indique que l'on considère une structure globale en capacité de relier un ensemble d'objets numériques, de traiter les données qui en sont extraites et même d'agir en fonction de celles-ci, pour en faire un système cohérent.

Les principales sources de divergences dans les définitions portent sur la prise en compte ou non des objets numériques complexes traditionnels : les ordinateurs, les téléphones, les téléviseurs, les voitures connectées, etc. Certaines définitions les intègrent quand d'autres choisissent de ne prendre en compte que **les nouvelles catégories d'objets connectés : les capteurs, les compteurs intelligents, les objets connectés du quotidien (lunettes, montres, électro-ménager, télévision, etc.), les puces RFID**. Ce rapport aborde en priorité cette seconde catégorie, en considérant que nous sommes à un moment de bascule où ces objets dont l'usage premier n'était pas nécessairement de communiquer vont constituer une part croissante des objets connectés. Ils sont désormais plus nombreux à être dotés de capacités de calcul, de mémorisation et de communication qui peuvent dépendre d'éléments externes comme des serveurs, des stations de travail ou des smartphones. D'autres définitions ne considèrent pas comme objet connecté un capteur sans capacité de traitement de l'information et de calcul, qui se bornerait à retransmettre ce qu'il mesure. Ainsi, selon certaines définitions, le tag RFID ne serait pas un objet connecté.

Cette première difficulté rend périlleuses toutes les tentatives de mesurer le nombre des objets aujourd'hui connectés. Certaines projections estiment à plusieurs centaines de millions le nombre d'objets connectés, d'autres à plusieurs milliards. 15 milliards d'objets seraient connectés dans le monde pour l'IDATE, contre quelque 180 milliards d'objets connectés au niveau mondial en 2028 pour IoT Analytics[2].

Certaines définitions retiennent la notion d'une interaction entre l'objet et son environnement ou « boucle de rétroaction ». Cette interaction peut concerner d'autres machines (Machine-to-machine, M2M) ou des usagers (Human-to-machine, H2M). Elle

[1] OCDE (2018), *IoT Measurement and Applications*, *op. cit.*, et Inria (2021a), *Internet des objets…*, *op. cit.*

[2] Site web : https://iot-analytics.com/

permet de générer des informations qui, une fois traitées, peuvent conduire à une prise de décision ou déclencher une procédure. Les boucles de rétroactions peuvent s'imbriquer les unes dans les autres et former ainsi des systèmes particulièrement complexes.

Enfin, certaines définitions apportent des précisions sur les infrastructures qui charpentent l'IdO, comme la nature des réseaux ou des infrastructures de stockage des données.

Encadré 1 – Quelques définitions

Union internationale des télécommunications (UIT), 2012

« L'Internet des objets est une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution. »

Commission européenne, 2014

« *The Internet of Things enables objects sharing information with other objects/members in the network, recognizing events and changes so to react autonomously in an appropriate manner. The IoT therefore builds on communication between things (machines, buildings, cars, animals, etc.) that leads to action and value creation*[1]. »

OCDE, 2015 et 2018

« L'Internet des objets comprend tous les appareils et objets dont l'état peut être modifié via l'Internet, avec ou sans la participation active des individus. Alors que les objets connectés peuvent nécessiter l'intervention de dispositifs considérés comme faisant partie de "l'Internet traditionnel", cette définition exclut les tablettes portables et les smartphones déjà pris en compte dans les mesures actuelles du haut débit de l'OCDE. » La définition a fait l'objet d'une révision en 2018, afin d'en exclure les ordinateurs, les smartphones et les tablettes qui sont déjà pris en compte dans d'autres outils de mesures de l'OCDE[2].

Gartner, 2017

« *A network of dedicated physical objects (things) that contain embedded technology to sense or interact with their internal state or the external environment.*

[1] « L'Internet des objets permet le partage d'information entre des objets appartenants à un même réseau en vue de reconnaître les événements ou les changements et de réagir de manière autonome et adaptée. L'IdO s'appuie donc sur la communication entre les choses (machines, bâtiments, voitures, animaux, etc.) qui conduit à interagir avec leur environnement et à la création de valeur. » (traduction des auteurs).

[2] Pour les détails de la justification de la taxonomie retenue, voir OCDE (2018), *op. cit.*

This excludes general purpose devices such as smartphones, tablets and PCs (…) the layers define what capabilities an IoT component, function or process must possess, while the tiers define where a component, function or process operates in the IoT architecture. The interfaces define how data and control flow into, out of and through the system[1]*.* »

European Union Agency for Network and Information Security (ENISA), 2017

« *A cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making*[2]*.* »

Inria, 2021

« Dans ce document, nous considérons l'IoT comme la forme tangible d'une composante importante de l'Internet de nouvelle génération. De ce point de vue, l'IoT représente un ensemble de technologies de portée générale, qui : jettent des ponts entre le monde numérique et le monde physique ; comblent l'écart entre les technologies Internet et des systèmes embarqués de plus en plus variés (…) l'IoT comme un équivalent de l'Internet du Tout (Internet of Everything, terminologie Cisco/W3C), de l'Internet physique (Physical Web, Google), de l'informatique physique (Physical Computing, Arduino), de la communication entre machines (Machine-to-Machine, M2M), des systèmes cyberphysiques (Cyber-Physical Systems, théorie des asservissements) ou du World-Sized Web. »

Arcep, 2016

« L'Internet des objets correspond à un ensemble d'objets connectés, et de technologies de réseaux qui se conjuguent en associant : des objets physiques qui possèdent des technologies embarquées de capteurs, d'intelligence et de connectivité, leur permettant de communiquer avec d'autres objets ; des réseaux de communications électroniques qui permettent de transporter les données issues des objets ; des applications de traitement des données qui apportent les outils pour le stockage, la corrélation et l'analyse de ces données. C'est d'ailleurs souvent dans ce cloud que se trouvent les processus décisionnels à même de rétroagir sur les objets physiques. »

[1] « Un réseau d'objets physiques dédiés qui contiennent une technologie intégrée pour détecter ou interagir avec leur environnement externe et modifier leur état interne en conséquence. Cela exclut les appareils à usage général tels que les smartphones, les tablettes et les PC (…) les couches définissent les capacités qu'un composant, une fonction ou un processus IdO doit posséder, tandis que les niveaux définissent un composant, une fonction ou un processus de l'architecture globale du dispositif de l'IdO. Les interfaces définissent la façon dont les données et le contrôle circulent dans, hors et à travers le système. » (traduction des auteurs).

[2] « Un écosystème cyberphysique de capteurs et d'actionneurs interconnectés, qui permet une prise de décision intelligente. » (traduction des auteurs).

Tableau 2 – Critères retenus pour définir l'Internet des objets, selon les sources

	Typologie des objets	Notion de réseau	Espace de stockage	Notion d'interaction avec l'environnement
UiT	Inclut les objets virtuels	Non	Non	Non
OCDE, 2018	Ne prend pas en compte les PC, tablettes, smartphones	Oui	Non	Oui
Enisa	Non précisé	Non	Non	Oui
Gartner	Ne prend pas en compte les PC, tablettes, smartphones	Oui	Non	Oui
Inria	Ne prend pas en compte les PC, tablettes, smartphones	Oui	Oui	Oui
ARCEP	Non précisé	Oui	Oui	Oui

Source : France Stratégie

3. Définition et concepts retenus dans ce rapport

On le voit, l'ambition d'une définition partagée est encore loin d'être atteinte. Dans le cadre de ce rapport, le comité d'experts s'est accordé sur la définition proposée par l'Arcep[1], en y apportant quelques précisions et nuances :

« **L'Internet des objets est un ensemble d'objets connectés et de technologies de réseaux qui se conjuguent en associant** :

- **des objets physiques qui possèdent des capteurs connectés**, éventuellement dotés de capacités de calcul et qui sont en mesure d'interagir avec leur environnement ;
- **des réseaux de communication numériques filaires ou non filaires** qui permettent de communiquer les données issues de ces objets ;
- **des espaces de stockages distants** pour les données recueillies ;
- **des applications de traitement des données qui engagent des processus décisionnels à même de rétroagir** sur des objets physiques inanimés ou vivants.

Un objet ou un ensemble d'objets de l'IdO est appelé un dispositif IdO. »

[1] Arcep (2016), *Préparer la révolution de l'Internet des objets. Document n° 1 : une cartographie des enjeux*, Livre blanc, Autorité de régulation des communications électroniques, novembre.

Pour faire suite à notre propos sur les spécificités de ces nouveaux objets connectés – qui ne sont pas conçus initialement pour communiquer –, nous excluons de cette définition les stations de travail, tablettes, téléphones portables et smartphones, bien qu'il s'agisse d'objets communicants, inclus dans d'autres études.

Notre définition tient compte :

– **de la diversité des objets connectés ou connectables** : les compteurs intelligents (électricité, eau ou gaz), les caméras de surveillance, les véhicules avec système de communication embarqué, les capteurs disséminés permettant d'optimiser une chaîne de production dans une usine, l'éclairage urbain ou la collecte des déchets à l'échelle d'une ville, la surveillance et le contrôle à distance des appareils ménagers, les systèmes domotiques assurant la gestion de l'éclairage, les appareils électro-ménagers, les jouets connectés, les assistants vocaux, les télévisions connectées, les textiles connectés, les objets personnels connectés (montres, etc.), mais aussi les cartes avec ou sans contact ou les tags RFID ;

– **des multiples technologies réseaux possibles**. Cette définition est agnostique aux technologies réseaux, sur lesquelles sont déployés les dispositifs IdO, qu'il s'agisse d'un réseau privé à l'intérieur d'un bâtiment ou d'un réseau satellitaire (suivi de containers dans le transport maritime) ;

– **des différents modes de stockage des données** qui peuvent être utilisés : localement (dans un réseau privé), en périphérie (*edge computing*) ou de manière centralisée (cloud) ;

– **des interactions avec l'environnement** qui peuvent prendre la forme de remontées périodiques d'informations (capteurs environnementaux de suivi de températures, de qualité de l'air ou de suivi des sols pour l'agriculture, par exemple), alimenter un système d'alerte (suivi des paramètres vitaux d'une personne hospitalisée via un tensiomètre ou un appareil d'oxygénation connecté) ou encore nourrir un algorithme pour des prises de décision dans des cas d'usages critiques (véhicule « autonome », appelé maintenant en particulier dans la législation « véhicule à conduite automatisée », opérations chirurgicales à distance).

BRÈVES DU MONDE

Le Chili possède actuellement entre 50 et 60 millions d'objets connectés à Internet pour 19 millions d'habitants. Selon une étude du groupe d'audit et de conseil britannique Deloitte, le Chili serait le pays d'Amérique latine le mieux adapté pour le développement du marché des IdO[1], sur la base d'une comparaison de 33 variables des pays appartenant à l'OCDE et à l'Amérique latine liées à l'infrastructure, la régulation, la capacité d'innovation, la stabilité politique et économique, l'adoption de technologies par les entreprises et le niveau de formation des ressources humaines. Selon une étude financée par la BID (Banque interaméricaine de développement), les trois pays qui connaîtront la plus forte croissance des dépenses en IdO entre 2017 et 2022 se trouvent tous en Amérique latine : le Mexique, la Colombie et le Chili[2].

En Israël, la possible explosion de l'IdO est commentée mais aucun chiffre n'est avancé pour démontrer cette tendance. Seul le ministère des Télécommunications se risque à une estimation de 100 000 connexions par km^2 à terme, sans détailler ce qui relève uniquement de l'IdO.

Au Nigéria, le secteur de l'IdO est en forte croissance, malgré les inégalités d'accès aux solutions numériques et aux réseaux en général à l'échelle du pays. Le secteur y est estimé à 1 milliard de dollars américains en 2025, mais peu de chiffres existent concernant le nombre d'objets connectés aujourd'hui et dans les années à venir.

Au Japon, on compte environ 1 milliard d'objets connectés à Internet – tous objets confondus – en 2021 (contre 800 millions en 2018), dont près de la moitié correspondent à des connexions de machine à machine (M2M) et 194 millions d'objets connectés grâce à une technologie de télécommunication mobile.

Selon le CAICT, un think tank affilié au ministère de l'Industrie et des technologies de l'information qui s'appuie sur les données de GSMA (Global System for Mobile Communications Association), **la Chine** comptait 3,6 milliards d'objets connectés en 2020, soit 30 % des connexions mondiales. Le pays présente un développement avancé en IdO, Shenzhen et Pékin faisant partie des cinq premières villes accueillant les sièges sociaux d'entreprises de plateformes IdO (Tuya, Alibaba Cloud, Baidu IdO Core et Huawei Connection Management Platform).

Source : Direction générale du Trésor. Ces brèves sont extraites des contributions du réseau des services économiques. Une enquête comparative menée auprès de huit pays – Inde, Israël, Chine, Chili, Japon, Nigéria, Finlande et Estonie –, sélectionnés par le comité d'experts en fonction de leur maturité technologique, de leurs caractéristiques socioéconomiques, institutionnelles et politiques, fournit des éclairages thématiques intéressants. Pour un tableau par pays et pour des sources bibliographiques complètes, le lecteur peut se reporter à l'annexe 7.

[1] Deloitte (2018), *IoT para el sector empresarial en América latina*, Centro de Estudios de Telecomunicaciones de América Latina (cet.la), juillet, 250 pages.

[2] Pérez R., Sergio C. et Terry E. (2019), *IoT in LAC 2019: Taking the Pulse of the Internet of Things in Latin America and the Caribbean*, BID.

CHAPITRE 2

L'INTERNET DES OBJETS, COMMENT ÇA MARCHE ?

1. L'architecture : capteurs, réseaux, données et services

L'Internet des objets fait donc référence à un écosystème dans lequel des applications et des services sont pilotés par des données obtenues du monde physique et transmises par des capteurs embarqués dans les objets.

Un dispositif IdO a ainsi la capacité de percevoir son environnement (température, humidité, présence, etc.), de traiter et de transférer les données recueillies dans des applications ou des services (mobilisant notamment des algorithmes d'intelligence artificielle) et enfin d'aider à la prise de décisions – décisions qui, si le dispositif contient des actionneurs, peuvent s'appliquer au monde physique.

Ces dispositifs mobilisent à la fois des équipements physiques (les capteurs), des réseaux de télécommunication (pour la transmission des données), des équipements pour la mémorisation des données, éventuellement des actionneurs et enfin des couches logicielles pour le traitement des informations réparties sur l'ensemble des éléments identifiés.

Nous distinguons quatre couches logicielles qui permettent de décrire une solution IdO dans son ensemble :

- une couche en contact avec les capteurs ou actionneurs de l'objet connecté qui récupère les données acquises et transfère les ordres d'actions (brique « objet connecté ») ;
- une couche réseau qui s'appuie sur un service de télécommunication qui peut selon les contraintes opérationnelles être filaire ou sans fil, et présenter des caractéristiques de débit et de portée qui déterminent les types d'application susceptibles d'être utilisées (brique « réseau IdO ») ;

- une couche jouant le rôle d'intergiciel (Middleware), dédiée au stockage et au traitement des données collectées (couche « plateforme IdO ») ;
- les applications utilisant ces données et fournissant des services, proposées aux utilisateurs finaux (applications IdO).

Le Tableau 3 synthétise les quatre dimensions d'une solution IdO. C'est l'interconnexion de ces différentes briques, qui peut différer selon les cas d'usages, les domaines d'applications, les configurations techniques, les protocoles ou les standards, qui créé un dispositif IdO.

Donnons un exemple : un compteur d'électricité intelligent recueille en temps réel les données relatives à la consommation électrique d'un bâtiment, d'une entreprise ou d'un foyer. Ce compteur communicant transmet les données – par réseau CPL, cellulaire, etc. – au gestionnaire du réseau de distribution qui sur sa plateforme traite ces données en vue de les exploiter pour améliorer sa gestion : relevé de compteurs à distance, mise en service, facturation, maintenance, etc. Les données recueillies, généralement anonymisées, sont ensuite utilisées pour le développement de nouveaux services à l'attention du consommateur. Ces services peuvent relever d'un autre domaine d'application que celui où s'est effectué le recueil de données.

Tableau 3 – les différentes dimensions d'une solution IdO

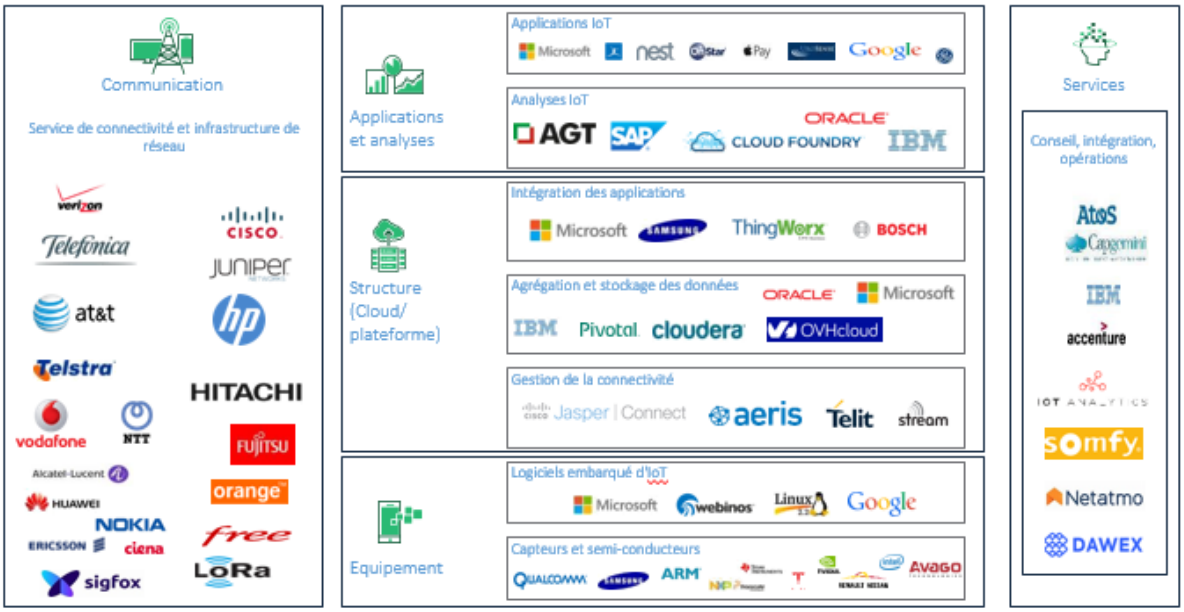
Objets connectés	Réseau IdO	Plateforme IdO	Applications IdO
Logiciel embarqué lié à l'IdO Contrôle et gestion des appareils, analyse des données, exportation	**Infrastructure de réseau** e.g., routeurs, stations	**Support d'applications** Accéder aux données des dispositifs et les manipuler, et établir des API communes pour créer/développer des applications	**Applications commerciales** (e.g., ERP)
Capteurs et semi-conducteurs e.g., capteurs, processeurs, microcontrôleurs	**Service de connectivité** e.g., cellulaire, filaire, satellite, Wifi, réseaux maillés	**Agrégation et stockage des données** Capturer, stocker et sécuriser les données collectées (structurées et non structurées) à partir de la multitude de capteurs	**Applications IdO** Conçues pour des cas d'utilisation IoT spécifiques
Machines connectées (e.g., voiture)		**Gestion de la connectivité** Les logiciels « middleware » aident les « objets » à découvrir, à se connecter et à communiquer. Fournit également une puissance de calcul	**Analytics via IdO** Plateformes horizontales permettant une série d'analyses sur les données capturées

Source : France Stratégie - BCG et EY-Parthenon

1.1. Une multiplicité d'acteurs

Chacune des couches décrites mobilise de multiples porteurs de solutions technologiques hétérogènes, voire non interopérables et s'appuie sur des modèles économiques distincts. La figure ci-dessous montre la pluralité des acteurs susceptibles de proposer des produits pour chaque brique. Ils interviennent à différents niveaux de la solution, mais aucun ne dispose aujourd'hui d'une capacité à contrôler la totalité d'une solution, même si certaines entreprises intègrent plusieurs compétences.

Tableau 4 – Acteurs de l'IdO dans le monde, liste non exhaustive



Note : sont inclus les services de connectivité (par exemple : cellulaire, réseau filaire, satellite, Wifi, réseaux maillés) et les infrastructures de réseau (par exemple : routeurs, stations de base).

Source : France Stratégie - BCG et EY-Parthenon

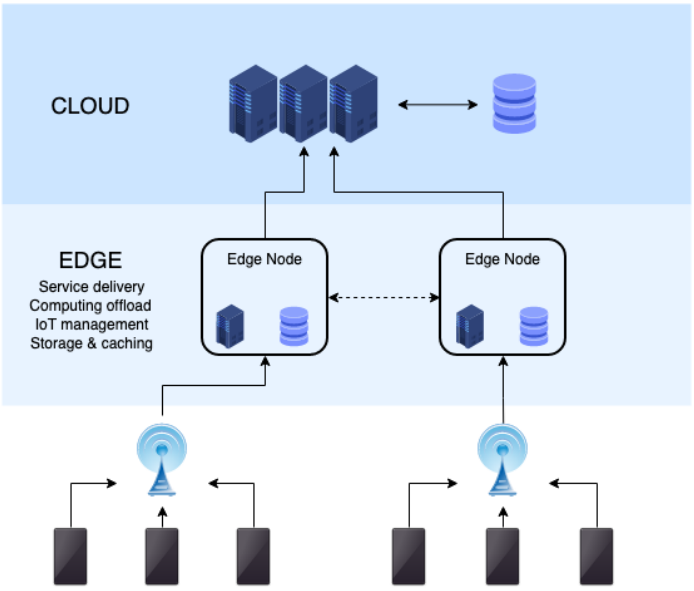
Les opérateurs télécom par exemple peuvent se positionner sur une large partie de la chaîne de valeur – fournisseurs de capteurs, fournisseurs de connectivité sur mesure, accès à une plateforme de données –, mais rarement sur le segment portant sur le traitement des données. Les questions posées par l'IdO n'en doivent pas moins être envisagées dans leur globalité, en tenant compte de l'interconnexion de l'ensemble de ces segments.

Différents acteurs, différents marchés mais aussi différents cadres réglementaires applicables sur chacun de ces segments sont explicités dans la suite du rapport. Ils impliquent des autorités de régulation différentes, dont les compétences peuvent s'exercer en complémentarité ou simultanément.

1.2. Une technologie co-évolutive

Il existe des liens étroits entre l'Internet des objets et le développement d'autres technologies. Ainsi l'IdO s'appuie sur les progrès de technologies connues de longue date qui visent à décentraliser et à distribuer l'informatique (informatique de périphérie ou *edge computing*). Selon l'enquête menée par Microsoft[1] auprès de 3 000 industriels, cette forme décentralisée et distribuée qui contribue à la convergence de ces technologies sera essentielle dans le déploiement à large échelle des solutions IdO.

Graphique 1 – Exemple d'une architecture de réseau d'*edge computing* pour un dispositif d'IdO



Source : NoMore201, CC BY-SA 4.0

Cette architecture permet de disposer de capacités de calcul et de traitement au plus près de la source de données – en l'occurrence les capteurs – en périphérie du réseau et en exploitant des objets intelligents, des téléphones mobiles ou des passerelles réseau pour effectuer des tâches et fournir des services en plus de serveurs centralisés. En déplaçant des services « sur le bord du réseau », il est possible de mémoriser temporairement du contenu et de fournir des services avec de meilleurs temps de réponse et de meilleurs taux de transfert.

De ce fait, le calcul en périphérie réduit les besoins en bande passante et permet de transmettre un nombre réduit d'informations aux centres de traitement centraux (dans le

[1] Microsoft (2021), *IoT Signals*, rapport, 3e éd., octobre.

cloud). Il contribue ainsi à réduire le volume de données à transmettre, les contraintes de charge des réseaux de télécommunication et la consommation énergétique liée à l'activation du transfert, du traitement et du stockage des données dans le *cloud*. Mais il implique le déploiement de nouveaux centres de traitement, eux aussi consommateurs de compétences, d'équipements et d'énergie.

Cette infrastructure décentralisée implique également un modèle décentralisé de confiance : quand on stocke les données à la périphérie, celles-ci sont partagées avec les intermédiaires de stockage.

Parallèlement, l'IdO est essentiel pour le développement d'autres champs importants du numérique, par exemple l'analyse des données massives, le développement de l'apprentissage machine (ML) ou encore l'informatique dite « en nuage ». Ces domaines permettront de traiter et de valoriser les grands volumes de données issus de l'IdO. Le terme « intelligence artificielle des objets » (AIOT) a émergé récemment. D'autres technologies s'interfacent avec l'IdO comme la *blockchain*, la réalité augmentée ou la réalité virtuelle, supports importants des univers virtuels persistants[1].

2. Typologie des réseaux et des usages

Les technologies de communication jouent un rôle clé dans l'IdO. Le service que fournit **le réseau de télécommunications utilisé dans un scénario d'IdO a une incidence importante sur la viabilité de l'application IdO sous-jacente**. Certaines applications peuvent avoir besoin d'une bande passante importante, comme la réalité virtuelle, d'autres nécessitent une durabilité longue, comme les capteurs environnementaux qui ne peuvent être rechargés fréquemment. Le service de communications offert par le réseau se caractérise par le niveau de qualité de service (*Quality of Service*, *QoS*) qui se décline en cinq dimensions : la connectivité, la bande passante, le délai, la fiabilité et la sécurité des communications. Chaque technologie de réseau est à même de fournir un service dans des plages opérationnelles définies selon ces cinq dimensions.

Par exemple, le Wifi fourni une connectivité sans fil avec un débit qui peut monter jusqu'à 150 Mbps sur la bande des 2,4 GhZ, dont la portée est typiquement limitée en extérieur à une centaine de mètres, avec une consommation énergétique relativement élevée de l'ordre de 20 dBm. Quant à lui, le ZigBee peut communiquer avec une puissance de l'ordre de -1 dBm, soit mille fois moins que le Wifi, mais avec une portée d'une dizaine de mètres seulement et un débit de quelques dizaines de kbps. Ces deux technologies utilisent néanmoins des bandes de fréquences non réglementées. Libres d'accès, ces bandes de

[1] https://fr.wikipedia.org/wiki/Métavers

fréquences ont l'inconvénient d'être ouvertes aux interférences d'autres émetteurs diffusant sur le même canal. Elles doivent alors diminuer leur puissance et leur portée, ce qui réduit leur bande passante et leur fiabilité, et augmente leurs délais (car il devient nécessaire de passer par des relais). D'autres technologies utilisent plutôt des bandes réglementées, avec des licences d'utilisation spécifiques octroyées par les pouvoirs publics, ou avec une spécialisation de la bande à un usage particulier (bande radar, par exemple).

Les conditions d'accès aux réseaux hertziens dépendent de l'octroi des autorisations d'utilisation de fréquence (AUF) qui représentent des enjeux économiques importants pour les opérateurs et les acteurs du secteur de l'IdO. Les bandes de fréquences sont des ressources rares et stratégiques et sont, en particulier en France, la propriété de l'État. Pour ce qui concerne les réseaux hertziens, on distingue :

– les fréquences libres utilisées sous un régime d'autorisation générale qui concerne des bandes de fréquences ouvertes à une utilisation libre soumise à des conditions d'utilisation permettant la cohabitation des utilisateurs mais pouvant comporter des risques de brouillage ;

– les fréquences réglementées qui sont attribuées par les régulateurs des télécoms (l'Arcep en France) et dont la gestion est confiée à l'Agence nationale des fréquences radio (ANFR) qui coordonne aussi les usages futurs au niveau international, en particulier en relation avec l'ITU-R[1]. Ainsi, en France, 31 bandes de 10 MHz ont été attribuées aux opérateurs pour le déploiement de la 5G, pour un bénéfice de 2,78 milliards d'euros pour le trésor public.

Les réseaux IdO peuvent utiliser des fréquences régies par ces deux modes de gestion.

Les perspectives de développement de l'IdO, aussi bien en termes de croissance du nombre d'objets à connecter, qu'en termes de débit de données à transporter et finalement d'exposition aux ondes électromagnétiques, rendent nécessaire une gestion efficace de la bande passante hertzienne qui est une ressource coûteuse pour les opérateurs de service IdO et qui y allouent d'importantes ressources. En particulier, la gestion des paramètres du réseau comme l'efficacité spectrale, le nombre de bits transmis par Hz de bande passante, la puissance d'émission, qui contrôle la portée et le niveau d'interférence, la densité d'émetteurs, qui définit le nombre d'objets de l'IdO qui peuvent être connectés dans une même zone géographique, sont des critères qui permettent d'assurer un service de communications fiable et efficace à grande échelle.

Enfin, on peut différencier les réseaux utilisés pour l'IdO selon la présence ou non d'une infrastructure de communications sous-jacente. Selon qu'elles sont filaires ou sans fil

[1] Secteur des radiocommunications de l'Union internationale des télécommunications basée à Genève.

(hertziennes ou satellitaires, etc.), les technologies réseaux utilisées répondent plus spécifiquement au déploiement de telle ou telle application de l'IdO. Par exemple, la 5G a été conçue avec une infrastructure permettant de multiplier par dix la bande passante par connexion et de réduire la latence à quelques millisecondes, pour répondre à des besoins d'usages précis, comme la mise en œuvre d'application dites « critiques ».

Techniquement, les dispositifs d'IdO peuvent donc utiliser :

– des réseaux satellitaires qui utilisent des bandes de fréquences licenciées et qui offrent de la connectivité à de larges zones géographiques sans le support d'infrastructures terrestres ;

– des réseaux longue portée qui utilisent des fréquences libres telles que les solutions proposées par l'Alliance Lora ou l'entreprise Sigfox ;

– les réseaux locaux de courte portée dont les protocoles les plus connus sont le Wifi, le Bluetooth ou encore la RFID qui se déploient sur des licences libres dans des fréquences non-réglementées ;

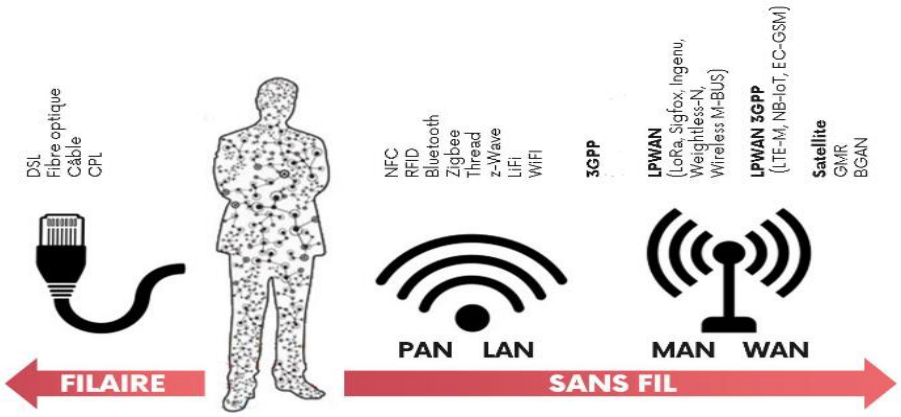
– des offres spécifiques pour l'IdO proposées par des opérateurs à l'attention des entreprises et industriels : Bouygues Télécom a axé sa communication autour de LoraWan mais propose également du LTE-M, depuis peu Orange propose la technologie LTE-M et LoraWan et SFR propose son offre NB-IOT ;

– les technologies filaires comme le xDSL[1], le câble coaxial ou encore la fibre, qu'il ne faut pas négliger. Ces technologies sont essentielles pour fournir la colonne vertébrale (*Backbone*) de l'infrastructure de connectivité globale que constitue l'IdO et pour permettre la mise à l'échelle de cette infrastructure, avec la croissance des volumes de trafic à transporter pour l'IdO ;

– les réseaux hertziens 2G, 3G, 4G, 5G et dans l'avenir 6G déployés par les opérateurs sur des bandes de fréquences licenciées. Les opérateurs peuvent également proposer des offres spécifiques pour l'IdO à l'attention des entreprises et industriels.

[1] La technique DSL consiste à découper la bande de fréquence disponible sur la ligne en deux voies – une pour la voix et l'autre pour les données, dont la plus connue est l'ADSL pour *Asymmetric Digital Subscriber Line*, xDSL est l'acronyme de groupe qui regroupe toutes les variantes de la DSL : ADSL, SDSL, etc.

Graphique 2 – Typologie des réseaux utilisables pour l'Internet des objets



Note : 3GPP comprend les réseaux cellulaires 2G, 3G, 4G et 5G

Source : Arcep

2.1. Différentes qualités de réseaux pour différents usages

Ces réseaux offrent des qualités techniques qui répondent aux différents besoins de déploiement des solutions IdO.

Les réseaux sur bandes licenciées

Sur les réseaux 2G et 3G on observe un débit plus faible qu'en 4G ou 5G, mais une plus grande autonomie des équipements. La 4G présente de forts débits mais une consommation électrique plus importante[1]. **L'utilisation de ces réseaux permet des garanties d'interopérabilité à l'échelle européenne et mondiale**, basée sur les accords de *roaming*.

Enfin, au-delà des réseaux grand public, certains acteurs industriels se dotent de réseaux cellulaires privés qui permettent des cas d'usages ciblés, le plus souvent liés aux objets communicants et qui facilitent notamment la maîtrise, la résilience et la sécurité du réseau. L'Arcep a ouvert un guichet d'attribution de fréquences pour ces réseaux privés 4G.

Les réseaux longue portée sur bande libre

Beaucoup de solutions IdO s'appuient sur des technologies de **type LPWAN[2],** proposées par Sigfox ou Lora sur les bandes de fréquences libres qui se distinguent notamment **par une**

[1] Précision apportés lors de l'audition de l'Arcep 18 novembre 2021.

[2] *Low Power Wide Area Network* (« basse consommation et longue portée »).

couverture très étendue (5 km à 40 km en espace ouvert, bonne pénétration en intérieur) mais qui offrent des débits faibles (moins de 100 bit/s) et des temps de latences élevés. Ces solutions consomment peu d'énergie (la durée des batteries utilisées peut aller jusqu'à dix ans) et de faibles coûts de déploiements (moins de 2 dollars par chipset radio).

Les solutions déployées sur des fréquences libres peuvent être sujettes à des conditions d'utilisation dégradées en l'absence de protection contre le brouillage. En outre, elles présentent des lacunes en matière d'interopérabilité : Lora et Sigfox par exemple ne sont pas interopérables. Par ailleurs, selon les pays où opèrent ces réseaux, les bandes de fréquence dites libres ne sont faciles d'accès : c'est le cas de la Chine où l'accès aux bandes libres peut présenter un frein dans le déploiement de ces solutions[1].

En réponse à la concurrence des réseaux LPWAN bandes libres, les opérateurs de réseaux cellulaires ont développé des **standards, le NB-IoT et le LTE-M, spécialement conçus pour développer l'IdO sur leurs réseaux mobiles. Ces deux normes ont été conçues pour être compatibles avec la 5G**. NB-IoT et LTE-M ont plusieurs similarités et présentent sensiblement les mêmes avantages, comme celui de fonctionner avec peu d'énergie, mais **ils diffèrent par leur débit et leur latence**. La technologie LTE-M présente une consommation énergétique faible et peut être utilisée pour des applications dans le domaine de la sécurité (usage de caméras, surveillance, etc.), du transport, du *tracking*, du suivi médical, etc. Le NB-IoT présente des débits supérieurs, une latence un peu moins performante et une très faible consommation d'énergie. Ces caractéristiques permettent l'utilisation de ces réseaux pour le déploiement de compteurs intelligents, les parcmètres, ou encore des capteurs pour effectuer des contrôles agricoles, pour le *smart grid*, pour la *smart city*. Ces deux technologies permettent des usages qui nécessitent une bonne pénétration au sein des bâtiments.

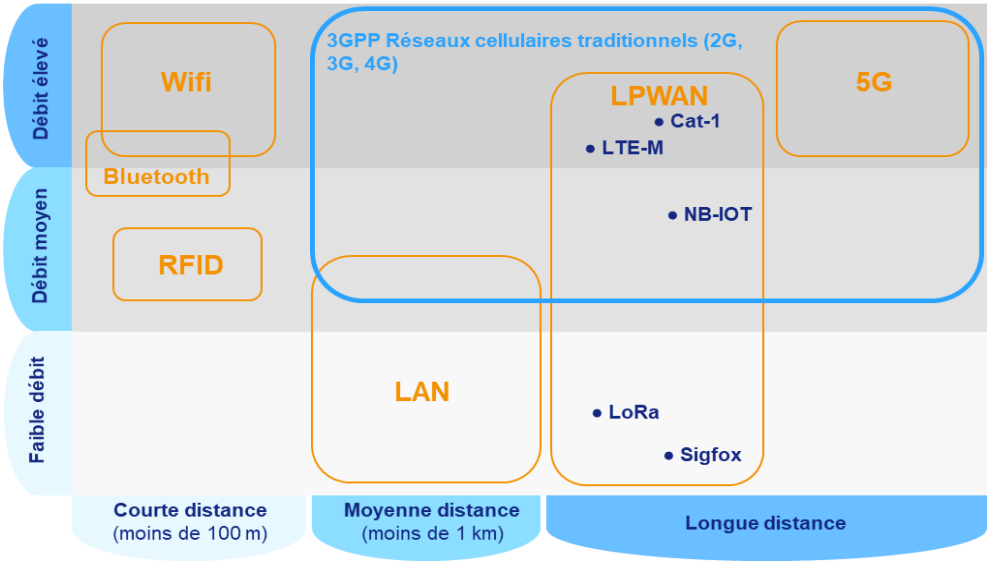
Les réseaux de courte portée

Les dispositifs IoT à plus courte distance (Wifi, Bluetooth, Zigbee, RFID, NFC, Z-Wave) sont les technologies utilisées pour acheminer les services dans les « derniers mètres » et sont répandus dans les cas d'usages dit « grand public » pour des applications telles que les systèmes d'alarme, les implants médicaux, les télécommandes, certaines applications de radiolocalisations industrielles ou médicales, les talkie-walkies et microphones amateurs, DECT, etc. Ils utilisent majoritairement le Wifi ou le Bluetooth[2].

[1] La décision 2021-1589 de l'Arcep en date du 29 juillet 2021 sur les dispositifs à courte portée, en cours d'homologation par le gouvernement, vise notamment à ouvrir des bandes de fréquences, pour élargir le champ des applications LPWAN.

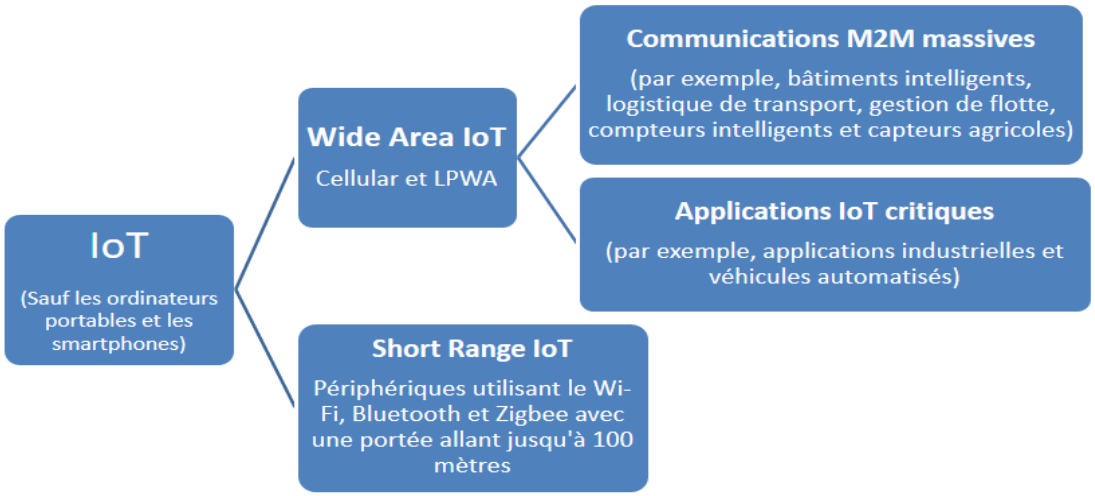
[2] Wifi : bande ISM 2,4 GHz et 5 GHz, en attendant l'homologation Wifi6 et la décision pour l'utilisation de la bande 6 GHz.

Graphique 3 – Synthèse de la typologie des réseaux utilisés pour l'IdO selon leur portée et les débits permis



Source : France Stratégie

Graphique 4 – Synthèse de la taxonomie (sous-catégories) de la mesure d'IdO de l'OCDE, avec les usages associés de l'IdO, selon les typologies d'usage



Source : comité de la politique de l'économie numérique (CPEN), OCDE (2018), op. cit.

Les réseaux satellitaires

Le marché mondial satellitaire est en pleine transition et on assiste à un engouement pour des **satellites de télécommunications bas débits et les projets de constellations ciblant particulièrement le marché de l'IdO** se multiplient. La constellation Starlink est disponible en France depuis mai 2021 et des acteurs français sont présents sur ce marché avec des acteurs comme Kineis ou Eutelsat (Leo).

Encadré 2 – L'offre satellitaire Eutelsat

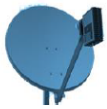
LEO for Objects (ELO) servira à évaluer les performances d'un satellite en orbite basse (LEO pour Low Earth Orbit) pour l'échange de données à bas débit des objets. L'opérateur s'appuiera notamment sur la technologie de Sigfox, qui possède un réseau terrestre mondial bas débit unique dédié à l'Internet des objets. L'orbite basse est particulièrement bien adaptée à la connectivité bas débit des objets car elle offre un lien satellite disponible en tout point du globe, complémentaire des réseaux IdO terrestres, sans impact ni sur le coût ni sur la consommation énergétique des objets en phase usage. ELO pourra ainsi rapatrier des informations concernant des objets situés dans les zones non desservies par les réseaux terrestres, ainsi qu'offrir une redondance sur la couverture terrestre existante (*Source : site Eutelsat).*

Graphique 5 – Les offres satellites opérables avec des dispositifs IdO – non exhaustif

La société française EUTELSAT propose un portefeuille de solutions de connectivité par satellite répondant à différents besoins IoT.

Les offres satellites ont un bilan environnemental généralement meilleur que les offres 4G ou 5G.

Il y a de fortes différences entre les différentes offres satellitaires. À noter que les offres Orbites basses (LEO) ne sont pas encore disponibles alors que celles géostationnaires (GEO) le sont.

VSAT — Disponible	IoT FIRST — Disponible	ELO — 2022
 	 	
• Service managé de connectivité IP • Créé pour le haut-débit • Idéal pour connecter des assets fixes nécessitant de transférer des gros volumes de données à haute vitesse • Prix indicatifs – Terminal satellite : ~500-1000 € – Abonnement mensuel : 50-150 € • Exemples de cas d'usage Superviser un parc d'éoliennes ou photovoltaique, connecter un SCADA ou une caméra de surveillance	• Service managé de connectivité IP • Créé spécifiquement pour l'IoT • Idéal pour connecter des assets fixes ne nécessitant pas de haut debit, qui transfèrent de faibles quantités de données • Prix indicatifs 3-5x moins cher que le VSAT, (même niveau de prix que le cellulaire) • Exemples de cas d'usage Connecter un station météo isolée, monitorer et contrôler un équipement d'un réseau d'eau ou d'électricité	• Service manage de connectivité LoRaWAN (non-IP) • Créé spécifiquement pour l'IoT LPWA • Idéal pour complémenter la couverture des réseaux LoRaWAN existants • Prix indicatifs 10x moins cher que les services satellitaires comparables (même niveau de prix que LoRaWAN) • Exemples de cas d'usage Monitorer la verticalité d'un poteau électrique, monitorer le niveau d'eau d'un bassin

Source : Arcep, audition du 18 novembre 2021

Les technologies satellitaires répondent **aux besoins de mobilité ou sur des espaces mal couverts par les autres technologies** et sont particulièrement utilisées dans le monde de la logistique, des transports terrestres et maritimes, environnement ou agriculture. Les premiers satellites de tests français sont déjà en orbite (Leo, Kineis) mais les services finaux devront attendre le lancement des constellations courant 2022. Ces offres satellitaires sont souvent conçues en complément d'offres « terrestres ». Kineis par exemple travaille à une meilleure interopérabilité avec la norme Lora. Les enjeux en matière de transmission sont considérables, d'un point de vue industriel mais aussi social et environnemental.

2.2. Les effets attendus de la 5G

La cinquième génération de réseaux sans fil, la 5G, s'inscrit dans le processus d'évolution des générations précédentes de réseaux sans fil (2G, 3G et 4G). Elle peut cependant représenter un changement de paradigme, car il s'agit de la première norme conçue dans l'optique de l'Internet des objets, où les appareils connectés ont des exigences diverses en matière de réseau[1]. La 5G est une norme « parapluie » c'est-à-dire intégrant d'autres normes (par exemple NB-IoT ou LTE-M) et conçue pour permettre la connexion massive d'objets en répondant simultanément à la diversité des usages de l'IdO avec trois classes de services :

- la capacité à supporter un nombre massif d'objets connectés (mMTC pour *massive Machine Type Communications*) et de répondre aux usages et services qui permettent de communiquer machine à machine (M2M) et de lever certaines des limites posées par d'autres technologies de communication, notamment les réseaux non cellulaires ;
- la capacité à connecter des objets nécessitant des débits importants et à très hauts débits (eMBB pour *enhanced Mobile Broadband*) ;
- pour les usages critiques à très faible latence et très haute fiabilité (URLLC pour *Ultra Reliable Low Latency Communications*).

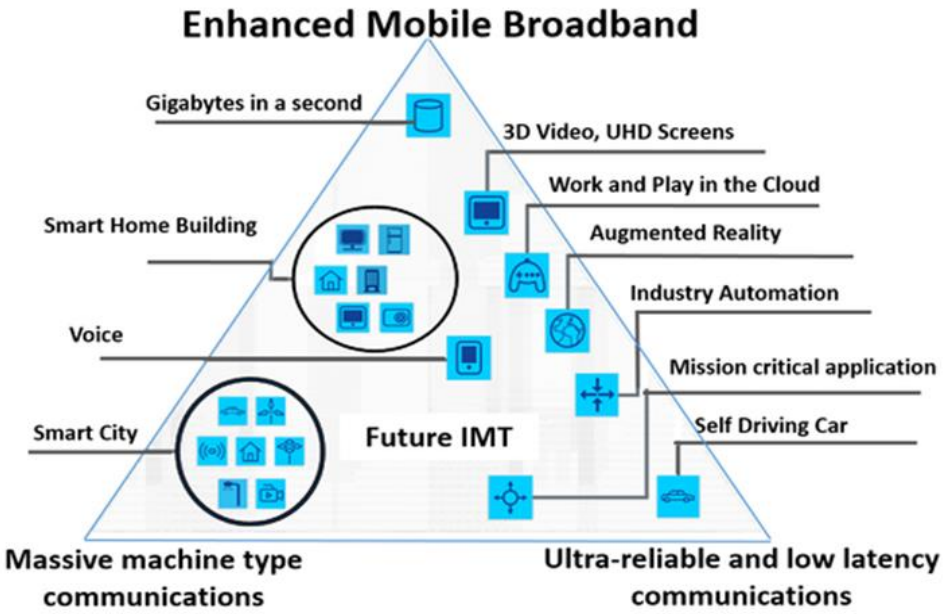
En regard des autres réseaux, la promesse de la 5G tient dans sa capacité à rendre possibles des solutions unifiées en faisant converger les autres technologies, les réseaux cellulaires 3GPP (2G, 3G, 4G) mais aussi les réseaux non 3GPP (Wifi, Sigfox et Lora, etc.). Les possibilités offertes par le « *slicing* » c'est-à-dire la possibilité de diviser pour répartir et contrôler, répondent particulièrement bien aux besoins des industriels, en permettant de distinguer différentes instances (tranches) du réseau qui pourront être dédiées à des offres de services sur mesure et différentes applications d'IdO.

[1] OCDE (2019), *The Road to 5G Networks. Experience to Date and Future Developments*, OECD Digital Economy Papers, n° 284, Paris, Publications de l'OCDE.

En France, le déploiement de la 5G est largement engagé, les licences pour la bande 3,5 GHz viennent d'être accordées aux opérateurs, avec des trajectoires de déploiement qui visent à installer près de 10 500 sites d'ici 2025, y compris dans les zones peu denses. Les premiers services commerciaux ont été déployés, mais dans un premier temps les déploiements de la 5G se font dans des architectures « non autonomes » (ou non *Stand alone*[1]) et s'appuient donc sur la coexistence avec des réseaux 3G/4G. Ce déploiement permet surtout de privilégier l'augmentation des débits. La cohabitation de ces différents réseaux est nécessaire mais elle complique le déploiement de la 5G, dont les configurations optimales ne seront opérationnelles qu'à partir de juillet 2026.[2]

Mais c'est l'ouverture de la bande millimétrique 26 GHz – attendue d'ici deux ou trois ans – qui devrait permettre les cas d'usages les plus prometteurs pour l'IdO. Selon le Comité stratégique de filière précité, les bandes millimétriques, vont permettre le développement de cas d'usage dans l'industrie, la santé, les villes. La 5G permettra le développement de la réalité virtuelle, des vidéos très haute définition, de la réalité augmentée, mais aussi des applications critiques (véhicule à conduite automatisée) et enfin des applications nécessitant de larges transmissions de données et des besoins croissants de bandes passantes.

Graphique 6 – Scénarios des usages de la 5G dans l'IdO



Source : ITU-R IMT-2020. Audition OCDE, novembre 2021. Voir aussi OCDE (2019), op. cit.

[1] C'est-à-dire s'appuyant sur les infrastructures des réseaux 4G déjà déployées.

[2] Conseil national de l'industrie (2020), *Contribution et éclairage du CSF Infrastructures numériques sur la question environnementale associée au numérique et à la 5G*, septembre.

À la suite d'un appel à projets lancé en 2019, l'Arcep autorise des acteurs à exploiter des plateformes d'expérimentation 5G ouvertes en bande 26 GHz[1]. Sur l'ensemble des expérimentations, le tableau de bord des expérimentations 5G de l'Arcep recense neuf projets concernant des applications d'IdO. Toutefois, à date, les résultats ne sont pas consultables et les informations relatives à des cas d'usages concrets restent limitées[2].

Dans son livre blanc[3], le *Comité stratégique de filière infrastructures numérique* souligne d'ailleurs que toutes les conditions nécessaires au déploiement optimum de la 5G ne sont pas encore réunies et identifie les principaux freins qui restent à lever :

– la maturité technologique de la 5G (une nouvelle version release 17 est attendue en décembre 2021) et des efforts importants sont encore attendus en termes de standardisation pour les cinq à dix prochaines années ;

– La nécessité de développer un « écosystème » favorable à son développement, et notamment l'adoption par les PME ou les acteurs verticaux et la nécessité pour cela de disposer de pilotes et d'expérimentations plus nombreux ;

– la coexistence et la synchronisation des réseaux 5G et des réseaux cellulaires ;

– les risques cyber qui restent importants.

2.3. Complémentarité et subsidiarité des réseaux télécom pour répondre aux multiples usages de l'IdO

Les caractéristiques techniques des réseaux – débit, consommation énergétique, couverture, latence – permettent de répondre aux différents cas applicatifs de l'IdO et de couvrir un large spectre d'usages. Le Tableau 5 ci-dessous présente une synthèse des principales caractéristiques des réseaux et des usages de l'IdO qui peuvent y être associés.

L'Observatoire des marchés de l'Arcep[4] constate que les technologies hertziennes mobiles qui ont connu une forte croissance entre 2016 et 2019 stagnent aujourd'hui alors que les technologies Sigfox et LoRa (Orange, ByT) connaissent une forte croissance depuis un an.

Au niveau mondial, CISCO confirme cette tendance et prévoit d'ici 2023 une croissance de 14 % du total des connexions sur les réseaux LPWAN. CISCO estime que les connexions

[1] À la date de la rédaction du rapport. Le tableau de bord est disponible sur le site de l'Arcep.

[2] *Le Monde* (2021), « Téléphonie mobile : espoirs, promesses et doutes autour de la 5G », par A. Sénécat, 24 octobre.

[3] Conseil national de l'industrie et CSF Infrastructures numériques (2020), *5G : stratégie et enjeux*, Livre blanc, septembre.

[4] Audition du 18 novembre 2021.

M2M mobiles étaient de 1,2 milliard en 2018, et qu'elles devraient atteindre près de 3 milliards en 2023, dont près de la moitié seraient connectées via les réseaux 4G et 5G[1].

Tableau 5 – Synthèse des caractéristiques des réseaux et des usages de l'IdO associés

	LPWAN*	Cellular	Lan**
	Technologies spécialisées dans l'IoT à faible consommation	Cellulaire traditionnel et 5G	Technologies à courte portée
Consommation d'énergie au niveau du capteur	Faible	Élevée	Basse à élevée
Débit (vitesse)	Bas (<200 kbps)	Élevé	Moyen à élevé
Coût relatif	Moyen	Coûteux	Coûteux
Maturité	Émergent	Très établi	Très établi
Opérateurs	Opérateurs de réseaux mobiles Spécialistes de l'IdO (ex. Sigfox)	Opérateurs de réseaux mobiles	N/A
Exemples de cas d'usage	Compteurs intelligents, suivi des colis et des expéditions, surveillance des sols et des cultures (hors drones)	Vidéosurveillance, gestion dynamique du trafic	Objets connectés de la maison (assistants virtuels, jouets, balance, etc.)

* Réseau étendu à faible consommation (par exemple Sigfox, LoRa, NB-IoT, LTE-M)

** Réseau local (par exemple, Wifi, Bluetooth)

Source : France Stratégie - BCG et EY-Parthenon

Tableau 6 – Nombre de connexions sur les réseaux, en France

Technologie	Nombre d'objets connectés
Cellulaire (2G à 5G, LTE-M et NB-IoT)	23 millions d'objets
LPWan (Sigfox et LoRa, etc.)	1,9 million d'objets + 25 % en un an

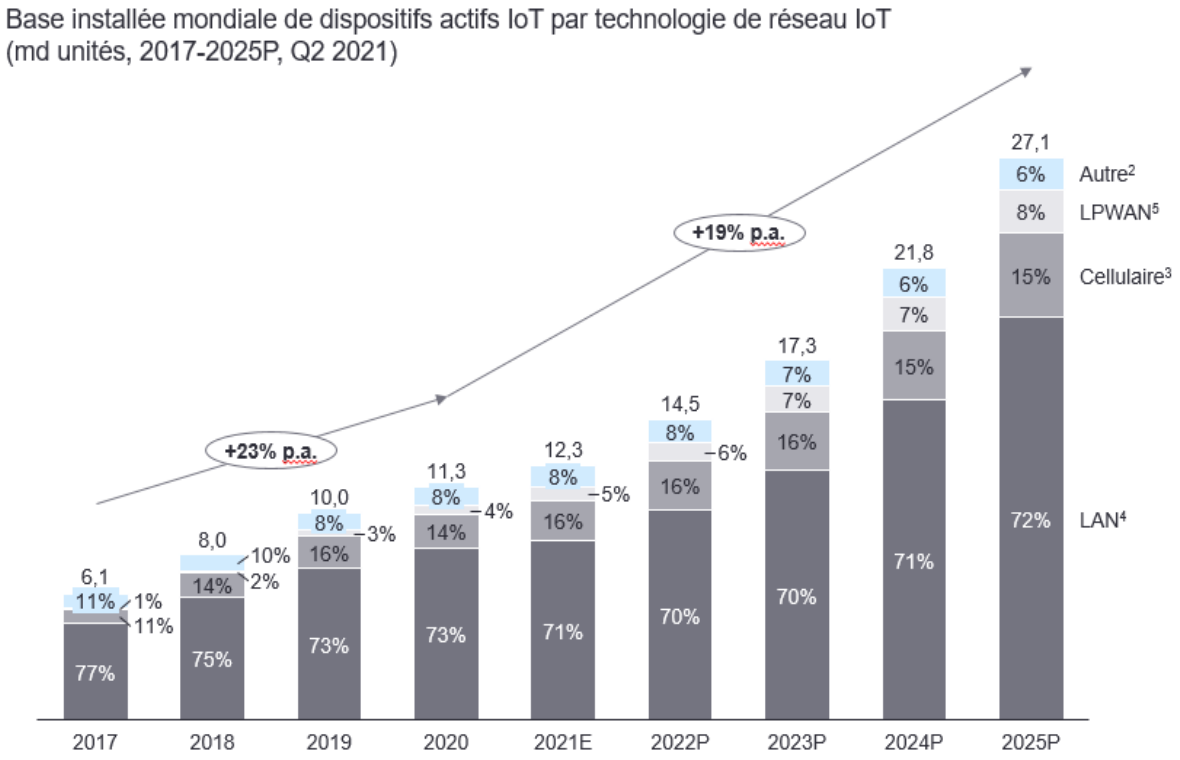
Source : France Stratégie, données Arcep

[1] Cisco Systems fabrique, développe et vend des logiciels, du matériel réseau, des produits de haut technologie et des équipements de télécommunication.

Les projections de déploiement de l'IdO (voir Graphique 7) montrent que les connexions sur des réseaux LPWan gagnent du terrain. Elles devraient connaître une accélération d'ici 2025, notamment en raison de leurs caractéristique techniques (longue portée, faible coût). La part relative des autres technologies devrait se modifier, laissant les technologies cellulaires (2G, 3G, 4G et 5G) à 15 % de la part des réseaux utilisée pour des applications de l'IdO.

Graphique 7 – Estimation de l'évolution de l'utilisation des réseaux de télécommunication pour l'IdO, horizon 2025

Dispositifs actifs[1] – Taux de croissance annuel moyen			
	2017-2020	2020-2023	2023-2025
Autres	+ 10 %	+ 11 %	+ 12 %
LPWAN	+ 86 %	+ 40 %	+ 31 %
Cellulaire	+ 36 %	+ 20 %	+ 20 %
LAN	+ 21 %	+ 13 %	+ 27 %



(1) Ne comprend pas les ordinateurs, les ordinateurs portables, les téléphones fixes, les téléphones cellulaires ou les tablettes. Sont comptés les nœuds/dispositifs actifs ou les passerelles qui concentrent les capteurs finaux, et non chaque capteur/actionneur. Les technologies de type (RFID, NFC) ne sont pas prises en compte.

(2) Satellites, réseaux propriétaires non classifiés de toute portée et réseaux câblés

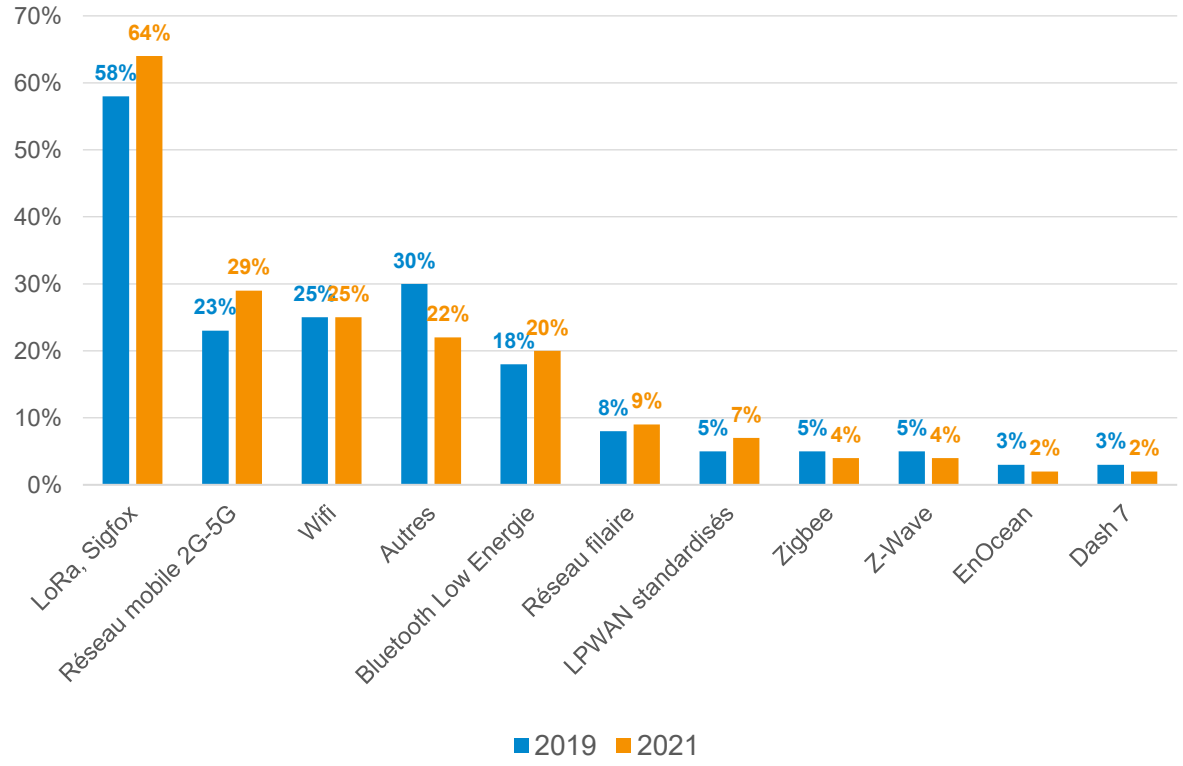
(3) Cellulaire traditionnel (2G, 3G, 4G) et 5G

(4) Réseau local (par exemple, Wifi, Bluetooth)

(5) Réseau étendu à faible consommation (par exemple Sigfox, LoRa, NB-IoT, LTE-M)

Source : BCG et EY-Parthenon, d'après IoT Analytics (2021), State of IoT*, rapport, septembre, p. 18*

Graphique 8 – Connectivité IdO selon les type de réseaux, en pourcentage des projets utilisant ces technologies en 2021



Note : LPWAN standardisés correspond à NB-IoT et LTE-M.

Source : Garcia-Montero C. (2022), « Marché de l'IoT en France : tous les chiffres », Journal du Net*, 4 février, à partir des données de Statista*

Il **existe donc une large complémentarité** entre les différentes caractéristiques des réseaux qui répondent à une très large panoplie d'usages. Mais le foisonnement des technologies peut conduire à une redondance d'offres sur des cas d'usages et **restreindre l'interopérabilité entre ces réseaux, qui n'est pas totalement acquise aujourd'hui** puisque certaines de ces technologies sont fermées et d'autres fonctionnent sur des standards ouverts.

Enfin, il en découle une **forte concurrence entre acteurs,** qui peuvent intervenir sur les mêmes segments de marché, notamment dans les applications industrielles – marché concurrentiel au sein duquel les offres 5G vont devoir s'inscrire.

BRÈVES DU MONDE

Au Chili, le développement du réseau mobile 5G n'est prévu par le gouvernement que sur le long terme. Il existe aujourd'hui cinq projets pilotes pour évaluer l'utilisation de la 5G, mis en place dans le cadre du programme « Observatorio 5G »[1].

En Finlande, l'entreprise Wirepas[2] dit avoir la première technologie de connectivité 5G non cellulaire[3] au monde pour l'IdO d'entreprise qui fonctionne sur des fréquences gratuites. Cette 5G non cellulaire et non opérée entend répondre aux besoins des réseaux IdO à très forte densité avec un coût modique et une empreinte environnementale réduite[4].

En Finlande encore, Connected Finland[5] offre un réseau mobile national conçu uniquement pour l'Internet des objets. Le réseau fait partie de l'écosystème mondial Sigfox[6] (français) et Connected Finland agit en tant qu'opérateur local exclusif. Sigfox atteint 90 % des Finlandais et la zone de couverture du réseau sera encore étendue.

Au Japon, le développement de l'IdO repose principalement sur les technologies suivantes. S'agissant de l'IdO en temps réel et haut débit, les cas d'usage s'appuient presque uniquement sur la 5G. S'agissant de l'IdO de masse s'appuyant sur des technologies LPWAN, de nombreux cas d'usage voient le jour : logistique et gestion de chaînes d'approvisionnement, monitoring d'équipements (notamment compteurs de gaz et d'eau). Les technologies LPWAN au Japon sont les suivantes : Sigfox, ELTRES, LoRa.

En Inde, selon les dernières estimations, la 5G ne devrait pas être lancée avant mi-2022, voire 2023. Toutefois, les principaux opérateurs téléphoniques ainsi que de grandes entreprises et des PME ont déjà lancé des solutions IdO. Tata Communications a développé un réseau dédié à l'IdO reposant sur la technologie LoRaWAN, couvrant 40 villes et 219 millions de personnes en juin 2019. En avril 2021, le deuxième opérateur téléphonique Bharti-Airtel a lancé Airtel IoT, une plateforme intégrée permettant de connecter et de contrôler des objets connectés en grand nombre.

En Chine, en matière d'infrastructures de télécommunications, plusieurs projets locaux voient le jour. Mi-2020, la ville de Shenzhen a annoncé avoir réalisé une couverture complète avec 46 000 stations de bases 5G *stand alone*, une avance qui pourrait favoriser le déploiement de l'IdO[7].

---

[1] www.subtel.gob.cl/observatorio5g/

[2] www.wirepas.com/

[3] Norme ETSI TS 103 636 series, plus connue sous l'appellation DECT-2020 NR

[4] Coutance P. (2021), « La 5G non cellulaire et non opérée de Wirepas obtient la certification de l'UIT », *VIPress.net*, 21 octobre.

[5] Voir sur le site de Connected Finland.

[6] Sigfox est le plus grand écosystème IoT au monde et est déjà disponible dans 75 pays.

[7] Lee J. (2021), « The Connection of Everything: China and the Internet of Things », *Merics.org*, 24 juin.

De projets de *smart cities* d'envergure, à l'instar du City Brain d'Alibaba à Hangzhou se développent. En particulier, la ville de Wuxi, dans la province du Jiangsu, cherche à se positionner sur l'ensemble des maillons nécessaires à l'IdO (puces, capteurs, réseaux de communications), pour des applications dans les véhicules connectés, les transports intelligents et les villes intelligentes. Elle accueille ainsi depuis 2009 une zone de démonstration de réseaux de capteurs, dont le développement a dès 2012 fait l'objet d'un plan du MIIT, ainsi que la ville IdO Hongshan, lancée en 2017 avec Alibaba (plateforme Feifeng, solution PAAS). En ligne avec la politique industrielle chinoise, l'objectif est de s'appuyer sur l'écosystème de Wuxi pour faire émerger le secteur IdO d'abord à Wuxi puis au niveau national. D'autres zones tentent de se positionner sur l'IdO (Yangzi River Delta), un développement à nouveau encouragé par le **plan triennal** du MIIT (2021-2023). Enfin, la Chine privilégie pour son LPWAN le NB-IoT. Plusieurs projets de China Unicom, China Telecom et Huawei déploient le NB-IoT pour leurs solutions de villes intelligentes – une technologie de plus en plus utilisée (90 % des connexions chinoises utilisant le NB-IoT).

Source : Direction générale du Trésor ; pour un tableau par pays et des sources détaillées, voir annexe 7

CHAPITRE 3

CHIFFRES ET PERSPECTIVES EN FRANCE ET DANS LE MONDE

1. Les limites des indicateurs statistiques

Dans ce rapport, l'Internet des objets est présenté comme un écosystème où des objets connectés communiquent via Internet, transmettent des données grâce à des capteurs et peuvent agir sur leur environnement s'ils intègrent des actionneurs. Ces données qui transitent via des réseaux filaires ou non filaires – y compris satellitaires –, peuvent en outre être stockées, traitées et faire l'objet d'analyse notamment avec des technologies d'intelligence artificielle. Dès lors, et compte tenu de cette grande diversité de l'écosystème, comment mesurer l'IdO ? Malgré plusieurs années de développement, cette mesure de l'IdO, en particulier dans la statistique publique nationale et internationale, reste à un stade embryonnaire. Au-delà de la diversité de l'écosystème, cette situation s'explique par plusieurs facteurs.

L'absence de définition harmonisée au niveau international

Au début des travaux au niveau international, sous l'égide de l'OCDE, la définition de l'IoT était mouvante. Il s'agissait en effet de fournir des éléments pour éclairer la politique publique et les discussions sur les sujets de régulation. La définition telle qu'elle a été présentée notamment dans le rapport de l'OCDE en 2015[1] ne permettait pas une collecte systématique et selon des normes de la statistique publique. Des travaux exploratoires ont été menés en 2018 et ont tenté de définir quelques indicateurs de mesures de l'IdO, par l'OCDE[2] et par la CNUCED (rapport 2021, voir paragraphe suivant). Plus récemment, des travaux ont été relancés au niveau de l'OCDE dans le cadre du Comité de la politique de

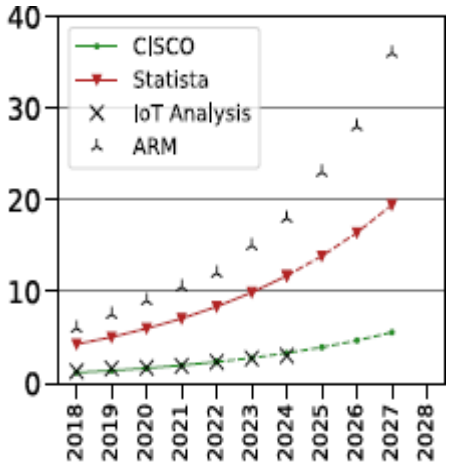
[1] OCDE (2015b), *Digital Economy Outlook 2015*, Paris, Publications de l'OCDE, juillet.

[2] OCDE (2018), *IoT Measurement and Applications*, *op. cit*.

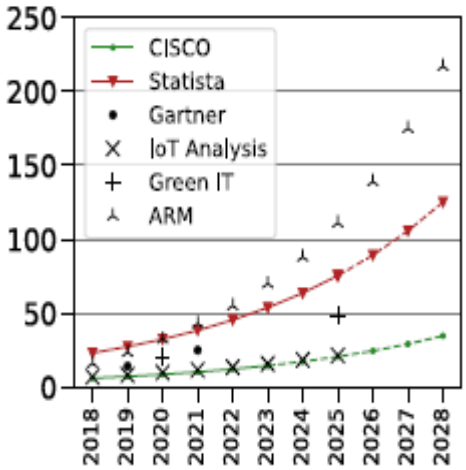
l'économie numérique de l'OCDE pour approfondir la question de la mesure de l'IdO[1]. Au niveau des pays, il y avait très peu de collectes de données dans ce domaine par les institutions statistiques. Seules certaines données issues des institutions de régulation ou d'organismes spécialisés sont publiés – notamment le nombre de cartes SIM et de numéros de téléphone portable destinés aux communications entre machines, ou l'estimation du nombre de brevets déposés (notamment par l'Organisation mondiale de la propriété intellectuelle). Cela explique le développement de données et d'indicateurs statistiques produits par des cabinets privés (Stastita, IoT Analytics, Gartner, IDC, etc.) et par des entreprises (CISCO, Microsoft, etc.). Si les périmètres retenus par ces institutions se traduisent par des écarts importants dans les estimations, les évolutions constatées concordent à souligner le très fort développement des objets connectés.

Graphique 9 – Variation des estimations de développement de l'IdO dans le monde, en milliards d'objets

Rythme de l'évolution annuelle



Perspectives du nombre d'objets cumulés



Lecture : selon la source considérée, en 2025, le nombre d'objets connectés pourrait augmenter entre moins de 10 milliards jusqu'à plus de 25 milliards, ce qui donne un total cumulé à moins de 50 milliards pour la fourchette basse et à plus de 200 milliards pour la fourchette haute.

Source : Pirson T. et Bol D. (2021), « Assessing the embodied carbon footprint of IoT edge devices with a bottom-up life-cycle approach », Journal of Cleaner Production*, vol. 322, novembre*

Les difficultés du décompte

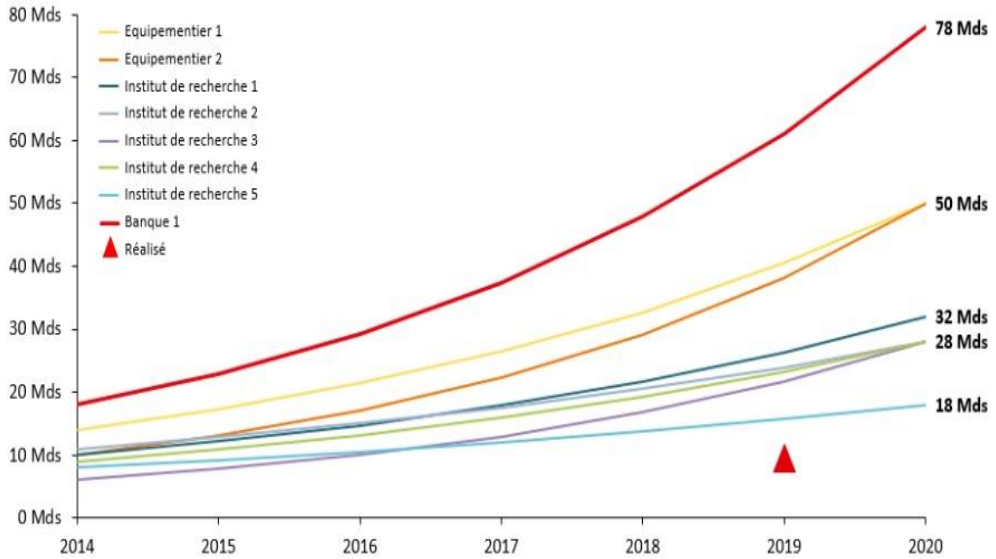
Donner un ordre de grandeur de l'IdO et de son développement dépend étroitement de la définition même de ce qu'est un objet connecté. Les périmètres diffèrent à tel point que les écarts entre estimations varient en milliards d'objets. Par exemple, l'OCDE qui incluait

[1] OCDE (2019), *The Road to 5G Networks…*, *op. cit.*

dans ses premiers travaux les smartphones, les tablettes et les ordinateurs les exclut dans ses travaux récents. De même, les étiquettes d'identification par radiofréquence ou RFID sont prises en compte dans certaines estimations, mais l'OCDE ne considère que les RFID constituant une composante d'un système IdO. Autre exemple, les télévisions dites intelligentes ou Smart TV ne sont pas systématiquement incluses dans les estimations présentées par les instituts privés. Dans le domaine de la logistique, si au début, on comptabilisait les grands ensembles (voitures de livraison connectées, bateaux connectés, etc.), aujourd'hui les connexions sont comptabilisées à un niveau plus fin – au niveau des conteneurs, voire des colis.

Par ailleurs, les objets connectés peuvent communiquer selon des réseaux filaires ou non filaires. Lorsque la connexion s'opère via un réseau wifi à domicile, faut-il comptabiliser le routeur (un objet donc) ou chacun des objets dotés d'une solution leur permettant de se connecter au réseau wifi ? Au niveau des entreprises, les machines connectées dites M2M ne sont pas toutes connectées à Internet. Faudrait-il donc ne compter que le nombre de machines disposant d'un moyen de communication avec connexion Internet (souvent des cartes SIM pour des connexions de machines) ? Récemment, Eurostat a précisé dans son questionnaire de 2021 sur les usages de l'IdO qu'il fallait exclure les détecteurs de fumée connectés ou les RFID qui ne peuvent être pilotés ou contrôlés via Internet ; et que le type de connexion utilisée était indifférent (réseau filaire ou non filaire, y compris via des réseaux privés virtuels ou VPN).

Graphique 10 – Les projections du marché de l'IdO 2014-2019 comparées aux données réalisées (estimées)



Source : Banque des territoires et Groupe Caisse des dépôts (2021), Les réseaux IoT en zone peu dense. État des lieux de l'IoT en France avec un focus sur les zones peu denses*, guide, janvier, p. 16*

Les estimations peuvent ainsi varier du simple au quadruple selon les sources (voir Graphique 10 et précédents) : entre 18 milliards et 28 milliards pour les instituts de recherche, et jusqu'à 78 milliards pour une banque d'affaires. Or les données réalisées en 2019 donnent un chiffre de près de 10 milliards d'objets connectés, soit 70 % de moins que les projections initiales les plus conservatrices. Malgré ces écarts importants, si on considère les tendances sur les six dernières années, toutes les sources concordent sur le constat d'une très forte croissance des objets connectés, dont le nombre aurait doublé en six ans.

En France, l'étude publiée en janvier 2022 par l'Ademe (Agence de l'environnement et de la maîtrise de l'énergie) et l'Arcep estime qu'en 2021 le nombre d'objets connectés s'élève à 10 milliards dans le monde, dont 1,8 milliard en Europe et 244 millions en France. Les ordinateurs, les tablettes et les smartphones ne sont pas inclus dans ce décompte.

Tableau 7 – Nombre d'objets connectés dans le monde en Europe et en France

	Monde	Europe	France
Estimation à l'horizon 2021	10 milliards	1,8 milliard	244 millions

Source : Ademe et Arcep (2022), Évaluation de l'impact environnemental du numérique en France et analyse prospective*, note de synthèse, janvier*

Le périmètre du marché et des activités IdO

Au-delà du manque de données statistiques comparables sur le nombre d'objets connectés, comment faut-il délimiter et estimer le marché de l'IdO ? Plusieurs questions se posent : doit-on comptabiliser seulement le marché des nouveaux produits IdO, comme les assistants vocaux, ou bien l'ensemble des produits devenus connectés (réfrigérateurs par exemple). La valeur du produit connecté correspond-elle au total des produits existants (réfrigérateurs et télévisions connectés) ou à la seule composante qui lui procure l'interaction avec Internet. Au sein de l'écosystème, comment évaluer la part IdO des activités de tel ou tel acteur ? Comment distinguer ce qui relève de la production de branche de celle du secteur ? Là aussi, malgré les différences de périmètres, les estimations prévoient une multiplication par dix du chiffre d'affaires sur la période 2018-2028. C'est le segment des objets connectés à destination des consommateurs qui connaîtrait la plus forte croissance. Du côté de l'offre, ce sont les logiciels et les données ainsi que leurs applications qui représenteraient la plus grande part de la chaîne de valeur (les deux tiers), le reste comprenant les capteurs et les différents réseaux mobilisés (voir point suivant).

La présence de l'IdO dans les enquêtes de la statistique publique porte principalement sur sa diffusion dans les entreprises et chez les ménages

Les enquêtes publiques existantes portent surtout sur la diffusion de l'Internet des objets dans les entreprises et les ménages. Des données comparatives entre pays européens

rendent ainsi compte du degré de diffusion auprès des entreprises et des individus. Du côté des ménages, les données d'Eurostat montrent que la diffusion de l'IdO est importante dans le domaine de la maison intelligente, avec en particulier l'adoption de la télévision connectée (en moyenne, une personne sur deux), des consoles de jeux (une personne sur cinq) et une percée importante des assistants virtuels (une personne sur dix, qu'il s'agisse d'une enceinte intelligente ou d'une application sur smartphone, par exemple). Toujours selon Eurostat, les craintes exprimées par les Européens pour justifier leur non-utilisation de ces technologies portent principalement sur les questions de sécurité informatique et de protection de la vie privée et des données personnelles, même si la première raison invoquée est une absence de besoin (43 % des individus).

D'autres indicateurs sont utiles pour appréhender l'évolution de l'IdO

Il n'y a pas de vision globale de la statistique publique, nationale et internationale, sur les indicateurs élémentaires pour appréhender l'évolution de l'IdO : nombre d'objets connectés, chiffre d'affaires de ce marché, valeur ajoutée, échanges internationaux, chaînes de valeur, etc. Les estimations disponibles sont donc fondées principalement sur les bases de données privées ou sur la mise en œuvre d'autres types d'indicateurs, comme l'OCDE le préconise, en utilisant par exemple :

– les données collectées par les acteurs de la régulation des télécommunications (par exemple les données sur les ventes de cartes SIM destinées aux machines) M2M ;
– les brevets, notamment les données de l'Organisation mondiale de la propriété intellectuelle ;
– les données sur les acteurs de la chaîne de valeur, notamment l'évolution des nombres de fusions-acquisitions ;
– les données sur les équipementiers, notamment les producteurs de capteurs et d'actionneurs, des circuits électroniques et des semi-conducteurs intégrés dans les solutions IdO ;
– les données des opérateurs des services de réseaux ou des producteurs de logiciels ;
– les données sur les startups dans ce domaine.

Ainsi, les données présentées dans ce rapport sont pour la plupart des estimations issues de sources différentes, et les valeurs varient selon la source mobilisée. Malgré leurs imperfections, elles permettent d'appréhender les tendances récentes et à venir. Elles concordent toutes sur le constat d'une forte croissance durant les six dernières années et sur le potentiel d'une croissance exponentielle durant les dix prochaines années. En conséquence, la recherche d'une meilleure observation de l'IdO figure parmi les éléments de la stratégie de certains pays leaders sur le marché (voir l'exemple des États-Unis au Chapitre 7 sur le cadre juridique) et parmi les recommandations formulées dans ce rapport.

2. Un marché mondial en pleine expansion

En 2025, l'IdO représenterait 50 % du montant du marché mondial de onze technologies de rupture, contre un tiers en 2018

Dans son rapport de 2021, la Conférence des Nations unies sur le commerce et le développement (CNUCED)[1] a distingué l'Internet des objets parmi les onze technologies dites à la frontière technologique (ou technologies de rupture) qui prennent appui sur le numérique et la connectivité et leurs interactions pour favoriser l'amélioration ou le développement de nouveaux produits et services. Les dix autres technologies sont : l'intelligence artificielle, le Big Data, la *blockchain*, la 5G, l'impression 3D, la robotique, les drones, l'édition génomique, les nanotechnologies et le photovoltaïque solaire. Selon les estimations recensées par la CNUCED (voir Graphique 11 page suivante), ces onze technologies représentent un marché mondial de l'ordre de 3 200 milliards de dollars par an en 2025, soit neuf fois la valeur de ce marché en 2018 (350 milliards de dollars)[2].

L'Internet des objets représenterait un marché estimé à 1 500 milliards de dollars en 2025, soit plus de dix fois sa valeur de 2018. Dans cette évolution, c'est l'Internet des objets[3] qui connaîtrait la plus forte croissance. De 130 milliards de dollars en 2018, son marché mondial atteindrait 1 500 milliards de dollars en 2025. En part relative, il passerait ainsi d'un tiers du marché des onze technologies de ruptures retenues en 2018 à près de la moitié en 2025. Les perspectives de développement sont donc importantes alors même que ces estimations concernant les objets connectés n'incluent ni les ordinateurs portables ni les smartphones[4]. La croissance du marché de l'IdO s'expliquerait d'une part par la forte diffusion et la grande variété des usages des objets connectés chez les ménages (la maison connectée en particulier), et dans une moindre mesure par leur développement dans l'industrie.

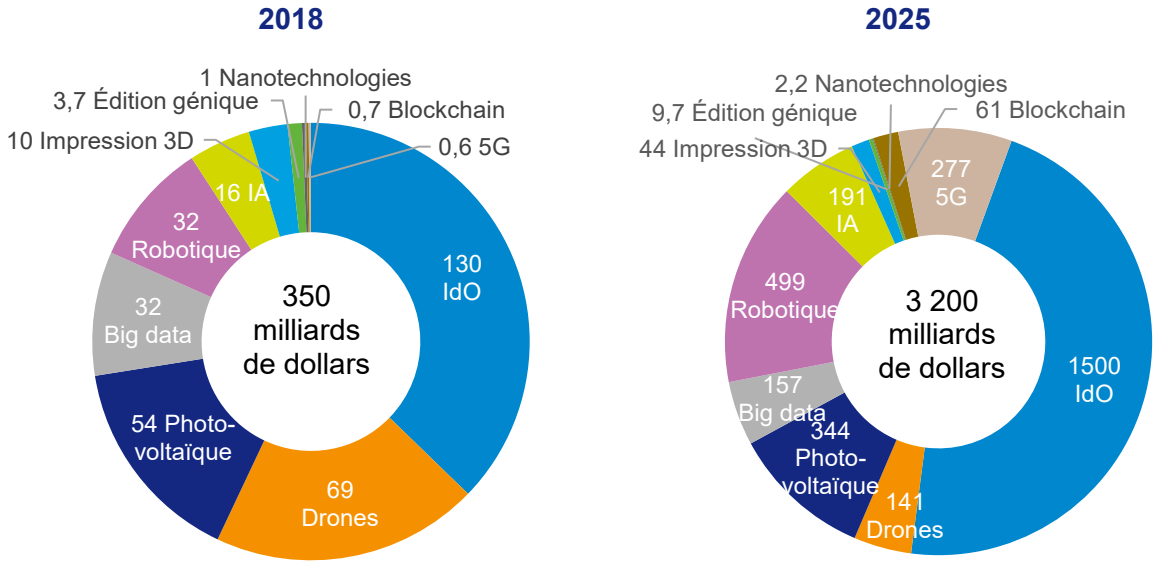
[1] CNUCED (2021), *Technology and Innovation Report 2021*, *op. cit.*

[2] Les estimations citées par la CNUCED dans son rapport de 2019, qui se basent sur les données de IoT Analytics (2018), sont assez proches (151 milliards de dollars en 2018 et 1 567 milliards en 2025).

[3] Définition de la CNUCED : l'Internet des objets « *refers to the growing array of Internet-connected devices such as sensors, meters, radio frequency identification (RFID) chips and other gadgets that are embedded in various everyday objects enabling them to send and receive various kinds of data. It has wide applications, including in energy meters, for RFID tagging of goods for manufacturing, livestock and logistics, for monitoring soil and weather conditions in agriculture, and for wearables*. »

[4] Les estimations de cinq organismes donnent une fourchette entre 1 271 milliards et 2 293 milliards de dollars en 2029. Voir Banque des territoires et Groupe Caisse des dépôts (2021), *Les réseaux IoT en zone peu dense. État des lieux de l'IoT en France avec un focus sur les zones peu denses*, guide, janvier.

Graphique 11 – Marché mondial de onze technologies de rupture en 2018 et en 2025, en milliards de dollars



Source : CNUCED (2021), Technology and Innovation Report 2021. Catching Technological Waves: Innovation with Equity*, Conférence des Nations unies sur le commerce et le développement*

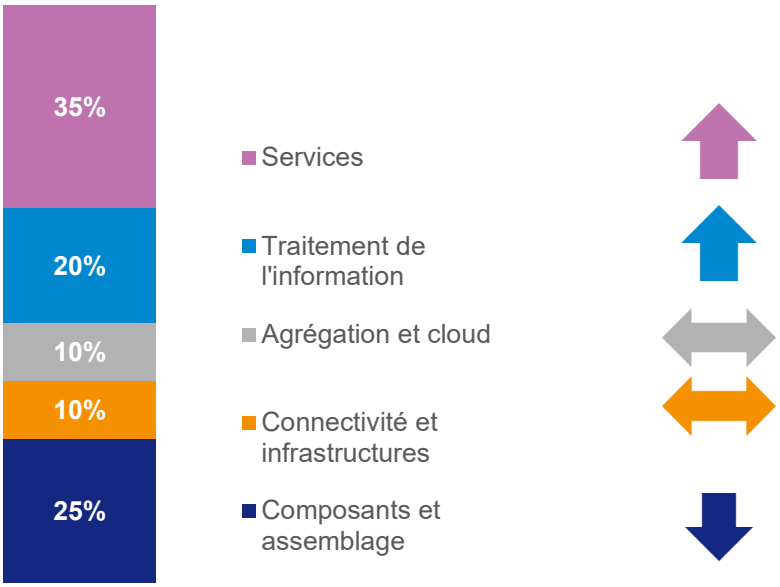
Côté offre, services et logiciels représentent près des deux tiers du marché

Qu'il soit destiné aux consommateurs, aux acteurs publics (dont les collectivités locales) ou aux entreprises, l'IdO implique une grande variété d'acteurs tout au long de la chaîne de valeur et des segments du marché (voir Tableau 3), qui peuvent être regroupés en deux grands ensembles : d'une part tout ce qui relève du hardware, avec notamment les composants et l'assemblage (capteurs et autres matériaux et appareils), la connectivité et les infrastructures ; d'autre part la brique logicielle, notamment les données, l'agrégation et les *clouds*, le traitement de l'information et les services.

Les estimations du marché en 2019 et de son évolution au cours des prochaines années montrent clairement que ce sont les segments logiciels qui représentent la plus grande part du marché. Selon l'étude précitée de la Banque des territoires, ils en constitueraient les deux tiers, dont les services et les traitements de l'information formeraient respectivement 35 % et 20 %. Ces estimations sont corroborées par d'autres sources[1].

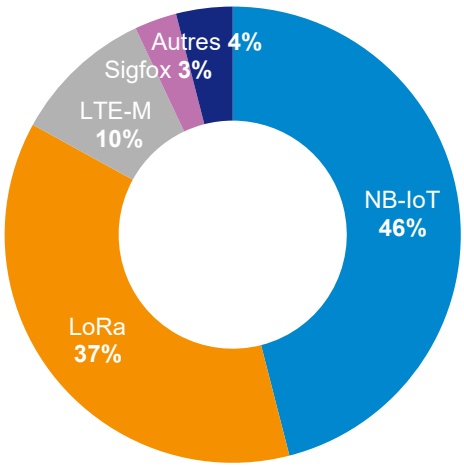
[1] IDC (2020), *Worldwide Internet of Things Spending Guide 2020 (V1 2020)*.

Graphique 12 – Marché de l'Internet des objets par segments en 2019



Source : estimations de la chaîne de valeur, par le Cabinet PMP, présentées dans l'étude de Banque des territoires et Groupe Caisse des dépôts (2021), Les réseaux IoT en zone peu dense…, op. cit., *p. 17*

Graphique 13 – Répartition des technologies IdO dans le monde, en pourcentage des objets connectés en 2021

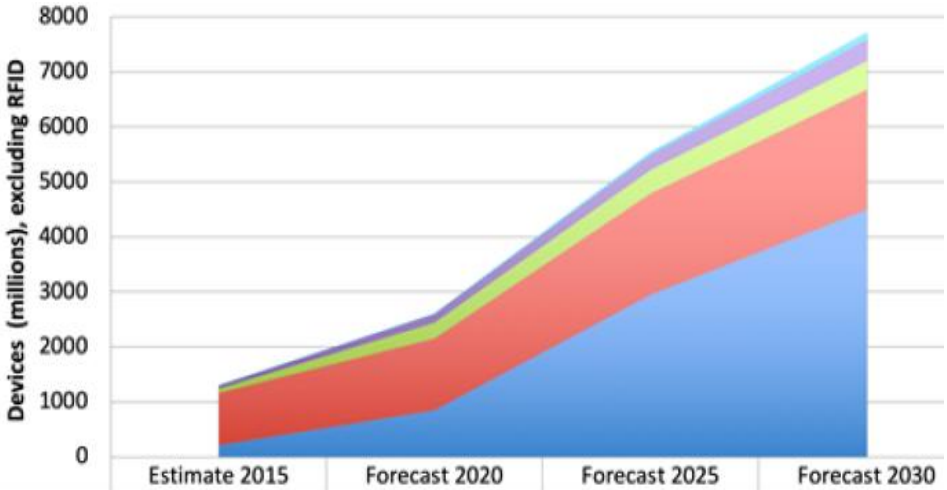


Source : Challenge, données « IoT analytics research 2021 » (2021)

Côté demande, plus de 60 % proviendraient du marché destiné aux usages des consommateurs

Le rapport préliminaire de l'enquête en cours de la Commission européenne sur les pratiques anti-concurrentielles dans le domaine de l'Internet des objets pour les consommateurs fournit des estimations. Le marché mondial des objets connectés pour les consommateurs devrait connaître une forte croissance, passant de 105,7 milliards d'euros en 2019 à 404,6 milliards en 2030[1]. Les dispositifs relevant de la maison intelligente (*smart home*) passeraient à eux seuls de 210 millions d'unités à plus de 4,5 milliards d'objets connectés. Ce développement traduit l'évolution des usages par les consommateurs, notamment dans l'Union européenne où l'on estime que 51 % des particuliers utilisent Internet via une télévision connectée, une console de jeux, un système audio domestique ou d'une enceinte connectée (voir point suivant).

Graphique 14 – Les dispositifs d'équipements radio dans les pays de l'UE en 2015 : estimation de leur évolution en 2030



	Estimate 2015	Forecast 2020	Forecast 2025	Forecast 2030
Transport & traffic telematics	3.0	11.9	45.2	132.0
Remote monitoring & wireless alarms	64.2	164.0	275.0	387.0
Audio/media wireless streaming	75.8	282.5	435.0	516.0
Wideband data transmission	948.5	1,304.4	1,836.0	2,184.0
Smart Homes (alarms and telecommand)	210.0	850.0	2,950.0	4,500.0

Note : les RFID et les équipements médicaux sont exclus.

Source : CSES and Tech4i2 (2020), Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment*, rapport final pour la Commission européenne, avril, p. 19*

[1] Commission européenne (2021a), *Prelimiray Report. Sector Inquiry into Consumer Internet of Things*, Commission staff working document, juin.

L'étude d'impact réalisée pour le compte de la Commission européenne dans le cadre de cette même enquête fournit aussi des estimations éclairantes sur le poids et les évolutions à venir pour ces catégories d'objets. Le Graphique 14 donne les prévisions entre 2015 et 2030 dans les pays de l'UE-28 du nombre de dispositifs d'équipement radio qui seraient utilisés selon différents types d'usages, regroupés en sept catégories d'applications (voir Tableau 8).

- Les estimations indiquent qu'il y avait en 2015 plus d'un milliard (1,097 milliard) d'équipements radio dans les États membres de l'UE-28. Leur nombre devrait être multiplié par sept pour atteindre 7,43 milliards en 2030[1], soit un taux de croissance annuel de 14,6 %. Rapporté à la population de l'UE, il représenterait l'équivalent de la mise en œuvre de 29 objets connectés par ménage.
- À eux seuls, les dispositifs intégrés aux appareils associés aux maisons intelligentes devraient atteindre 4,5 milliards en 2030, soit plus de 60 % du total des équipements.
- Les deux catégories d'applications à plus forte croissance concerneraient des appareils utilisés sur les réseaux locaux à courte portée utilisant généralement le Wifi et le Bluetooth.

Tableau 8 – Les catégories d'équipement radio retenues dans l'étude d'impact sur la protection des équipements radio connectés à Internet

Catégories d'application	Type de dispositif
Identification par radiofréquence (RFID)	Lecteurs portables et fixes pour les paiements et le suivi
Télématique du transport routier et de la circulation routière	Radars anticollision embarqués, perception de télépéage, systèmes de transport intelligents, terminaux de données mobiles à bord des véhicules
Dispositifs de maison intelligente (alarmes, télécommandes et télémétrie)	Alarmes sans fil, clés électroniques, écoute-bébés, systèmes d'ouverture de porte de garage ou de portail, équipement de télémétrie, télécommandes
Streaming audio/média sans fil	Mini-émetteurs FM, casques sans fil, lecteurs multimédias, haut-parleurs, micros sans fil
Télésurveillance et alarmes sans fil	Compteurs, alarmes sociales, alarmes de détresse
Transmission de données à large bande	Tablettes, smartphones, consoles de jeux, lecteurs multimédias, haut-parleurs, téléviseurs intelligents, voitures connectées, dispositifs portables, jouets et drones

Note : ce tableau comporte des produits qui ne sont pas classés comme IdO selon la définition retenue dans ce rapport.

Source : CSES and Tech4i2 (2020), Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment*,* op. cit.*, p. 18*

[1] Ces estimations n'intègrent pas les RFID, l'étude indiquant que 99 % de ces objets ne disposent pas de batterie d'alimentation interne et ne peuvent pas transmettre de données. L'étude estime leur nombre à 3,7 milliards en 2015 et 58,8 milliards d'unités en 2030.

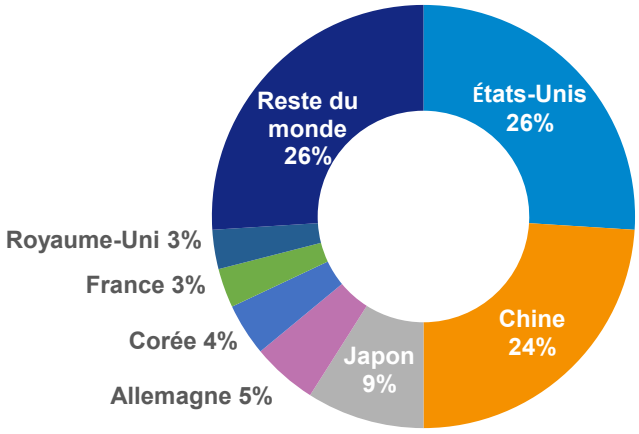
De nombreuses estimations produites par des instituts statistiques privés confirment ce constat. Selon l'article de Techjury[1], les produits de l'IdO destinés aux consommateurs demeureront le segment le plus important avec près des deux tiers du marché de l'IdO entre 2018 et 2020[2].

Comme indiqué plus haut, les données sur le taux d'équipement des consommateurs en IdO souffrent de difficultés de mesure. Comme le souligne le rapport de l'OCDE (2018, *op. cit.*), certains objets ou applications ne sont pas systématiquement identifiés par les consommateurs comme des objets connectés. Le rapport cite l'exemple de l'enquête de 2016 de TNS and Bearing Point auprès de 3 700 consommateurs en Europe, qui montrait que 39 % des automobilistes n'étaient pas conscients que leur véhicule était connecté à Internet. Des indicateurs sont ainsi proposés comme le nombre de cartes SIM (pour la communication mobile) utilisées pour les communications entre machines.

La répartition du marché par pays

Les données par pays[3] présentées par la CNUCED montrent que les États-Unis, la Chine et l'Europe sont en tête du marché mondial, avec chacun quasiment un quart du marché en valeur (respectivement 26 %, 24 % et 23 % en 2019). Le Japon (9 %), l'Allemagne (5 %), la Corée (4 %), la France (3 %) et le Royaume-Uni (3 %), les États-Unis et la Chine représentent les trois quarts du marché mondial de l'IdO.

Graphique 15 – Le marché mondial des objets connectés en 2019, en pourcentage



Source : CNUCED (2021), Technology and Innovation Report 2021*, sur la base des données IDC de 2019*

[1] Petrov C. (2022), « 49 Stunning Internet of Things statistics 2021. The Rise of IoT », *TechJury*, 4 janvier.

[2] Voir également Froese M. (2018), « Global IoT market to reach $318 billion by 2023, says GlobalData », *Windpower Engineering & Development*, 18 novembre.

[3] CNUCED (2019), *Digital Economy Report 2019. Value Creation and Captures: Implications for Developing Countries*, Conférence des Nations unies sur le commerce et le développement.

Le poids des États-Unis et de la Chine est confirmé par d'autres indicateurs :

- Sur les 66 467 publications scientifiques sur l'IdO entre 1996 et 2018, un grand nombre provenaient de Chine (10 081), des États-Unis (7 520) et d'Inde (5 700).
- En matière de brevets, sur les 22 180 brevets déposés en lien avec l'IdO, 9 515 ont été attribués à la Chine, 5 106 à la Corée et 4 275 aux États-Unis. Les trois principales entreprises déposantes sont la société coréenne Samsung Group (avec 2 508 brevets) et les deux sociétés américaines Qualcomm (1 213 brevets) et Intel (667 brevets). Enfin, les sociétés de services sont principalement américaines (notamment Alphabet, Amazon, IBM, Cisco, Microsoft, Oracle).

Le marché des objets connectés destinés aux consommateurs est estimé à 2,7 milliards d'euros en 2020[1]. Même si les sources sont différentes, en tenant compte des estimations de la CNUCED, on peut considérer que le marché destiné aux entreprises en 2020 serait de l'ordre de 7 milliards d'euros (soit 70 %).

3. La diffusion en France et en Europe

Une entreprise française sur dix utilise des systèmes interconnectés

Selon l'enquête TIC 2020 de l'Insee, en 2020, 10 % des entreprises de dix salariés ou plus utilisaient l'Internet des objets. Si seulement 7 % des entreprises de 10 à 19 salariés sont dotées de systèmes interconnectés[2], cette proportion atteint 29 % pour les entreprises plus importantes (250 personnes ou plus)[3]. L'accroissement de l'usage de ces technologies avec la taille des entreprises s'expliquerait selon l'Insee par le nombre d'équipements et de produits à prendre en charge, qui seraient plus importants dans les grandes entreprises. L'usage de l'IdO leur permet d'automatiser, voire de centraliser le contrôle et la gestion à distance des équipements interconnectés.

Par ailleurs, l'usage de l'Internet des objets en France présente une intensité très variable selon les secteurs. Les données de l'enquête Insee montrent par exemple que ce sont les secteurs des transports, des TIC (technologies de l'information et de la communication) et de l'industrie qui utilisent le plus ces équipements interconnectés, avec respectivement 16 %, 12 % et 11 %. Les secteurs qui y ont le moins recours sont ceux du commerce de gros, du commerce et de la réparation automobile, ainsi que l'hébergement et la

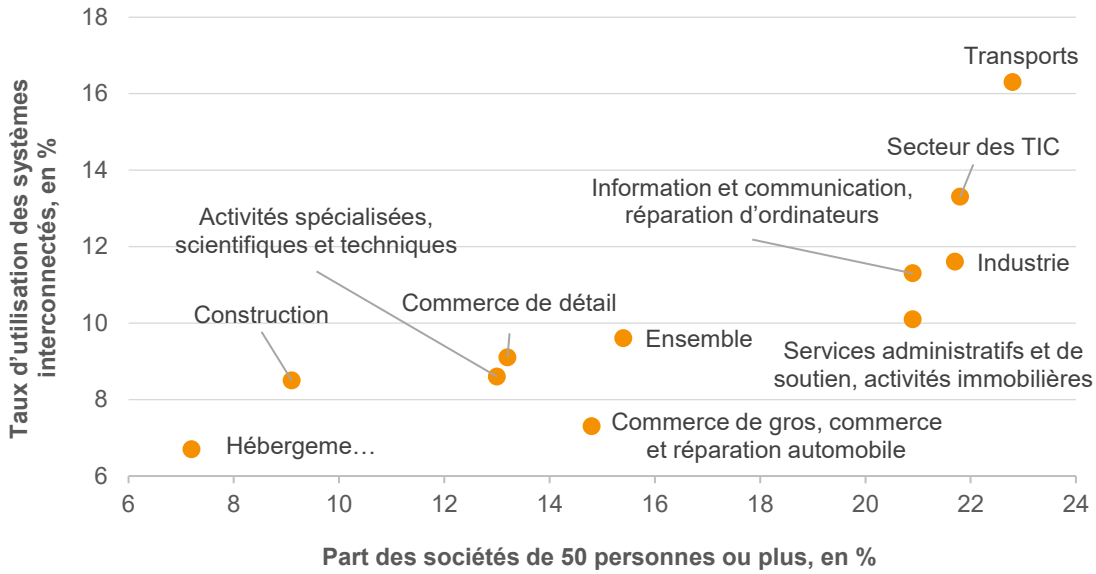
[1] D'après Garcia-Montero C. (2021), « Le Royaume-Uni, champion de la domotique en Europe », *Journal du net*, 8 avril, à partir des données de Statista.

[2] « Système interconnecté » est le terme retenu pas l'enquête de l'Insee pour désigner les objets connectés.

[3] Boudrot N. (2021), « Internet des objets, impression 3D, robotique : des technologies davantage utilisées par les grandes sociétés », *Insee Première*, n° 1854, avril.

restauration (autour de 7 %). Pour ces derniers secteurs, une explication résiderait dans la plus faible proportion de grandes sociétés : 7 % des sociétés y emploient 50 personnes ou plus, contre 15 % dans l'ensemble des secteurs.

Graphique 16 – Utilisation des dispositifs interconnectés par secteur en 2020



Lecture : en 2020, 16 % des sociétés de transport ont recours aux systèmes interconnectés. Dans ce secteur, 23 % des sociétés emploient 50 personnes ou plus. * Technologies de l'information et de la communication.

Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.

Source : Insee, enquête TIC entreprises 2020 ; Boudrot N. (2021), « Internet des objets, impression 3D, robotique : des technologies davantage utilisées par les grandes sociétés », Insee Première*, n° 1854, avril*

Par ailleurs, l'enquête de l'Insee distingue cinq usages des objets connectés selon les objectifs poursuivis par l'entreprise : optimiser la consommation d'énergie, améliorer le service à la clientèle, surveiller les besoins en maintenance des véhicules ou des produits, surveiller ou automatiser les processus de production ou la logistique, et autres usages (voir Tableau 9). Trois constats en découlent :

– parmi les sociétés qui utilisent des systèmes interconnectés, plus des deux tiers ne sont équipées que d'un seul type de dispositif. Une entreprise sur cinq combine au moins trois types de dispositifs ;

– si l'on considère les dispositifs interconnectés, c'est-à-dire plusieurs systèmes combinés au sein d'une même entreprise, ce sont les associations de dispositifs qui permettent d'optimiser la consommation énergétique et d'améliorer le service client qui sont les plus fréquentes, avec plus de 80 % d'utilisation ;

– les entreprises utilisant un seul type de dispositif interconnecté (32 % des entreprises) recourent à des capteurs de suivi ou d'entretien des véhicules ou des produits.

Tableau 9 – Principaux types d'utilisation des dispositifs interconnectés en 2020, en % de sociétés utilisant des dispositifs interconnectés

	Optimiser la consommation d'énergie	Améliorer le service à la clientèle	Surveiller les besoins en maintenance des véhicules ou des produits	Surveiller ou automatiser les processus de production ou la logistique	Autres usages
10 à 19 personnes	29	23	35	11	30
20 à 49 personnes	33	24	41	13	37
50 à 249 personnes	38	27	41	25	34
250 personnes ou plus	53	33	30	35	48
Commerce de détail	48	63	9	21	33
Information et communication, réparation d'ordinateurs	44	19	24	22	58
Activités spécialisées, scientifiques et techniques	38	18	13	14	42
Industrie	37	23	34	24	35
Hébergement et restauration	37	38	15	7	31
Commerce de gros ; commerce et réparation automobile	34	28	33	19	39
Services administratifs et de soutien ; activités immobilières	31	20	45	21	35
Construction	25	7	69	6	18
Transports	21	19	74	14	37
Secteur des TIC	43	18	26	26	66
Ensemble	**34**	**25**	**38**	**17**	**35**

Lecture : en 2020, 53 % des sociétés de 250 personnes ou plus qui utilisent des dispositifs interconnectés s'en servent pour optimiser la consommation d'énergie dans les locaux de l'entreprise.

Champ : sociétés de 10 personnes ou plus qui utilisent des systèmes interconnectés, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.

Source : Insee (2021), enquête TIC entreprises 2020 ; Boudrot N. (2021), « Internet des objets, impression 3D, robotique : des technologies davantage utilisées par les grandes sociétés », op. cit.

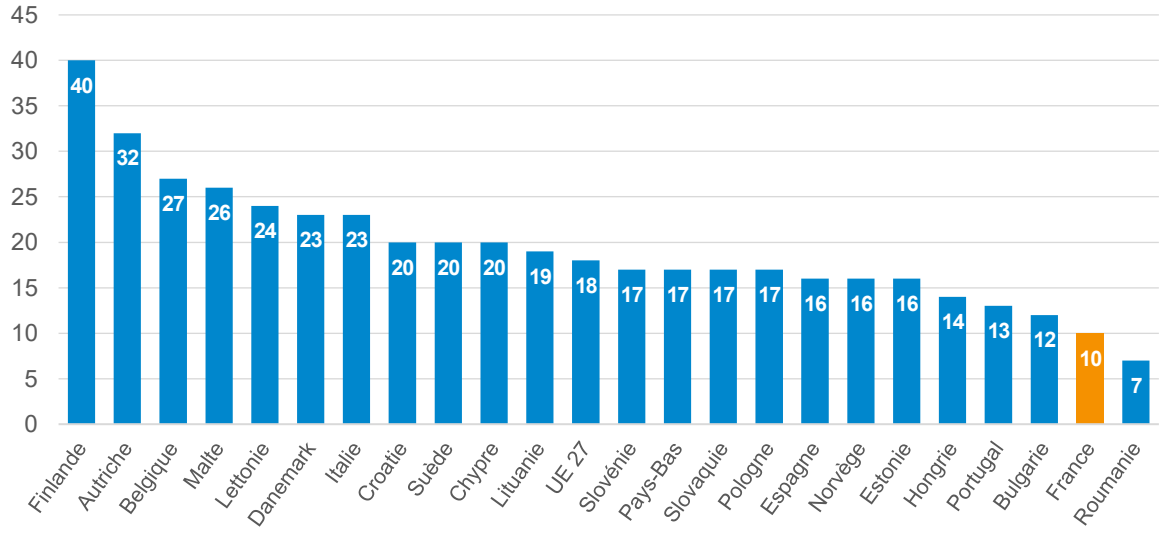
Enfin, les systèmes d'objets connectés génèrent des masses de données importantes. L'Insee souligne que l'utilisation des dispositifs interconnectés se traduit pour les entreprises de 10 salariés ou plus par un recours deux fois plus important à des services de *cloud computing* (une proportion de 44 % contre 25 % pour les autres entreprises). En comparaison internationale, les entreprises qui utilisent l'IdO ont une propension de 10 à 20 points de plus que les autres à accompagner cet usage par des activités de *cloud computing* (en interne ou via l'achat de services spécialisés dans ce domaine).

Au niveau européen, l'enquête sur les usages de l'Internet des objets par les entreprises est harmonisée par Eurostat. Avec une proportion de 10 %, les entreprises en France enregistrent presque la proportion la plus faible d'Europe, juste avant la Roumanie, dernier du classement. Au niveau européen, l'usage de l'Internet des objets augmente aussi avec la taille des entreprises : 30 % pour les grandes entreprises contre 20 % pour les entreprises de taille moyenne et 10 % pour les petites.

Parmi les entreprises européennes qui disposent de systèmes interconnectés (voir Graphique 17), un quart utilisent « des compteurs, lampes ou thermostats intelligents pour optimiser la consommation d'énergie dans leurs locaux » (34 % en France, voir Tableau 8). Un quart également de ces entreprises européennes déploient « des capteurs de mouvements ou de maintenance pour suivre le déplacement des véhicules ou des produits ou proposer un service d'entretien des véhicules en fonction de leur état », une proportion légèrement supérieure à celle constatée en France (38 %).

Si les données disponibles donnent un éclairage sur le développement de l'IdO selon les fonctions d'usage dans les 10 % des entreprises qui y ont recours, elles ne permettent pas d'appréhender les raisons pour lesquelles les autres entreprises (soit 90 % de l'ensemble et 70 % des grandes entreprises) n'y ont pas recours aujourd'hui.

Graphique 17 – Utilisation des systèmes interconnectés dans l'Union européenne en 2020



Note : la Grèce et la République tchèque ne sont pas représentées, les critères minimaux de fiabilité n'étant pas remplis pour cet indicateur.

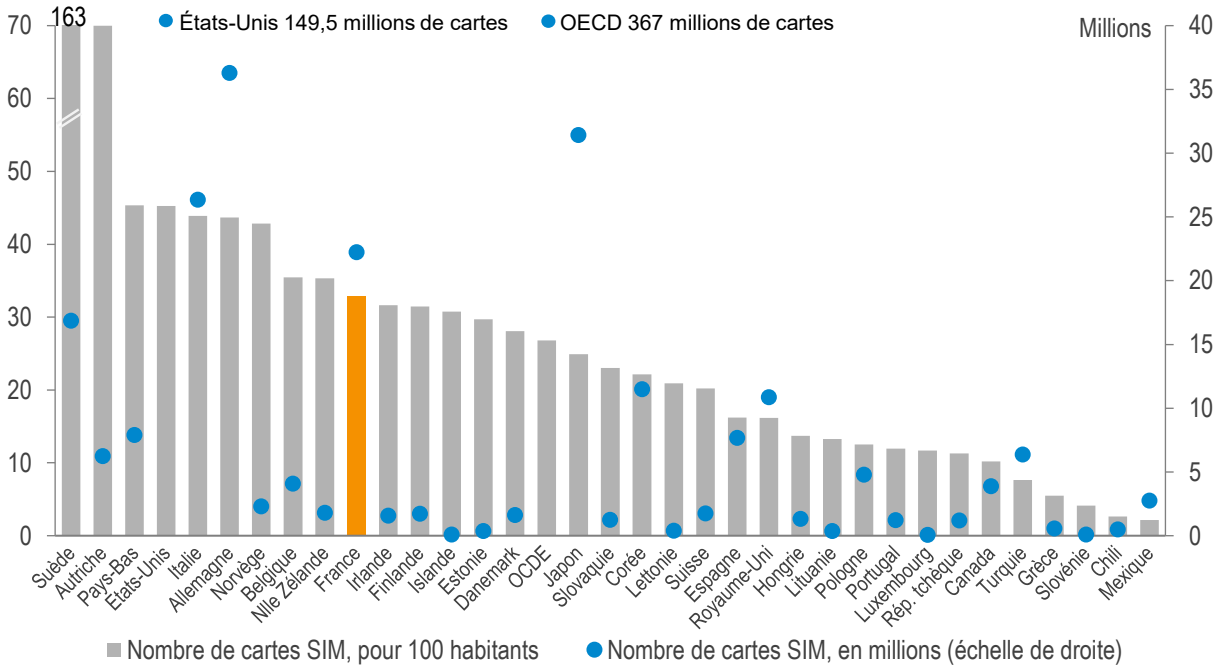
Lecture : en Italie, 23 % des sociétés utilisent des systèmes interconnectés en 2020

Champ : sociétés de 10 personnes ou plus, implantées en France ou dans l'UE à 27, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.

Sources : Eurostat ; Insee, enquête TIC entreprises 2020

Si on considère un des indicateurs qui mesurent le nombre d'objets connectés via les seuls réseaux mobiles et utilisant des cartes SIM (communications mobiles machine à machine, M2M), l'OCDE dénombre un total de 367 millions de machines connectées dans les pays de l'OCDE, dont 149,5 millions sont localisées aux États-Unis. La France, avec 22 millions, occupe la dixième place, et la neuvième pour le nombre de cartes M2M pour 100 habitants (voir Graphique 18).

Graphique 18 – Nombre de cartes SIM dans les pays OCDE, en millions et pour 100 habitants



Source : OCDE Broadband Statistics

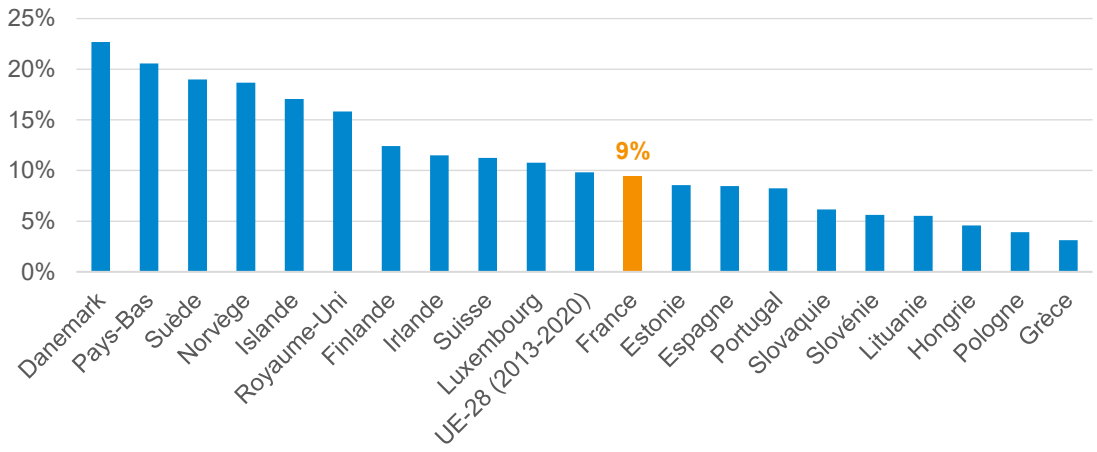
Des craintes relatives à la sécurité, à la protection de la vie privée et des données personnelles

L'expression « Internet des objets » n'est pas encore très répandue. Il n'existe pas dans les enquêtes de la statistique publique des pays de l'OCDE de questions sur son usage par les ménages. Toutefois, les enquêtes sur l'utilisation de l'Internet, notamment celles harmonisées au niveau européen par Eurostat, permettent d'appréhender en grande partie les usages de l'IdO par les ménages à la maison comme dans leurs activités quotidiennes. Selon les données disponibles, en 2019, un individu sur 10 dans les pays de l'UE a utilisé Internet pour interagir avec des objets connectés à domicile[1]. La France, avec 9 %, se

[1] La question posée est la suivante : « *In the last 3 months, I have interacted via the Internet with household equipment or appliances (such as a thermostat, light bulb, robot vacuum or security system)* ».

situe dans la moyenne. Les pays du Nord de l'UE se caractérisent par une plus forte proportion d'utilisation de l'IdO, avec des valeurs supérieures ou égales à 12 %, atteignant même 23 % au Danemark. De l'autre côté de la distribution, les nouveaux pays membres ont des proportions inférieures ou égales à 5 %. Les autres pays, dont la France, ont des proportions qui varient peu autour de 10 %[1].

Graphique 19 – L'utilisation de l'IdO par les ménages en Europe en 2019 (proportion d'individus ayant utilisé Internet pour communiquer avec des objets connectés)



Source : France Stratégie, données Eurostat (2020), « Statistiques communautaires sur la société de l'information »

L'enquête Eurostat distingue cinq catégories d'usage selon que la connexion à Internet soit intégrée à :

– un thermostat, un compteur, des lampes ou modules d'extension connectés à l'Internet ou d'autres solutions connectées à l'Internet, afin de gérer l'énergie au domicile ;

– un système d'alarme résidentiel, un détecteur de fumée, des caméras de sécurité ou des serrures connectées à l'Internet, ou d'autres solutions de sécurité ou de sûreté connectées à l'Internet pour le domicile ;

– des appareils domestiques connectés à l'Internet, comme des aspirateurs robotisés, réfrigérateurs, fours ou machines à café ;

– des assistants virtuels sous forme d'une enceinte intelligente ou d'une application ;

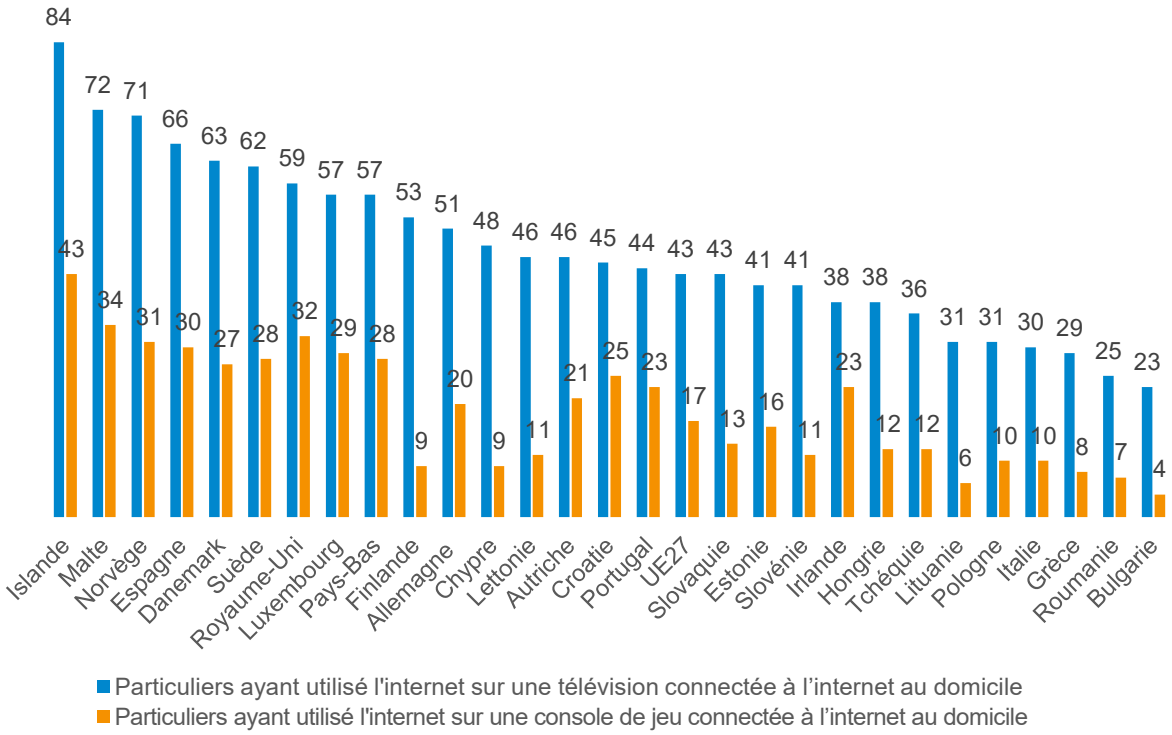
– une télévision ou une console de jeux connectée à l'Internet au domicile.

[1] Selon le *Journal du Net* (JDN), qui se base sur les données publiées dans le *Digital Market Outlook* de Statista, le taux d'équipement des ménages français en domotique connectée est estimé à 17 %. Voir Garcia-Montero C. (2021), « Le Royaume-Uni, champion de la domotique en Europe », *op. cit.*

Les résultats de cette enquête, présentés dans les Graphiques 20, 21 et 22, révèlent les préférences actuelles des individus en Europe en matière d'usage de l'IdO. L'enquête 2020 ne comporte pas les données de la France car l'Insee a dû interrompre son enquête en raison de la crise sanitaire.

Avec en moyenne un foyer sur deux, Internet est devenu le premier canal de diffusion de la télévision. Le succès de la télévision connectée s'explique en partie par le confort du téléviseur pour le visionnage des contenus, notamment en famille. Dans certains pays d'Europe, le taux d'équipement atteint même des proportions très élevées, comme en Islande (85 %), en Espagne (66 %) et au Royaume-Uni (59 %). Seuls trois pays enregistrent, pour le moment, un taux d'équipement inférieur à 30 % : la Grèce, la Roumanie et la Bulgarie.

Graphique 20 – L'utilisation de l'Internet des objets par les ménages pour la télévision et les consoles de jeu, en %, en 2020

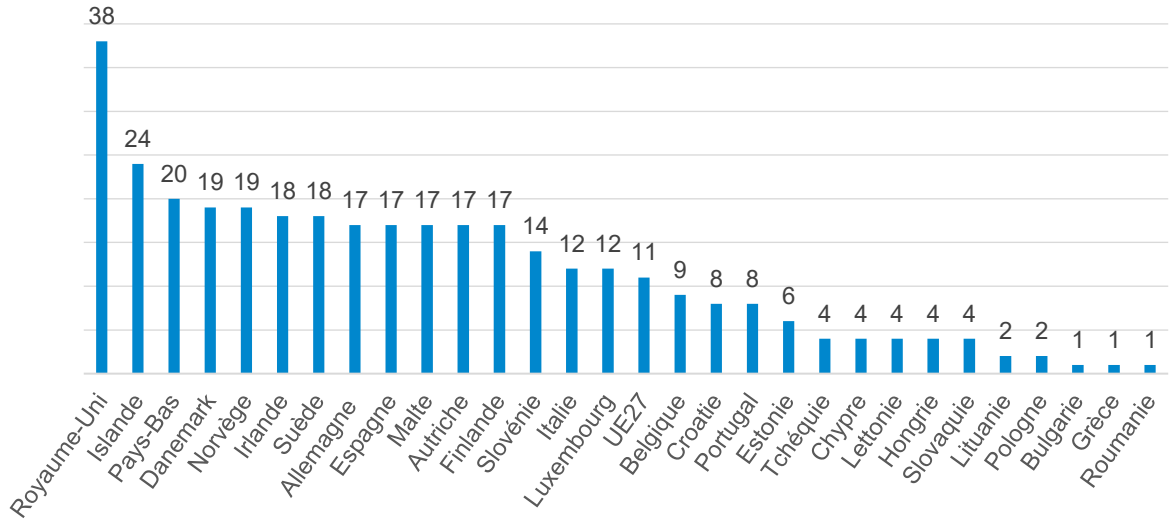


Source : France Stratégie, données Eurostat (2020), « Statistiques communautaires sur la société de l'information »

Les consoles de jeux occupent la deuxième place avec un individu sur cinq. Les appareils de divertissements sont donc en tête des usages de l'IdO par les individus en Europe.

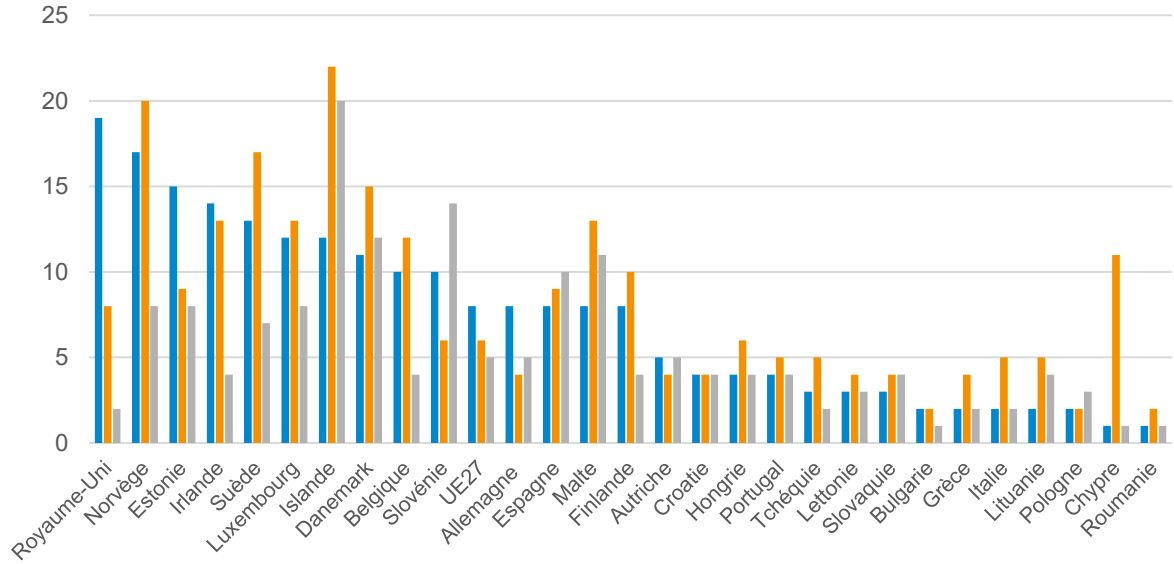
Les assistants virtuels (Google Home, etc.) constituent le troisième principal usage de l'IdO. Un peu plus d'un Européen sur dix a utilisé un assistant virtuel en 2020. Selon les instituts statistiques privés, les ventes des assistants virtuels, y compris les applications intégrées, connaissent une forte croissance ces dernières années.

Graphique 21 – Proportion d'individus ayant utilisé des assistants virtuels sous forme d'une enceinte intelligente ou d'une application, en pourcentage, en 2020



Source : France Stratégie, données Eurostat (2020), « Statistiques communautaires sur la société de l'information »

Graphique 22 – L'utilisation de l'Internet des objets par les individus pour la sécurité, l'économie d'énergie et les appareils domestiques, en pourcentage, en 2020



■ Particuliers ayant utilisé un thermostat, un compteur, de lampes ou de modules d'extension connectés à l'internet ou d'autres solutions connectées à l'internet, afin de gérer l'énergie au domicile

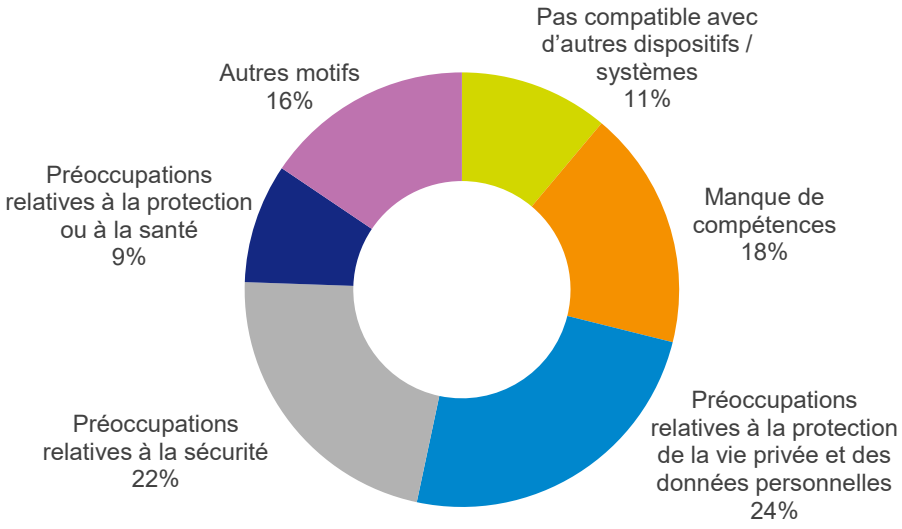
■ Particuliers ayant utilisé un système d'alarme résidentiel, un détecteur de fumée, de caméras de sécurité ou de serrures connectés à l'internet, ou d'autres solutions de sécurité ou de sûreté connectées à l'internet pour le domicile

Source : France Stratégie, données Eurostat (2020), « Statistiques communautaires sur la société de l'information »

Selon le *Baromètre du numérique*[1], en 2020, 23 % des Français disposent d'un objet connecté en lien avec la santé, 20 % des personnes interrogées disposent d'une enceinte connectée, 17 % ont de l'électroménager connecté, 15 % ont un objet connecté en lien avec la sécurité (contre 6 % en 2019), 14 % ont un objet dans le domaine de la domotique (contre 5 % en 2019). 17 % possèdent aujourd'hui un livre numérique.

La diffusion de l'IdO s'accompagne chez les personnes de craintes liées à la sécurité, à la sûreté des produits et à la confidentialité des données recueillies. Les données de l'enquête harmonisée par Eurostat permettent d'identifier des facteurs qui contribuent à expliquer que les individus n'utilisent pas l'Internet des objets aujourd'hui (voir Graphique 23). La première raison, invoquée par 41 % des personnes, est le fait qu'ils n'en éprouvent pas le besoin. La deuxième raison, relative aux questions de sécurité et de protection de la vie privée et des données personnelles, est indiquée par un quart des personnes (23 %). Un troisième facteur réside dans le coût jugé élevé des produits de l'IdO. Enfin, 5 % des personnes interrogées évoquent les problèmes de compatibilité entre les différents systèmes mobilisés.

Graphique 23 – Les raisons de la non-utilisation d'objets connectés par les ménages en Europe, en pourcentage, en 2020



Source : France Stratégie, données Eurostat (2020), « Statistiques communautaires sur la société de l'information »

[1] Arcep et Anct (2021), *Baromètre du numérique, édition 2021. Enquête sur la diffusion des technologies de l'information et de la communication dans la société française*.

Les estimations du nombre de dispositifs connectés existants et plus encore, les projections de développement de ces dispositifs sont aujourd'hui très incertaines et varient selon les sources ou les périmètres pris en compte. Mieux appréhender le développement des technologies utilisées, les usages en cours d'adoption ou encore les stratégies des principaux acteurs du secteur est nécessaire pour les décideurs publics mais aussi pour les entreprises.

C'est le sens de notre recommandation n° 1 : disposer d'un outil d'observation dédié à l'IdO.

BRÈVES DU MONDE

D'après une étude de juin 2020 du cabinet de conseil Zinnov, **l'Inde** comptait 200 à 250 millions d'objets connectés fin 2019. Ce nombre serait multiplié par dix en deux ans pour atteindre deux milliards d'équipements en 2021. De même, les investissements indiens dans l'IdO passeraient de 5 milliards de dollars en 2019 à environ 15 milliards en 2021, portés par l'industrie manufacturière, l'automobile et les transports, et l'énergie. Environ 60 % à 70 % de ces investissements concernent les objets connectés eux-mêmes (logiciels et électronique) et le solde les services associés à l'IdO.

Au Chili, le développement de l'IdO sera porté par les acteurs privés. Des dispositifs d'appui aux entreprises sont mis en place via des financements, des formations ou des appels à projets du ministère des Sciences, de la Technologie, de la Connaissance et de l'Innovation et de CORFO (Corporación de Fomento de Chile), agence publique de promotion de l'entrepreneuriat et l'innovation dépendante du ministère de l'Économie. Le programme de soutien au développement des entreprises qui reposent sur des technologies telles que l'intelligence artificielle, l'Internet des objets et la réalité augmentée[1], ou l'appel à projets du programme « Net Zero » pour l'accélération de projets dans le secteur cleantech auxquels participent des startups du domaine de l'énergie et de l'IdO. Le secteur des IdO n'est pas abordé en tant que tel par le gouvernement : il s'insère dans une politique plus générale de développement technologique du pays. À Santiago par exemple, un programme d'accompagnement aux entreprises qui produisent des produits et des services de « ville intelligente », dont l'IdO, appelé « Sé Santiago »[2] a été mis en place par CORFO et Fundación Pais Digital, association d'entreprises qui a pour but la promotion de la technologie au Chili.

En Chine, identifié comme stratégique par le MIIT, l'IdO voit son développement promu dans plus de 24 plans entre 2010 et 2020, dont certains sur des segments spécifiques (NB-IoT par le MIIT en 2017). Le plan *Made in China 2025* et l'initiative « Internet Plus » (2015) lui ont donné une

[1] Inria (2020), « Ministerio de Ciencia y Corfo lanzan Startup Ciencia », Institut national de recherche en sciences et technologies du numérique, 25 mai.

[2] Site web : http://www.sesantiago.cl/

impulsion supplémentaire. Plus récemment, l'IdO a été mentionné dans le quatorzième plan quinquennal (2021-2025) général, ainsi que dans sa déclinaison pour les technologies ICT (mentionné 36 fois). L'accent est notamment mis sur le développement de l'IdO cellulaire et sur l'intégration avec les réseaux LTE/5G.

En septembre 2021, le MIIT et huit autres administrations publient le plan triennal pour l'établissement des infrastructures pour l'IdO (2021-2023). Celui-ci fixe plusieurs objectifs principalement nationaux : création de dix entreprises IdO dont la valeur de la production doit excéder 10 milliards de yuans d'ici 2023 ; amélioration du système de standardisation (et de la sécurité des réseaux) ; développement d'applications dans les villes intelligentes et applications industrielles ; promotion à grande échelle d'IPv6. Les projets d'investissements dans les « nouvelles infrastructures » (5G, cloud, Internet satellitaire, etc.) permettront de rendre plus efficaces et plus rapides les communications entre appareils constituant un réseau IdO. Ce plan triennal pour l'établissement des infrastructures pour l'IdO promeut l'intégration de la 5G, du Big Data, de l'IA et de la *blockchain* au développement de l'IdO. En ce sens, la volonté de développement de l'IdO en Chine peut être comprise, du moins partiellement, comme un effort de développement d'un secteur pluriel, qui viendra de fait compléter, voire irriguer celui d'autres secteurs identifiés comme prioritaires.

Selon le livre blanc 2020 du CAICT, le secteur de l'IdO en Chine a crû de 20 % annuellement sur la période 2016-2020, et représentait en 2020 une industrie de l'ordre de 236 milliards d'euros. L'Internet des objets est d'abord employé pour les solutions de « maisons intelligentes » (43 %) – avec la présence notamment de Xiaomi : l'entreprise prétend que 30 % de son chiffre d'affaires en 2019 est généré par le secteur des produits IdO. Viennent ensuite les solutions de véhicules connectés (11 %), de services publics (8 %), d'agriculture intelligente (7 %), de logistique (5 %), de services de détails (3 %), l'industrie et les soins de santé ne représentant chacun que 1 %.

Au Japon, on compte environ 1 milliard d'objets connectés à internet (tous objets confondus) en 2021 (contre 800 millions en 2018). Près de la moitié correspondent à des connexions de machine à machine (M2M). Sur le segment des particuliers (B2C), la récente baisse du prix des abonnements de télécommunications et l'émergence de la 5G promettent une expansion des usages et services liés aux objets connectés. Néanmoins, le marché de l'IdO qui cible les particuliers ne semble pas être le plus développé, car on constate que la propension du consommateur final japonais à payer pour le service associé est assez faible. En revanche, le marché B2B est en croissance, tiré par des secteurs comme l'automobile (véhicules connectés), l'énergie (compteurs connectés), la livraison (drones), la sécurité ou encore la santé. Environ 14 % des entreprises japonaises déclarent utiliser l'Internet des objets en 2020 pour leur activité et 10 % envisagent de l'utiliser dans un avenir proche, cette tendance touchant toutefois davantage les grandes entreprises que les PME[1].

Source : Direction générale du Trésor ; pour un tableau par pays et des sources détaillées, voir annexe 7

[1] Voir le Livre blanc du ministère japonais de l'Intérieur et des Communications (MIC) sur le secteur des télécommunications et du numérique.

CHAPITRE 4

DOUZE CAS D'USAGE

Les cas d'usage exposés ici sont issus des travaux de BCG et EY-Parthenon. France Stratégie ne fait que relater les références présentées par ces deux cabinets[1]. Les chiffres qui sont présentés ci-après sont donnés à titre indicatif et ne relèvent pas d'une analyse menée par France Stratégie.

1. Des exemples remarquables dans six domaines

Les prochaines années vont connaître une accélération massive du déploiement de l'Internet des objets dans presque tous les secteurs de la production de biens et services et dans notre vie quotidienne. **L'examen des cas d'usage proposés a pour objectif de donner à voir les conditions de mise en œuvre de ces dispositifs, les bénéfices que ces solutions peuvent apporter tout en attirant l'attention sur les risques qui pourraient en découler**, pour les usagers, pour les citoyens mais aussi pour les entreprises.

Nous présentons des cas d'usages qui sont à la fois révélateurs :

– de la maturité des technologies utilisées et de leur capacité à émerger rapidement sur les marchés ;

– des évolutions sociales à venir, de cette transformation de notre vie quotidienne et du monde du travail mais aussi des modes de production de biens ou de services que l'on voit déjà se dessiner dans les secteurs des transports, de l'industrie ou de l'agriculture ;

– des enjeux environnementaux posés par leur généralisation et leur massification ;

– des enjeux de politiques publiques qu'ils peuvent soulever.

Pour étayer nos choix, nous avons considéré un faisceau de critères explicités dans le Tableau 10 page suivante.

[1] Voir la présentation des travaux en annexe 5.

Tableau 10 – Critères de sélection des cas d'usage étudiés

	Choisir des cas d'usage représentatifs des différentes catégories de données ou typologies de capteurs, par exemple : • Données relatives à l'activité de l'usager (rythme cardiaque, nombre de pas, etc.) • Données relatives à l'environnement (température, hygrométrie, qualité de l'air, etc.) • Données relatives à un processus (traçage de bout en bout d'un produit alimentaire, etc.)
	Couvrir une large partie de la douzaine de politiques publiques suivantes : mobilité, énergie, déchets et eau, emploi et dynamisme économique, sécurité et sûreté, services aux citoyens, santé, logement et habitat, voirie et propreté, action sociale et solidarité, culture, éducation.
	Couvrir les différents secteurs économiques (industrie, santé, énergie, transport, commerce, assurance, agriculture, etc.) et les différentes technologies (LAN, cellulaire, LPWAN).
	Illustrer des effets de système et d'hybridation de l'IoT. • Usages multiples pour un capteur (montre connectée pour un usage de santé et de géolocalisation, par exemple).
	Se projeter à horizon de cinq ans sur la base des études de tendance en incluant des cas d'usage développés et prometteurs.
	Identifier des cas d'usage avec un impact direct/indirect fort sur les citoyens.
	Identifier des cas d'usage qui impactent l'ensemble de la population sur toutes les tranches d'âge.

Sources : France Stratégie - BCG et EY-Parthenon

Nous avons également souhaité examiner des cas d'usages qui soient représentatifs de champs applicatifs, en sélectionnant nos exemples au sein de six grands domaines :

- la vie quotidienne ;
- la ville et les mobilités ;
- la maison et le bureau intelligents ;
- la santé ;
- l'usine, le transport et la logistique ;
- l'agriculture et l'écologie.

Cette première approche nous a permis d'identifier près de **soixante-cinq cas d'usage qui nous paraissent particulièrement représentatifs,** qu'ils soient déjà largement adoptés ou prometteurs et dont la généralisation devrait se confirmer dans les deux à cinq prochaines années.

Tableau 11 – Les six domaines, les soixante-cinq cas d'usage et les douze cas retenus

Vie quotidienne	Maison et bureau intelligents	Usine, transport et logistique
Commerce de proximité • Paiement automatique (Caddie intelligent) • Gestion des stocks • Promotion et prix en temps réels **Divertissement et Culture** • TV connectée • Autosurveillance de l'activité et du bien-être personnel • Montre connectée • Téléphone connecté • Vêtement connecté • Assistant vocal / personnel intelligent • Jouets connectés • Œuvres d'art connectées	**Maison intelligente** • Suivi de consommation en temps réel / compteur intelligent d'eau, d'électricité ou de gaz • Contrôle à distance d'appareils électro-ménagers • Éclairage intérieur intelligent • Surveillance et détection d'intrusion (caméras, détecteurs) **Bureaux et salles de classe intelligents** • Climatisation et chauffage intelligents • Gestion des espaces de travail	**Industrie manufacturière** • Automatisation et optimisation d'usine • Gestion d'équipement à distance • Entrepôt intelligent • Suivi de qualité • Maintenance prédictive • Prévention de risque et accidents • Optimisation de la consommation énergétique • Travail augmenté • Contrôle d'accès (badges connectés) **Transport de marchandise et logistique** • Gestion des stocks • Suivi et traçabilité des marchandises • Gestion de flotte • Maintenance prédictive (avion, train, bateau, bus) • Énergie et ressources naturelles • Gestion de centrale à distance • Forage minier autonome
Ville et mobilités	**Santé**	**Agriculture et écologie**
Mobilité urbaine • Parking intelligent • Véhicule connecté • Gestion dynamique du trafic • Suivi de flotte (bus publics et scolaires) • Gestion mobilité douce (dont trottinettes, vélos électriques, etc.) **Espace public** • Éclairage intelligent • Surveillance intelligente : reconnaissance faciale, détection des armes à feu et objets dangereux • Gestion des déchets **Aéroport / Port / Gare** • Entretien intelligent (sols, sanitaires) • Gestion du trafic sur le tarmac • Localisation et suivi de conteneurs • Affichage dynamique • Maintenance prédictive	**Santé de chacun** • Suivi, diagnostic et prévention de santé à distance **Hôpital** • Chirurgie à distance • Équipements connectés à l'hôpital (y compris la maintenance prédictive des équipements) • Gestion des stocks de médicaments et petits dispositifs médicaux • Surveillance médicale des patients à distance • Ambulance connectée	**Agriculture** • Suivi du bétail • Système d'irrigation intelligente • Suivi des sols • Automatisation de la récolte **Environnement** • Gestion de barrages • Anticipation et gestion climatique • Monitoring de la qualité de l'air et de la pollution sonore

Sources : France Stratégie - BCG, EY-Parthenon

Dans cet ensemble, nous avons donc sélectionné douze cas d'usage, à dire d'experts, présentés ici de façon plus approfondie. Pour chacun d'entre eux, l'analyse s'articule autour d'une grille de lecture qui comporte six items.

Tableau 12 – Critères de sélection des cas d'usage étudiés

Maturité technologique et économique	• Technologies en phase de test laboratoire, en phase de développement ou déjà déployée • Technologie de rupture ou amélioration incrémentale • Si la technologie est déjà mise sur le marché, quelques indicateurs économiques • Potentialité d'impact sociétal disruptif majeur
Impacts environnementaux connus ou anticipés	• Analyse du cycle de vie • Empreinte écologique directe ou indirecte, contribution à la maîtrise des émissions de gaz à effet de serre • Niveau de consommation énergétique à l'utilisation et si possible selon les phases du cycle de vie
Impacts potentiels de transformation sociale	• Quels bénéfices potentiels ou déjà identifiés pour l'usager et pour la collectivité ? • Quels impacts sur l'emploi et l'organisation du travail ?
Enjeux liés à l'exploitation des données	• Données recueillies, typologie et modalités de leur stockage • Type de traitement, d'utilisation et de valorisation de ces données • Enjeux de souverainetés (numérique, sanitaire, environnemental, défense, etc.)
Cadre de régulation national et international	• Cadre spécifique de régulation ou le cadre général de régulation qui s'applique • Articulation ou pas entre les différents cadres (France, Europe et international hors Europe)
Débats et conditions d'acceptabilité	• Débats passés ou actuels, notamment à l'occasion du déploiement. Si les débats sont organisés par les pouvoirs publics, en donner les principales caractéristiques (référendum, débats parlementaires, conférences citoyennes, etc.) • Enjeux en termes de surveillance ou de sécurité des utilisateurs

Sources : France Stratégie - BCG et EY-Parthenon

2. Description de douze cas d'usage

Les cas d'usage qui sont résumés ci-après ont un fort potentiel sur les deux à cinq années à venir. Ils sont déjà matures ou plus prospectifs mais avec une forte présomption d'être adoptés rapidement. Ils sont représentatifs de différentes technologies disponibles : typologies de capteurs, réseaux mobilisés. Ils couvrent des secteurs économiques variés et peuvent avoir sur les chaînes de valeur ou les verticales économiques concernées des impacts de nature diverse. Ils illustrent non seulement les différentes catégories de données qui peuvent être utilisées mais aussi les effets d'hybridation entre secteurs et concernent des usagers de toutes les tranches d'âge.

Tableau 13 – Les douze cas d'usage retenus pour une analyse détaillée

Thématique	Sous-thématique	Cas d'usage	Description	Potentiel élevé à 2-5 ans	Justification de la sélection
Vie quotidienne	Divertissement et culture	Jouets connectés ou intelligents	Jouets pour surveiller ou localiser les enfants ou compagnons virtuels intelligents (peluches, poupées)	✓	• Cas d'usage en développement • Impact citoyen direct fort • Impact sur une population jeune et à risque
	Divertissement et culture	Assistants virtuels	Haut-parleur sans fil intégrant un assistant virtuel/intelligence artificielle avec laquelle l'utilisateur peut interagir en langage naturel	✓	• Cas d'usage développé • Impact citoyen au quotidien fort • Enjeux forts sur l'usage de la donnée (écoute données personnelles)
Ville et mobilités	Espace public	Surveillance intelligente	Détection automatisée de situations à risque par l'analyse des données des caméras de rue, des capteurs, etc., pour renforcer la sécurité	✓	• Cas d'usage développé • Existant dans des pays en développement (Chine) et avec de forts enjeux de données
	Mobilité urbaine	Gestion dynamique du trafic	Objets connectés permettant l'optimisation du trajet pour les citoyens et entreprises (affichage dynamique, péage dynamique, etc.)	✓	• Cas d'usage en développement • Caractère original et usages multiples (livraison, personnel, etc.) • Impact direct fort sur le citoyen
Maison et bureau intelligents	Maison intelligente	Suivi de consommation d'électricité en temps réel	Compteur avec technologie AMR (Automated Meter Reading) qui mesure de manière détaillée et en temps réel la consommation d'électricité	✓	• Cas d'usage développé • Enjeux environnementaux forts d'optimisation énergétique
	Bureau ou salle de classe intelligente	Gestion des espaces de travail et des classes	Optimisation des espaces de travail (espace disponible, connexion équipements des bâtiments, suivi du nombre d'employés présents, etc.)	✓	• Cas d'usage en développement • Expansion rapide et forte depuis le Covid / sujet d'actualité grandissant
Santé	Hôpital	Équipement connecté (incluant la maintenance prédictive)	Équipements connectés permettant d'informer l'équipe médicale en temps réel, dans l'hôpital, en incluant la maintenance préventive	✓	• Cas d'usage en développement • Impact citoyen direct et fort • Multi-usages sur différentes pathologies
	Santé de chacun	Suivi, diagnostic et prévention de santé à distance	Suivi à distance et en temps réel de fonctions de santé via des capteurs et vêtements connectés hors hôpital, pour améliorer la prévention	✓	• Cas d'usage développé • Impact citoyen direct et fort • Multi-usages sur différentes pathologies

Thématique	Sous-thématique	Cas d'usage	Description	Potentiel élevé à 2-5 ans	Justification de la sélection
Usines, transport et logistique	Industrie manufacturière	Automatisation et optimisation de la production	Utilisation des technologies IoT pour automatiser des tâches de travail en usine et ainsi optimiser la production	✓	• Cas d'usage développé • Multi-usages • Impact direct sur les conditions de travail
	Industrie manufacturière	Travail augmenté	Utilisation de technologies portables qui augmentent l'environnement de l'usine avec des données sensorielles générées par ordinateur	✓	• Cas d'usage en développement • Caractère original du cas d'usage et impact direct sur le travail des citoyens • Impact direct fort sur le citoyen
Agriculture et écologie	Agriculture	Suivi de la qualité des sols et suivi de production	Analyse des sols à l'aide de capteurs au sol et drones aériens pour suivre les paramètres, améliorer la production et l'élevage	✓	• Cas d'usage développé • Enjeux environnementaux forts de protection des sols et sur l'agriculture
	Environnement	Anticipation de difficultés liées au climat	Analyse et prédiction des événements climatiques pour déclencher des alertes et prévention auprès des autorités et individus	✓	• Cas d'usage en développement • Enjeux environnementaux forts et de protection des pays en développement

Sources : France Stratégie - BCG et EY-Parthenon

Nous résumons dans les pages qui suivent les cas d'usage étudiés[1]**.** Le nombre d'étoiles qualifie la maturité (et la croissance) du marché, depuis une étoile pour un marché très peu mature (peu croissant) jusqu'à cinq étoiles pour un marché très mature (très croissant).

2.1. Jouets connectés

Technologie très mature mais toujours en cours d'industrialisation ★★★★
Marché en pleine croissance ★★★★★

« Les jouets connectés prennent la forme d'objets d'apparence anodine (poupées, robots, montres connectées, baby-phones, consoles, etc.) qui collectent des informations et les envoient par ondes radio (Bluetooth, Wifi) et sur Internet[2]. » Ces **technologies multiformes et matures** connaissent un **très fort développement**. Sur le marché, il

[1] Les douze cas d'usage sont détaillés dans l'étude BCG/EY-Parthenon disponible sur le site de France Stratégie.

[2] Définition de la CNIL.

existe différentes catégories de jouets connectés comme le CognitToys Dino qui inclut des histoires et des jeux d'apprentissage et adapte ses réponses en fonction de l'âge de l'enfant et de ses aptitudes. Ces jouets peuvent être dotés d'un ou plusieurs équipements numériques, tels que des caméras ou des microphones, mais aussi de technologies plus évoluées de tracking, de reconnaissance vocale, de réalité virtuelle, de détection de mouvements. Des fonctions de connectivité avec d'autres appareils (assistants vocaux) peuvent également être incluses.

Ces applications utilisent le **Wifi** (pour sa présence dans de très nombreux foyers) ou le **Bluetooth** (pour sa facilité d'utilisation et sa consommation de batterie faible). Les jouets connectés sont des cas applicatifs jugés peu complexes, sans contrainte technologique forte. Cette technologie très **mature** reste **en cours d'industrialisation**. Sur le plan économique, 20 % des familles américaines ayant un enfant âgé de moins de 12 ans possèdent un jouet connecté, selon une étude Ipsos 2018.[1] Évalué à 7,62 milliards de dollars en 2020, le marché devrait enregistrer un **taux de croissance annuel moyen de 24,3 % au cours de la période 2020-2025,** selon l'étude de Mordor Intelligence[2].

Ce type d'objets connectés, mis à disposition d'enfants de plus en plus jeunes pose des questions d'éthique, de cybersécurité et de contrôle des capacités d'influence et de modification de la cognition des enfants de tous âges.

2.2. Assistants conversationnels

Technologie mature et déployée restant perfectible ★★★★
Marché mondial en forte croissance ★★★★★

« Un agent conversationnel (appelé aussi *chatbot*) est une machine qui, à travers des échanges écrits ou oraux, interagit avec son utilisateur en langage naturel. Le plus souvent, un agent conversationnel ne constitue pas une entité indépendante mais est intégré dans un système ou une plateforme numérique multitâche, comme un smartphone ou un robot[3]. » La technologie associée à ces objets connectés est **mature et déployée** mais elle reste **perfectible**.

[1] Selon une étude Ipsos réalisée aux États-Unis auprès de 5 000 familles (étude payante). Recherche documentaire, presse professionnelle, étude de Mordor Intelligence, Grand ViewResearc, Ipsos, analyse BCG et EY-Parthenon.

[2] Mordor Intelligence (2022), *Connected Toys Market. Growth, Trends, Covid-19 Impact, and Forecasts (2022-2027)*.

[3] Comité national pilote d'éthique du numérique (2021b), « Agents conversationnels : enjeux d'éthique », Avis n° 3, septembre.

Les assistants vocaux sont des solutions IdO très largement industrialisées dans les pays développés et présentent des perspectives de croissance forte. À date, la principale technologie réseaux utilisée est le Wifi. Des produits lancés depuis plusieurs années s'implantent progressivement dans les foyers et s'améliorent continuellement. En France, les perspectives de développement sont aussi importantes. Parmi les enceintes intelligentes commercialisées en France, Amazon Echo est une des solutions les plus populaires. Ce type d'objets connectés, très largement déployé, pose de sérieuses questions de cybersécurité et de respect de l'intimité. Les enjeux d'éthique sous-jacents sont en particulier analysés dans un avis du Comité national pilote d'éthique du numérique[1].

2.3. Gestion dynamique du trafic routier :

Technologie mature, déployée mais perfectible ★★★★
Marché avec une perspective de forte croissance ★★★

5G

La gestion des espaces urbains et des territoires est un domaine prometteur pour le développement de l'Internet des objets[2] mais nous avons choisi d'observer le cas de la gestion du trafic qui nous semble représentatif. La gestion dynamique du trafic comporte deux axes très imbriqués et complémentaires.

- **La gestion en temps réel de la circulation dans les agglomérations** consiste à exploiter les informations en temps réel recueillies auprès des véhicules, des infrastructures et des personnes pour une gestion active du trafic, qui intègre l'adaptation de l'offre de mobilité, voire une tarification dynamique.
- **L'assistant de voyage intermodal proactif** propose à chacun une sélection, une réservation et une navigation intermodale qui intègre tous les moyens de transport pertinents avec un seul outil mobile, en exploitant les informations en temps réel et en optimisant les besoins personnels.

Ce cas d'usage se concentre sur ces deux axes clés, l'un centré sur les acteurs publics et l'autre sur les citoyens. Les deux axes doivent *in fine* garantir à la fois la **fluidité du trafic, la qualité de l'air, les droits d'accès et la sécurité**. Ils s'appuient sur des données communes. Au total, les travaux en cours depuis plus de cinq ans sur ces sujets, dans de nombreuses régions du monde, ont conduit à imaginer une architecture de projet qui

[1] *Ibid*.

[2] Consortium Civiteo – Datactivist – Innopublica – KPMG – Parme Avocats pour le compte de la DGE, la FFTélécoms, Sycabel, InfraNum et AFNUM (2021), *De la Smart City à la réalité des territoires connectés. L'émergence d'un modèle français ?*, rapport, coll. « Les dossiers de la DGE », octobre.

permette non seulement d'optimiser les applications mais aussi une fertilisation croisée entre les différents domaines d'application.

Il s'agit d'un **cas d'usage bien avancé** puisque la situation actuelle correspond à un large ensemble d'initiatives. Cependant l'enjeu est la **mise à l'échelle** de concepts déjà éprouvés lors des pilotes. Sur la partie gestion globale, de nombreuses expérimentations plus ou moins étendues permettent de progresser. Les exemples les plus connus sont le péage dynamique à Londres et à Singapour, l'affichage dynamique à San Francisco. Sur la partie assistant de voyage, les exemples les plus avancés sont des applications comme MyTransport.SG (Singapour). Plusieurs projets et initiatives incluant des acteurs publics et des GAFA visent à identifier de nouvelles solutions de gestion de la mobilité en Île-de-France (projet à Paris Saclay avec le soutien des autorités locales, pour définir l'avenir des autoroutes urbaines). Ces **investissements** sont **conséquents** pour les pouvoirs publics. Les coûts peuvent varier entre 150 000 et 900 000 euros[1], voire plus, pour doter un tronçon de 6 km des plus récentes technologies de commande de feux adaptative. Cela représente environ 140 millions d'euros pour une ville avec 1 600 km de rues comme Paris.

2.4. Surveillance intelligente

Technologie déployée industriellement ★★★★★
Marché en forte croissance avec des taux d'adoption différents selon les zones géographiques ★★★ **5G**

Les solutions IdO de surveillance intelligente permettent de **surveiller les villes en temps réel** afin de réagir de manière proactive aux éventuelles menaces grâce notamment à la reconnaissance faciale ou à la détection d'armes ou d'objets dangereux. Ces technologies regroupent principalement **des caméras de surveillance connectées** mais aussi des **drones**, des **capteurs de mouvement**, des **capteurs sonores**, des **détecteurs de fumée** etc. Ces technologies impliquent de **nombreuses parties prenantes,** que ce soit les forces de l'ordre, les collectivités et les villes, les entreprises type SNCF ou RATP qui s'équipent de ces solutions de surveillance, les citoyens qui sont le sujet de la surveillance mais également les entreprises privées qui fournissent les solutions IdO (et peuvent proposer leur gestion). Dans le monde, de nombreux exemples d'initiatives de surveillance incluent des solutions IdO. À New York, par exemple, a été mis en place un réseau de surveillance et de détection des menaces terroristes.

[1] CAA (s.d.), *Les systèmes de gestion de circulation*, volume 1, *Le problème de la congestion urbaine au Canada*.

Ce cas d'usage illustre une technologie **déployée industriellement**. Selon Gartner[1], les caméras de surveillance extérieures constituaient le plus grand marché pour les solutions Internet des objets 5G en 2020 (70 % de la base installée des terminaux IdO 5G en 2020). Elles constitueront encore le deuxième plus grand marché en 2023. Selon cette même source, à l'échelle mondiale, plus de la moitié des dépenses des gouvernements en matière de terminaux et de services de communication IdO seront consacrées à la surveillance extérieure. Toutefois, le niveau d'adoption de ces technologies reste très dépendant des contextes nationaux. De toute évidence, certains modèles semblent inacceptables en France, comme l'ont montré les débats sur l'utilisation de la reconnaissance faciale à l'occasion de l'adoption de la loi sur la sécurité globale en 2021[2].

2.5. Suivi de consommation d'électricité en temps réel

Technologie mature et déjà déployée ★★★★★
Marché en forte croissance ★★★

Le compteur connecté d'électricité est capable de **suivre en temps réel la consommation électrique d'un bâtiment, d'une entreprise ou d'un foyer**. Ce compteur communiquant transmet les données de consommation en temps réel au gestionnaire du réseau de distribution d'électricité. Le traitement de ces données permet une large variété d'applications : relevé de compteur à distance, optimisation du planning de production, détection automatique d'incident, etc.

Les compteurs connectés sont déjà déployés dans de nombreux pays avec des taux de pénétration assez élevés. Ils **reposent sur des technologies matures et présentent des avantages économiques** estimés à 90 euros par compteur[3].

En France fin 2021, 35 millions de compteurs connectés[4] auront été installés alors que l'Allemagne vise un déploiement complet en 2032.

[1] Sources : Gartner (2021), « Gartner says global government IoT revenue for endpoint electronics and communications to total $21 billion in 2022 », communiqué de presse, 30 juin ; analyse EY-Parthenon et BCG.

[2] CNIL (2021), « La CNIL rend son avis sur la proposition de loi "sécurité globale" », Commission nationale de l'informatique et des libertés, 3 février.

[3] Sur la base d'une expérience BCG en Australie. Facture moyenne d'un ménage de 993 euros. Source : recherche documentaire, presse professionnelle.

[4] *Advanced Metering Infrastructure* (« infrastructure de mesure avancée »).

BRÈVES DU MONDE

En Estonie, dans le cadre de l'Electricity Market Act[1] de 2003, le gouvernement a exigé que tous les compteurs électriques soient remplacés par des compteurs intelligents. Chaque utilisateur peut ainsi surveiller précisément sa consommation et le mix énergétique de l'électricité qu'il consomme, et les adapter au besoin. Depuis l'Electricity Market Act de 2013, chaque citoyen peut librement choisir son fournisseur d'énergie – notamment en se fondant sur les informations récupérées avec ces compteurs connectés.

En Lituanie, Sigfox tente d'investir le marché de compteurs d'eau intelligents. L'entreprise française propose d'ores et déjà certaines de ses solutions à des municipalités. Contrairement au marché public relatif aux compteurs électriques qui a été passé au niveau national, les municipalités sont en charge des appels d'offre pour les compteurs d'eau. Sigfox Lithuania est la branche baltique (anciennement nommée 0G Baltic) de Sigfox.

Source : Direction générale du Trésor ; pour un tableau par pays et des sources détaillées, voir annexe 7

2.6. Gestion des espaces de travail

Technologie mature en cours de déploiement ★★★★

Coûts d'exploitation et de maintenance réduits, économies d'énergie ★★★★

Les solutions IdO peuvent améliorer l'expérience de travail et le confort au bureau en optimisant l'occupation de l'espace et en réduisant les coûts de fonctionnement (électricité, eau, nettoyage, gardiennage). Elles permettent également d'augmenter la productivité des salariés. Ainsi se trouvent garanties une **optimisation économique importante** mais aussi une réponse aux **attentes des collaborateurs** et aux enjeux de **transformation des espaces de travail**. Dans ces solutions IdO, on trouve des capteurs de température, d'humidité et de lumière, des capteurs de présence, des capteurs d'entrées et de sorties (accès aux immeubles ou parkings), des systèmes de réservation connectés, des capteurs sur les bureaux (ergonomie du poste de travail). Les technologies réseaux utilisées sont la Wifi ou le LPWAN, selon la quantité de données nécessaire au cas d'usage, sur des réseaux privés en général. Ces technologies sont **matures et en cours de déploiement.**

La crise du Covid a accéléré le développement des technologies pour gérer les espaces et le nombre de personnes présentes dans les bureaux ou les classes afin d'assurer le respect de la distanciation physique. De nombreux acteurs se sont lancés sur le marché

[1] Electricity Market Act – Riigi Teataja.

avec des technologies plus ou moins pointues. Par exemple, Cisco propose un écran de contrôle des salles avec des capteurs de température, de qualité de l'air, etc.

Sur le plan économique, ces technologies permettent une réduction des coûts d'exploitation et de maintenance mais aussi des économies énergétiques de l'ordre de 20 % à 30 % de la consommation[1].

2.7. Suivi, diagnostic et prévention de santé à domicile

Technologie déployée en phase expérimentale ★★★★

Marché en forte croissance ★★★★★

5G

Les solutions IdO de prévention, suivi, diagnostic à domicile permettent de **surveiller les constantes vitales** (tension, rythme cardiaque, etc.) et plus largement la **bonne santé des patients**. Cela est rendu possible par des **technologies portables ou des équipements médicaux à domicile** connectés à un cloud ou à un serveur de proximité qui collectent des données de façon régulière, voire en **temps réel**.

Il existe de nombreuses technologies IdO de prévention, de suivi et de diagnostic à distance, dotées de capteurs corporels ou intégrés dans le domicile. Des dispositifs comme les montres, les bracelets, les ceintures connectées pour la surveillance des grossesses, les chaussettes connectées pour diabétiques, les balances ou les lits sont déjà **déployées et en constant développement**. D'autres sont encore en phase expérimentale. Elles s'appuient principalement sur le **Wifi et le Bluetooth pour la partie à domicile, sur la 4G/5G quand l'individu se déplace**. Les bénéficiaires peuvent être les patients de retour au domicile après une hospitalisation, des personnes souhaitant suivre leur état de santé par prévention mais également les professionnels de la santé qui reçoivent les données.

2.8. Équipements connectés à l'hôpital

Technologie en phase expérimentale ★★★★

Marché en forte croissance ★★★★★

5G

[1] Sur la base de Wattsense, start-up française spécialisée dans la gestion de bâtiments de petite et taille intermédiaire, qui propose avec Schneider des dispositifs simples permettant d'attester les besoins énergétiques d'un bâtiment afin de réaliser des économies d'énergie.

Les objets connectés à l'hôpital peuvent **améliorer les soins de santé (sécurité et qualité), fluidifier le parcours (connectivité entre les professionnels) et numériser les processus**. En effet, les équipements connectés dans les blocs opératoires permettent d'améliorer les techniques de soins aux patients en réduisant les risques d'erreur. Aujourd'hui, il y a un fort besoin de fluidifier et de sécuriser les données des patients, mais aussi de simplifier les prises de rendez-vous, de repérer les équipements mobiles comme des brancards, de gérer les stocks de médicaments ou de dispositifs médicaux. En outre, la numérisation des processus en interne devrait permettre aux services supports de gagner en qualité et en productivité. Ainsi, l'Internet des objets **améliore le fonctionnement quotidien des hôpitaux.**

Ici, **trois solutions IdO** sont étudiées. Elles recouvrent l'ensemble du parcours d'un patient dans un hôpital et transforme le mode de gestion des établissements, depuis la localisation des équipements médicaux jusqu'à l'opération chirurgicale connectée, en passant par la maintenance prédictive des équipements connectés. Chacun des cas d'usage impliquent des solutions différentes (capteur de localisation sur les équipements et fournitures, lunettes connectées, etc.).

Différentes initiatives à Paris concernent l'hôpital connecté. L'AP-HP s'est ainsi doté d'un entrepôt de données de santé qui rassemble, standardise et structure les données administratives et cliniques, les comptes rendus d'hospitalisation, les prescriptions, les résultats d'examens biologiques et d'imageries de plus de 13 millions de patients.

Les usages IdO dans les hôpitaux se développent progressivement, souvent encore au stade expérimental. Aujourd'hui, ils concernent surtout le fonctionnement de l'hôpital – gestion des stocks de médicaments, localisation des matériels – mais ils pourraient évoluer vers des technologies pour les patients. Des utilisations sont ainsi envisagées pour la chirurgie mini-invasive (imagerie vidéo reliée à des instruments longs et fins). Les solutions IdO avancées à destination des blocs opératoires en sont encore au stade expérimental.

Sur le plan technologique, les hôpitaux intelligents doivent déployer leur propre réseau et une capacité dédiée pour garantir la protection des données personnelles. Selon le cas d'usage, ils utilisent des **réseaux privés, la Wifi, la 4G ou 5G** pour les débits importants comme la réalité augmentée ou la maintenance préventive d'équipements, ou du **Lora** pour les cas nécessitant moins de débit comme la localisation d'individus dans un hôpital.

2.9. Travail augmenté en usine

Technologie déployée mais recherche en cours sur les perspectives de développement ★★★ **5G**

Marché en forte croissance ★★★★★

Le travail augmenté repose sur l'usage des nouvelles technologies permettant à l'employé d'être mieux informé pour une **meilleure prise de décision dans une situation donnée ou d'être assisté lors d'une manœuvre**. Il repose sur la combinaison d'objets connectés et de technologies de réalité augmentée ou virtuelle (casque RV, mobile, tablette, lunettes RA). Les applications sont particulièrement intéressantes dans les domaines de la maintenance, du contrôle qualité ou de la logistique. Les technologies mobilisées – **Intelligence artificielle, jumeaux numériques, fabrication 3D –** ont connu un fort développement ces dernières années. Il existe un enjeu actuel de **passage à l'échelle**[1], avec des défis technologiques et organisationnels encore importants. En France, par exemple, la réalité mixte est utilisée pour le contrôle qualité moteur de la ligne de production Renault Truck à Lyon. Elle met à disposition des outils d'aide à la décision sur les tâches et les contrôles les plus complexes. Selon les informations fournies par les cabinets BCG et EY-Parthenon, la maintenance pourrait permettre une baisse des coûts par l'efficacité des opérations et la réduction du temps de formation, ainsi qu'une augmentation du chiffre d'affaires de 1,2 %. Le coût de la mise en œuvre est estimé à 0.4 % du chiffre d'affaires (CA). Quant à la logistique, elle permettrait une réduction des coûts de 0, 5 % du CA et une augmentation des revenus de 0,2 %. Sa mise en œuvre est estimée à 0,2 % du CA.[2]

2.10. Automatisation et optimisation d'usine

Technologie moyennement mature ★★★

Amélioration de la productivité
mais les coûts d'installation restent élevés ★★★★★

L'automatisation et l'optimisation de la production repose sur :

– un **ensemble d'objets connectés** couvrant toute la chaîne de valeur de la production ;

– une forte composante **d'intelligence artificielle** notamment pour les tâches répétitives ;

– **l'intégration de données** amont (fournisseurs) et aval (clients).

[1] Selon Microsoft, « si ces technologies sont de plus en plus répandues, de nombreux projets s'enlisent dans les étapes d'essai/preuve de concept en raison de lacunes infrastructurelles et de la complexité du travail d'évolutivité et de gestion des systèmes ». Voir Microsoft (2021), *IoT Signals*, *op. cit.*, p. 5.

[2] Selon le cabinet BCG, cette étude de cas repose sur l'hypothèse suivante : un fabricant avec un chiffre d'affaires annuel d'environ 3 milliards de dollars et un chiffre d'affaires annuel de service après-vente d'environ 1 milliard de dollars. Employant 1 000 ingénieurs de service, dont seulement 20 % à 30 % utilisent une solution IoT-AR. Ces chiffres s'appliquent pour une entreprise avec un chiffre d'affaires élevé. Les gains d'efficacité et de productivité sont possibles pour les entreprises ayant les moyens d'adopter ces technologies.

L'automatisation et l'optimisation de la production repose sur de nombreuses avancées technologiques récentes, incluant les imprimantes 3D, les robots avancés, la réalité augmentée, les objets connectés mais aussi une forte composante liée au traitement de la donnée à grande échelle nécessaire à l'optimisation des processus de production. Associées à l'IA, les applications d'IdO peuvent améliorer la **productivité comme la qualité, permettre une plus grande efficience en matière de consommation énergétique et de matières premières**. L'automatisation de la production regroupe différents usages permettant d'améliorer les opérations (pilotage de production), le suivi de la performance (tableau de bord électronique) et l'implication des employés (formation immersive). Différentes technologies, notamment les jumeaux numériques de la production et de la logistique, assurent des gains dans les vitesses de construction ou d'adaptation des sites.

L'enjeu actuel est la **mise à l'échelle de concepts déjà prouvés**, car on est déjà bien au-delà des pilotes. Selon une étude de cas fournie par BCG et EY-Parthenon, cette solution IdO repose sur différentes **technologies et techniques qui ne sont pas toutes matures**, mais elle pourrait permettre à terme une amélioration de la productivité de 10 % à 15 % sur le court terme et de 20 % à 40 % sur le long terme. Cependant, les coûts de mise en œuvre restent relativement élevés et dépendent de la complexité du processus de fabrication ainsi que de la taille de l'usine[1].

2.11. Suivi des sols

Technologie en cours de développement ★★★

Marché avec une perspective de croissance forte ★★★★★

Différents types de sols peuvent être suivis (agricoles, forestiers, miniers, urbains, désertiques, marins, etc.). Le cas d'usage étudié ici se focalise sur les **terres agricoles**. Dans ce domaine, l'Internet des objets peut permettre de **meilleures prises de décision sur la chaîne de valeur agricole**.

Les objets connectés qui permettent le suivi des sols s'appuient sur des capteurs et des caméras fixés au sol, sur des drones, etc. Ils récoltent des données comme la composition organique ou des données topographiques. Les objectifs peuvent être d'optimiser la production, de limiter les intrants ou de détecter des signes cliniques liés à la présence de parasites ou de maladies. En somme, ce cas d'usage vise à faciliter la gestion des terres agricoles ou d'élevage. Selon un entretien expert mené par BCG et EY-Parthenon, il

[1] Source : BCG (s.d.), page « Industry 4.0 ». Chiffres variables selon le niveau de développement de l'usine.

permettrait une hausse des rendements pouvant aller jusqu'à 20 %[1] selon les zones. L'analyse de BCG et EY-Parthenon indique que le suivi des sols peut entraîner une **baisse des coûts d'exploitation en diminuant les intrants** (fertilisants, pesticides, eau)[2]. Il s'agit d'un **cas d'usage peu avancé** car les coûts de mise en œuvre restent relativement élevés. L'enjeu actuel est la mise à l'échelle de concepts déjà prouvés lors des premiers pilotes. Le suivi des sols repose sur des objets connectés (drones, robots, avions, etc.) et des **technologies sous-jacentes en cours de développement**. En effet, l'exploitation des données est ici un champ d'innovation majeur (cybersécurité, notion de bien commun). La question de l'interopérabilité se pose alors car les nombreux outils et plateformes ne suivent pas toujours les mêmes normes technologiques.

2.12. Anticipation et gestion climatique

Technologie en cours de développement ★★★

Marché avec une perspective de croissance forte ★★★★★

Les cas d'usage liés aux risques climatiques se structurent autour de trois fonctions :

- **modélisation, anticipation, prévision** : il s'agit de suivre en temps réel des indicateurs climatiques clés pour améliorer la prévision et l'anticipation ;
- **alerte** : il s'agit de développer des systèmes d'alerte performants à destination des autorités et des populations ;
- **gestion opérationnelle** : le but est de collecter des données relatives à une catastrophe en temps réel pour adapter et coordonner les actions des intervenants.

L'anticipation et la gestion des catastrophes climatiques est un enjeu économique majeur, car l'impact s'annonce grandissant, avec des dommages d'ores et déjà estimés à plusieurs milliards de dollars chaque année[3]**.** Le nombre de catastrophes naturelles est en augmentation constante : il a été multiplié par cinq depuis 1970. Cela induit le développement de **nombreuses technologies** (capteurs, robots, drones, caméras, etc.)

[1] Entretien expert mené par BCG et EY Parthenon.

[2] La confirmation biologique restant nécessaire. Il ne peut s'agir que d'outils d'alerte qui nécessitent des investigations supplémentaires.

[3] Pour la France seule, la Fédération française de l'assurance estime que la facture des sinistres climatiques a triplé, passant de 1,2 milliard d'euros par an entre 1984 et 1989 à 3,6 milliards d'euros entre 2016 et 2020. Voir Ségur M. (2021), « Catastrophes climatiques : quelles limites au modèle assurantiel ? », *Futuribles.com*, 7 décembre ; ou Abadie A. (2021), « Catastrophes naturelles : la mise en garde de l'ACPR sur une hausse significative des primes d'assurance », *L'Argus de l'assurance*, 4 mai.

s'appuyant majoritairement sur des **réseaux de données structurés** où la **vitesse de transmission** et la **précision des analyses** jouent un rôle clé. Ces technologies de réseaux sont en cours de développement. Différents projets voient le jour, comme OWL, un projet open source centré sur les réseaux maillés, l'IdO et la **connectivité LoRa** : l'objectif est d'aider les services d'urgence et les victimes à rester en contact à la suite de catastrophes naturelles, en ciblant les coupures de communications qui font souvent suite aux catastrophes. Le projet Divirod propose de son côté une solution de surveillance de l'eau en continu qui améliore la prédiction des catastrophes naturelles liées à l'eau (inondations, tsunami, etc.).

Dans la suite du rapport, les douze cas d'usage retenus seront identifiés par leur numéro.

Cas d'usage n° 1 – Jouets connectés

Cas d'usage n° 2 – Assistants conversationnels

Cas d'usage n° 3 – Gestion dynamique du trafic routier

Cas d'usage n° 4 – Surveillance intelligente

Cas d'usage n° 5 – Suivi de consommation d'électricité en temps réel

Cas d'usage n° 6 – Gestion des espaces de travail

Cas d'usage n° 7 – Suivi, diagnostic et prévention de santé à domicile

Cas d'usage n° 8 – Équipements connectés à l'hôpital

Cas d'usage n° 9 – Travail augmenté en usine

Cas d'usage n° 10 – Automatisation et optimisation d'usine

Cas d'usage n° 11 – Suivi des sols

Cas d'usage n° 12 – Anticipation et gestion climatique

DEUXIÈME PARTIE

ANALYSER LES ENJEUX

CHAPITRE 5

LES ENJEUX SOCIAUX

1. Enjeux individuels

1.1. Les droits des personnes au défi de l'IdO

L'Internet des objets favorise le développement de services qui peuvent améliorer le confort et le bien-être des consommateurs, incitant ainsi à la multiplication d'objets connectés au sein du domicile. L'exposition de notre vie personnelle à une kyrielle de machines est-elle compatible avec nos libertés fondamentales et avec la protection des données et de notre vie privée ? L'invisibilité de nombreux de ces capteurs et leur omniprésence, dès lors qu'ils collectent et traitent des données personnelles, peuvent rendre difficile la mise en œuvre des exigences du RGPD (Règlement général sur la protection des données), notamment en ce qui concerne la transparence et les droits des personnes (accès, modification, limitation, effacement, opposition, portabilité). Cette prolifération des objets communicants dans les espaces privés ou publics pose aussi la question du consentement, dans les cas où cela est nécessaire – ce consentement devant être « libre et éclairé »[1].

Comment par exemple informer de ses droits – droit d'accès, droit de rectification, droit d'effacement, opposition au traitement, etc. – un usager qui circule dans un espace où se trouvent des dispositifs de détection capables de localiser son téléphone portable ? Et même dans certains cas, comment obtenir son consentement ? Les objets connectés, notamment les assistants vocaux, présente « un vrai risque d'opacité de ces systèmes (…)

[1] Le consentement est une des bases légales prévues par le RGPD sur laquelle peut se fonder un traitement de données personnelles. Le RGPD impose que ce consentement soit libre, spécifique, éclairé et univoque (audition de la CNIL le 20 septembre 2020).

et les modalités d'information et de consentement de l'individu doivent être particulièrement réfléchies[1] ».

Au quotidien, certaines situations rendront difficile ce consentement (voir les cas d'usage n° 4, 5, 6 et 7). Les droits des personnes vulnérables – personnes présentant des troubles cognitifs, enfants – doivent être examinés avec attention dès lors que ces personnes peuvent être exposées involontairement à la collecte de leurs données par ces nouveaux objets connectés (cas d'usage n° 1).

Au-delà des droits des personnes, ce sont les dispositions relatives à la sécurité et à la confidentialité des données qui méritent d'être examinées. Le cas d'usage n° 1 illustre parfaitement les dérives qui peuvent se présenter : mésusages sur les données fournies volontairement via les jouets connectés (partage de données non consenti, conservation des données au-delà de la durée de conservation autorisée, utilisation des données à des fins commerciales, sans consentement de la personne) ou encore attaque malveillante à partir des données fournies automatiquement par le système (adresse IP, historique de navigation, etc.).

Dans les espaces publics, faut-il revendiquer un droit « au silence des puces[2] » qui permettrait aux individus d'être « invisibles » et de ne pas être détectés dans leurs déplacements par exemple ? Si le législateur doit arbitrer entre la nécessité d'assurer la sécurité publique et le respect des droits et libertés fondamentales de chaque citoyen, dans quelle instance démocratique ce débat pourra-t-il avoir lieu ? La question des réseaux de caméras de vidéo-surveillance connectées et plus généralement de la surveillance dans les espaces publics a déjà permis de poser certaines de ces questions (voir cas d'usage n° 4).

La porosité des réseaux, l'invisibilité des interconnexions possibles (effet cocktail) et les multiples acteurs rendent peu transparent le cycle de vie de la donnée pour les usagers non avertis. Les cas d'usage dans le domaine de la santé révèlent ces spécificités. Les données connectées par les objets de santé sont en effet particulièrement sensibles : elles sont protégées par des dispositions spécifiques[3] mais encore faut-il que la qualification

[1] CNIL (2020), *À votre écoute. Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux*, collection « Livre blanc », n° 1, Commission nationale de l'informatique et des libertés, septembre, p. 37.

[2] AFNIC et Institut de la souveraineté numérique (2021), *Internet des objets et souveraineté numérique. Perspectives industrielles et enjeux de régulation*, rapport, mars.

[3] Dès lors que la qualification des « données de santé » est retenue, un régime juridique spécifique justifié par la sensibilité des données s'applique. Par exemple règlement général sur la protection des données (art. 8 et chapitre IX) et les dispositions relatives au secret (art. L.1110-4 du code de la santé publique).

d'une donnée de santé soit clairement établie[1]. Les données recueillies par des capteurs de type montre, ceinture, vêtements sont essentiellement des données personnelles. Il existe encore de nombreux débats sur les conditions de partage de ces données, sur leur utilisation abusive (assurances, banques) dans le cadre assurantiel ou de vol de ces données (voir cas d'usage n° 7).

S'il est indéniable que les applications et les services que permettra le déploiement de l'IdO pourront donner accès à plus de confort et de bien-être, à des services plus sûrs, il n'en est pas moins nécessaire d'anticiper les droits du consommateur et notamment son information, dans un cadre de confiance respectueux de sa vie privée et de ses droits fondamentaux.

C'est pourquoi nous proposons les pistes de recommandations n° 9, 10, 11, 12, 13, 15 et 16 (voir troisième partie).

N° 9 – Informer le citoyen sur la protection de ces données personnelles.

N° 10 – Rendre explicite l'utilisation de dispositifs IdO lors d'interventions médicales.

N° 11 – Consolider la mise en œuvre du recueil du consentement de l'usager pour les services IdO.

N° 12 – Informer les usagers de la présence de capteurs.

N° 13 – Adapter le cadre règlement actuel pour un bon niveau de protection des personnes vulnérables.

N° 15 – Confier le soin d'organiser une réflexion sur les enjeux éthiques de l'IdO au Comité national pilote d'éthique du numérique.

N° 16 – Étendre le champ de compétence de la CNDP sur les questions relatives au numérique et à l'environnement.

[1] Le statut de données de santé est établi dans le RGPD (voir la définition sur le site de la CNIL). La notion de données de santé est désormais large, mais elle est à apprécier au cas par cas, compte tenu de la nature des données recueillies. Entrent dans cette notion trois catégories de données : a) les données de santé par nature : antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc. ; b) celles qui, par le croisement avec d'autres données, deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne : croisement d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques, etc.), croisement de la tension avec la mesure de l'effort, etc. ; c) celles qui deviennent des données de santé en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical.

BRÈVES DU MONDE

En Estonie, le débat autour des données de l'IdO est le même que pour les données en général, à savoir « quelle protection ? » et « quelle utilisation ? ». Il est notamment question de laisser la possibilité aux citoyens de choisir quelles données peuvent être utilisées par l'État et par les entreprises, que ces données soient personnelles ou non. Autre débat plus général, celui du droit à l'oubli, notamment auprès des entreprises. Aucune disposition nationale ne s'ajoute à celles prévues par le RGPD. Trois explications sont avancées pour la quasi absence de débat sur l'usage et le développement de l'IdO :

- la confiance dans les institutions et le cadre légal, qui tient que si une technologie est en place, c'est qu'elle respecte les droits de chacun, notamment en matière de confidentialité ;
- l'omniprésence de l'Internet des objets, qui est considéré comme une part courante de la vie. Pour reprendre la métaphore du PDG de la start-up Eliko : les Estoniens ne « contestent pas le fait de porter des vêtements, pourquoi contesteraient-ils la présence d'objets connectés ? ».
- il y a une part d'ignorance à ne pas négliger. La plupart des Estoniens utilisent des produits sans chercher à savoir ce qu'il y a derrière (montres connectées, par exemple). Lorsqu'on prend la peine d'expliquer, des contestations peuvent naître : ainsi, à propos des smart cities, l'IoT Lab a rencontré le rejet de certains habitants qui jugent certaines technologies trop intrusives.

Au Nigéria, la question de la protection des données, bien qu'elle fasse l'objet d'une attention particulière des milieux économiques et des acteurs du digital, n'est pas un sujet central quand on évoque l'Internet des objets. Cela est principalement dû au fait que ses usages sont jusqu'à présent limités au B2B (pas ou peu de collecte de données personnelles par l'IdO). Par ailleurs, la protection des données personnelles, si elle peut être un sujet de droit, est moins un sujet de société.

Au Japon, l'opinion publique est surtout préoccupée par les questions de sécurité des données. Selon un sondage réalisé par le MIC en 2020 auprès des utilisateurs d'objets connectés, plus de 60 % des répondants ont fait part de leur inquiétude quant à l'utilisation de leurs données personnelles. La plupart des entreprises qui recourent à des solutions IdO demandent le stockage des données sur le territoire japonais et les autorités japonaises sont particulièrement attentives aux risques de fuite (notamment vers la Chine).

En Chine, les enjeux autour des données de l'IdO portent davantage sur la sécurité des données et sur la protection des données personnelles des utilisateurs que sur les risques identifiés en matière de libertés individuelles, du fait du contexte politique propre au régime chinois. Le pays s'est récemment doté d'un cadre réglementaire qui continue de s'étoffer, d'abord avec la loi sur la cybersécurité (2017), puis avec la loi sur la sécurité des données et la loi sur la protection des données personnelles, entrées en vigueur en 2021. Pour les données considérées comme peu sensibles, le gouvernement souhaite favoriser leur valorisation et leur partage en promouvant notamment la création de plateformes d'échanges. Dans l'industrie, de telles plateformes sont

déjà mises en place, liant les machines et les équipements de production entre eux afin d'optimiser la production. En amont des lois cadres et des réglementations sur les données, des entreprises comme Haier ont ainsi développé des solutions permettant de telles connexions (COSMOPLAT). Cela s'est fait dès 2015 avec l'initiative « Internet Plus », ou encore avec une injonction de la part des autorités à ce que les entreprises publiques partagent leurs données[1]. À l'inverse, d'autres données considérées comme « importantes » et « essentielles » voient leur gestion, stockage et transfert strictement encadrés. Comme prévu par la loi sur la cybersécurité (2017) et comme rappelé par la loi sur la sécurité des données (2021), ces données générées en Chine doivent être protégées via des mesures de cybersécurité strictes, au niveau technologique ou opérationnel. Elles doivent en outre être stockées sur le territoire chinois, et leur transfert est conditionné à l'obtention d'une licence de l'Administration du cyberespace (CAC) selon des termes qui se déclinent en fonction des secteurs[2]. En particulier, les entreprises qualifiées d'« opérateurs d'infrastructures critiques d'information » (CII) devront se soumettre à cette procédure d'approbation avant de procéder à tout transfert transfrontalier de données. De la même manière, les données personnelles doivent être stockées sur le territoire chinois, et leur exportation est conditionnée à une autorisation et un audit de sécurité.

En Israël, l'autorité de protection de la vie privée est chargée de veiller à la protection des données personnelles contenues dans les fichiers informatiques ou papier, aussi bien publics que privés. Cette institution a été placée sous tutelle du ministère de la Justice. La protection des données fait l'objet de débats un peu lointains – dans la presse ou sur les réseaux sociaux – mais ne semble pas inquiéter le public israélien, qui conserve une confiance bien établie en son État et qui est habitué à donner son numéro d'identité national pour toutes les démarches voire pour de simples prises de rendez-vous.

Source : Direction générale du Trésor ; pour un tableau par pays et des sources détaillées, voir annexe 7

1.2. Protéger et informer les consommateurs

En matière de droit et d'information du consommateur, l'approche par cas d'usage nous a permis de constater qu'il existait des risques en matière d'utilisation des objets connectés.

La loi affirme que le défaut ne peut pas être postérieur à la mise en circulation de l'objet et écarte la responsabilité de plein droit du producteur lorsque l'état des connaissances scientifiques et techniques au moment où le produit a été mis en circulation ne permet pas de déceler le défaut du produit. Cette disposition ne suffit pas à protéger le consommateur dans le cas d'utilisation d'un objet connecté. En effet, l'objet connecté « apprend » et

[1] Par exemple, la société de gestion des actifs d'État (ou SASAC, qui assure la gestion des actifs d'État et en particulier les SOE) a publié une liste de 28 entreprises chargées de fédérer les entreprises de leurs industries respectives en mettant en place des plateformes sectorielles visant de tels échanges de données.

[2] Pour plus de détails, voir la fiche consacrée à la Chine dans l'annexe 7.

s'adapte aux comportements de son utilisateur (notamment lorsqu'il est connecté à une IA, comme un assistant virtuel). Son fonctionnement dépend également des mises à jour correctes des couches logicielles qui lui permettent de fonctionner. Le « défaut » peut donc être l'effet d'un apprentissage ou d'une évolution logicielle qui n'était pas détectable au moment où l'objet a été vendu. En 2019, la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) a déjà alerté la plateforme RAPEX, dédiée à l'échange d'informations sur les dangers relevant de l'utilisation des produits de consommation sur un problème concernant les montres connectées pour enfant.

Mais les éléments collectés à l'occasion de la mission confirment la nécessité de conduire une **analyse approfondie des dispositions actuelles du droit de la consommation au regard des spécificités présentées par les objets connectés.**

Un autre volet nécessaire à l'émergence d'un environnement de confiance pour le consommateur est son information. Ce dernier doit pouvoir disposer des informations nécessaires à l'usage des équipements connectés qu'il utilise. Les principaux points restés sans réponse au cours de la mission portent notamment :

– sur la sûreté et la sécurité des objets. Dans le meilleur des cas, l'objet devient inutilisable, mais il peut aussi devenir dangereux (cas des objets de suivi et de diagnostic médical, voir cas d'usage n° 7) ;

– sur la notion de responsabilité en cas de dysfonctionnement de l'appareil : cette responsabilité incombe-t-elle au vendeur, à l'importateur ?

– sur les risques d'attaques malveillantes qui peuvent découler de son utilisation. Si la CNIL ou l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ont publié des recommandations sur les bonnes pratiques, une information des consommateurs plus systématique à l'occasion de l'achat du produit pourrait s'avérer plus efficace ;

– sur l'empreinte environnementale de ces appareils et de leur utilisation. Les dispositions de la loi sur la REEN[1] du 15 novembre 2021 concernant les informations relatives à l'empreinte environnementale des usages des communications électroniques pourraient être adaptées à l'usage des objets connectés.

[1] La loi n° 2021-1485 du 15 novembre 2021 vise à réduire l'empreinte environnementale du numérique en France à partir de 2024. Elle définit un référentiel général d'écoconception qui spécifiera les critères de conception durable des services numériques. Les consommateurs devront être informés en matière de consommation d'énergie et d'équivalents d'émissions de gaz à effet de serre de la consommation de données.

Afin que puissent être pris en compte les intérêts du consommateur, nous proposons les pistes de recommandations n° 21, 22, 25 et 26.

N° 21 – Sensibiliser l'utilisateur des objets connectés aux impacts de leur usage sur l'environnement mais aussi sur sa sécurité.

N° 22 – Compléter la liste des produits concernés par l'indice de réparabilité.

N° 25 – Veiller à préserver des pratiques concurrentielles sur les différents marchés de l'IdO.

N° 26 – Procéder aux analyses juridiques permettant de définir les responsabilités sur la chaîne des usages.

1.3. Assurer la portabilité des solutions IdO

Les enjeux de portabilité – soit la capacité de transférer son environnement personnel, données de paramétrage ou d'utilisation sur un autre équipement ou un autre environnement logiciel – conditionnent la sécurité et la confiance des consommateurs. Ils auront un impact sur les conditions de développement de l'IdO et de son adoption par usagers.

L'émergence de l'IdO transforme en profondeur nos modes de consommation et amplifie aussi la dématérialisation de notre vie quotidienne. Notre dépendance aux technologies numériques et aux solutions logicielles ou plateformes sur lesquelles elles s'appuient s'accroît. Ces services sont aujourd'hui détenus en grande majorité par les grands acteurs du numérique transnationaux. Et dans de nombreuses filières où la connectivité va devenir un avantage concurrentiel du produit distribué, ces acteurs vont tenter d'imposer leur modèle économique ou leurs standards pour s'assurer de la maîtrise du marché.

L'exemple des assistants vocaux est significatif. Dominé par quelques acteurs (voir cas d'usage n° 2), ce marché pourrait s'étendre au-delà de celui de l'assistant vocal individuel. Il existe des briques logicielles ou « skills » qui permettent d'ajouter de nouvelles fonctionnalités à l'assistant, en lui associant par exemple des équipements domotiques ou des véhicules intelligents. L'assistant devient ainsi, comme le smartphone, une télécommande universelle et disqualifie les équipements qui ne sont pas compatibles avec sa couche logicielle.

Du côté consommateur, cette situation pourrait entraîner un risque de *lock-in* et une dépendance à une solution technologie trop coûteuse à abandonner, bien connu des économies de réseau. On peut citer l'exemple des ampoules intelligentes commercialisées par Philips qui ne sont pas compatibles avec Alexa d'Amazon. Lors de l'achat, le

consommateur devra donc vérifier la compatibilité de ces équipements, ce qui actuellement est encore difficile en raison de l'absence d'information normalisée.

2. Enjeux dans le monde du travail

Un des principaux espaces où chacun d'entre nous est susceptible d'être concerné par le déploiement de l'Internet des objets est celui des activités productives, qu'elles soient industrielles, logistiques ou de services.

L'IdO a la maturité et la capacité à se diffuser, de façon plus ou moins perceptible pour les travailleurs, dans de multiples secteurs et métiers. Il permet de collecter des données et d'accompagner leur activité. Selon Eurofound (2021a)[1], cette technologie numérique – par rapport à l'impression 3D ou à la réalité virtuelle et augmentée – a l'un des plus forts potentiels disruptifs dans les années à venir car elle est susceptible d'impacter tous les domaines de l'organisation du travail et la plupart des secteurs et métiers.

Ce déploiement de l'IdO s'insère dans une numérisation plus globale de l'entreprise – mais aussi des organisations publiques. Il s'articule par exemple avec les technologies qui relèvent du traitement des données tels que les algorithmes ou l'intelligence artificielle ou encore les plateformes, si bien qu'il est parfois difficile d'isoler ce que sont les enjeux ou les risques propres à l'IdO. Si de nombreuses réflexions ont émergé ces dernières années de façon plus générale sur les enjeux de numérisation dans le monde du travail et en particulier autour de l'impact de l'intelligence artificielle[2], l'analyse spécifique sur l'IdO est plus récente et exploratoire. En témoignent les travaux récents, au niveau européen, relatifs à son impact sur le travail et l'emploi produits par Eurofound (2020, 2021a, 2021b)[3], ou de l'Agence européenne pour la sécurité et la santé au travail (EU-OSHA).

---

[1] Eurofound (2021a), *Digitisation in the Workplace*, Luxembourg, Publications Office of the European Union, octobre.

[2] Au niveau international, on peut mentionner les travaux de l'OCDE ayant débouché sur les principes d'utilisation de l'IA en 2019. Au niveau européen, de nombreux rapports d'expertise ont nourri la réflexion de la Commission en vue d'une réglementation propre à l'IA. Par ailleurs, en matière de conditions de travail, des travaux prospectifs ont notamment été développés au sein de l'Agence européenne pour la sécurité et la santé au travail (EU-OSHA). Voir EU-OSHA (2019), « Le numérique et la sécurité et la santé au travail : un programme de recherche de l'EU-OSHA », 16 décembre . Certaines réflexions ont été initiées par les partenaires sociaux européens tel que l'European Trade Union Institute (ETUI) : voir Ponce Del Castillo A. (2020), « Le travail à l'ère de l'IA : pourquoi la réglementation est nécessaire pour protéger les travailleurs », *Note de prospective*, n° 8, ETUI, février. Au niveau français, voir notamment France Stratégie (2018), *Intelligence artificielle et travail*, rapport à la ministre du Travail et au secrétaire d'État chargé du numérique, mars.

[3] Voir Eurofound *(*2020), *Employee Monitoring and Surveillance: The Challenges of Digitalisation*, Luxembourg, Publications Office of the European Union ; Eurofound (2021a), *Digitisation in the Workplace*, *op. cit.* ; Eurofound (2021b), *The Digital Age: Implications of Automation, Digitisation and Platforms for Work*

2.1. Les potentialités

Eurofound (2021a) identifie plusieurs registres sur lesquels l'IdO est susceptible d'affecter significativement l'organisation productive des entreprises : processus de décision, définition des tâches, contrôle qualité, supervision des travailleurs.

Tableau 14 – Domaines de l'organisation du travail les plus impactés par l'usage des technologies numériques d'après Eurofound (2021a)

	IdO	Impression 3D	RV/RA
Organisation interne et prise de décision	**Favorise une plus grande prise de décision individuelle et une communication accrue entre les services.**	Pas d'impact majeur sur l'organisation interne ou la prise de décision.	Favorise une plus grande prise de décision individuelle.
Définition et contenu des tâches	**Passage de tâches manuelles et routinières à des tâches de gestion et d'analyse.**	Accent mis sur les tâches de prétraitement/pré-production et réduction des tâches physiquement exigeantes. Passage à des tâches plus cognitives pour les travailleurs manuels.	Tâches enrichies ou simplifiées.
Flux de travail, contrôle de la qualité et normes	**Amélioration du contrôle de la qualité et optimisation des flux de travail et des processus. Flux de travail et contrôle de la qualité guidés par les données, ce qui permet une meilleure planification.**	**Flux de travail plus prévisibles et rationalisés. Processus plus flexibles favorisant la décentralisation de la production.**	**Amélioration du contrôle de la qualité et optimisation des flux de travail et des processus.**
Surveillance et contrôle des employés	**Possibilité accrue de surveiller étroitement les employés. Capacité technologique d'étendre l'utilisation des données des employés à d'autres fins.**	Aucune préoccupation particulière concernant la surveillance des employés.	Des problèmes de protection des données se posent lorsque cette technologie est associée à d'autres potentiellement plus invasives, telles que l'IdO.

Note : ce tableau est repris et traduit d'une étude d'Eurofound (2021a), s'appuyant sur des études de cas et sur une enquête Delphi auprès d'experts en 20210-2021. Voir la publication originale pour plus de précisions sur la méthodologie et le détail des analyses. Le code couleur indique dans quelle mesure les experts d'Eurofound ont jugé, sur la base d'un consensus, les impacts attendus de chaque technologie positifs (bleu) ou négatifs (orange). Le code couleur n'a pas été appliqué aux évaluations des domaines pour lesquels il n'y a pas eu d'accord global entre les experts.

Sur la base des résultats de l'enquête Delphi d'Eurofound et des études de cas, 2020-2021.

Source : Eurofound (2021a), Digitisation in the Workplace, Luxembourg, Publications Office of the European Union, octobre

and Employment, Luxembourg, Publications Office of the European Union, coll. « Challenges and prospects in the EU », décembre.

Les projections de l'impact de l'IdO sur le champ du travail restent très largement subordonnées à des enjeux d'amélioration de l'efficacité productive globale des entreprises, de la productivité du travail, de la qualité de la production.

- L'IdO offre des possibilités de profonds changements dans le pilotage par les données des processus de production, avec un impact variable sur le degré d'interdépendance et d'interaction au sein des entreprises entre différents acteurs, ou entre acteurs de la chaîne de valeur (fournisseurs et clients). Il participe à la formalisation et à la rationalisation accrue des processus de production, au repérage voire à l'anticipation sur les chaînes de production de malfaçons ou de dysfonctionnement des équipements[1]. Un contrôle qualité plus intense et continu (et non par échantillonnage) contribue à une réduction des délais et des erreurs, mais aussi à une réduction des *reporting* « papiers » puisque ces processus deviennent plus automatisés. Ils peuvent aussi en traçant l'origine d'une malfaçon identifier l'étape de la chaîne et donc potentiellement les travailleurs concernés, et permettre à ces derniers d'adapter leurs pratiques. (Voir cas d'usage n° 10.)
- Des équipements connectés portés directement par les travailleurs, ou des outils de réalité augmentée articulés avec des objets connectés, tels que des lunettes connectées ou autres assistants vocaux, permettent directement d'assister l'activité en apportant des informations voire des instructions sur la tâche à accomplir. C'est le cas notamment dans la logistique ou les activités de maintenance, secteurs où des évolutions technologiques se sont très vite développées ces dernières années. Ces mêmes équipements peuvent être dotés de capteurs faisant remonter des informations en continu sur l'activité et alimentant alors des outils de supervision et d'organisation managériaux. (Voir cas d'usage n° 9.)
- Dans le champ médical, par exemple, l'usage de l'IdO pour un « hôpital connecté » (maintenance prédictive des équipements médicaux, gestion logistique des médicaments, etc.) ou pour le suivi à distance des patients (capteurs corporels ou intégrés dans le domicile) peut faciliter le travail des soignants. Les capteurs diffusés à différentes échelles font gagner du temps en localisant le matériel, les médicaments et en permettant d'optimiser le suivi des patients selon les pathologies, grâce aux informations centralisées. (Voir cas d'usage n° 7 et n° 8.)
- Dans le champ du tertiaire et des professions intellectuelles, le lien avec l'IdO *per se* est plus indirect. La massification des données collectées en temps réel fait évoluer les tâches de conception et d'innovation en permettant une conception en 3D plus précise ou les tâches de supervision et maintenance en alimentant une représentation virtuelle

[1] Voir l'étude de la Fabrique de l'industrie : Mandon R. et Bellit S. (2021), *Vos données valent-elles de l'or ? L'Internet industriel des objets à l'épreuve du réel*, Paris, Presse des mines, coll. « Les docs de la fabrique ».

de l'ensemble d'un système productif ou d'un réseau (d'eau, d'électricité, etc.). Dans un second registre, les bénéfices productifs attendus concernent l'optimisation des espaces de travail (occupations des bureaux, mise en commun de salles de réunion et équipements par exemple) et la possibilité de développer le travail à distance, avec des conséquences notables en termes de coûts liés à l'immobilier et aux charges courantes (consommation électrique, consommables, etc.). (Voir cas d'usage n° 6.)

- La relation à l'emploi peut également être affectée par certaines formes de technologies connexes à l'IdO, telles que l'utilisation d'agents conversationnels en situation de travail. Ces outils peuvent aussi être mobilisés dans les processus de recrutement ou d'évaluation des salariés.

Conditions de travail

L'IdO peut participer à l'amélioration des conditions de travail, de la sécurité et de la santé des travailleurs de multiples manières.

- La détection continue de l'environnement des travailleurs (capteurs d'air ou luminosité, cameras, etc.) permet d'anticiper des risques (pollution dans les espaces industriels, endormissement pour des chauffeurs, etc.) ou d'adapter en temps réel l'environnement de travail (ajustement d'éclairage et de température, etc.) par exemple dans des bureaux (voir cas d'usage n° 6). Dans certaines activités relatives à la gestion du réseau d'eau ou d'électricité, le déploiement de capteurs permet une surveillance à distance, ce qui épargne à certains professionnels des risques liés à l'accès à des lieux difficiles ou dangereux.
- Des équipements (vêtements, bracelets, etc.) peuvent intégrer des capteurs corporels à même de saisir différents registres de pénibilité ou de risques physiques ou psychologiques (fatigue, tension, posture, sédentarité excessive). Ils pourraient à terme participer « en temps réel » à la démarche de prévention en termes de santé et de sécurité au travail que doivent déployer les entreprises.
- Certaines expérimentations actuelles, à partir de combinaisons équipées de capteurs, permettent d'étudier le risque ergonomique lié à la robotique et à l'interaction croissante entre robots et opérateurs dans l'industrie[1].
- L'optimisation plus générale des espaces de travail par l'IdO, notamment dans la logique des bureaux « intelligents » et de systèmes d'accès (badges, capteurs de présence, reconnaissance biométrique, etc.) peuvent aussi constituer des éléments d'amélioration des conditions de travail par une meilleure adéquation entre besoins des

[1] Inria (2021b), « Industrie 4.0 : opérateur et robot sont-ils faits pour s'entendre ? », Institut national de recherche en sciences et technologies du numérique, 7 décembre.

travailleurs et ressources logistiques (bureaux adaptés et équipement informatiques) voire en termes de sécurité sur le lieu de travail (sécurisation d'accès, intrusion). Néanmoins, lorsque ces évolutions débouchent sur des logiques de *flex office* extrêmes ou de densification des bureaux, des risques psychosociaux peuvent émerger.

Accès et qualité de l'emploi

En matière d'emploi – qu'il s'agisse de volume, de composition ou de qualité –, les perspectives sont plus ambivalentes.

- Certains équipements permettant d'augmenter les capacités des travailleurs peuvent être des facilitateurs d'insertion ou de maintien dans l'emploi face par exemple à des handicaps ou des maladies professionnelles[1].
- Des recrutements dans certains métiers se trouvent stimulés par l'IdO dans l'industrie : informaticiens et spécialistes de l'électronique embarquée, techniciens en domotique, etc. Les compétences requises ne sont pas forcément nouvelles sur le plan technologique mais plus orientées vers la capacité à faire cohabiter des solutions existantes ou en devenir[2].
- De façon plus générale, l'impact de l'IdO sur l'emploi reste largement une interrogation, à l'image des travaux sur l'effet de la numérisation sur l'emploi publiés ces dix dernières années[3]. Ceux-ci tendent à souligner l'effet substitutif de la numérisation sur les tâches routinières, physiques et de manipulation de machines, tout en mettant en valeur les tâches mobilisant les capacités intellectuelles et sociales ou mobilisant les technologies de l'information et de la communication. Si un processus de polarisation des emplois est ainsi mis en avant par différents travaux, la numérisation transforme surtout le contenu des métiers, les compétences requises pour réaliser les tâches. Dans ce cadre analytique général, quelle place occupe spécifiquement l'IdO ?
- La collecte d'information par capteurs dans l'environnement de travail est de prime abord moins substitutive à des travaux humains en termes d'automatisation. Elle

[1] Voir dans le rapport Eurofound (2021a), *Digitisation in the Workplace*, *op. cit.*, l'exemple de l'entreprise Mariasteen où un « light guidance system » facilite l'activité de personnes handicapées.

[2] Apec (2017), « L'Internet des objets. Tendance métiers dans l'industrie », 27 juin.

[3] Selon une estimation de l'OCDE, les technologies numériques source d'automatisation pourraient placer environ 14 % des travailleurs face à un risque élevé d'automatisation de leurs tâches au cours des quinze prochaines années, tandis que 30 % supplémentaires verront ces tâches changer radicalement, et avec elles les qualifications requises par leur emploi. Ce risque diffère fortement selon les secteurs et les métiers. Mais au niveau global, l'OCDE ne décèle pas sur la décennie écoulée d'effet négatif de l'automatisation sur l'emploi, celui-ci ayant progressé entre 2012 et 2019 dans la plupart des pays. La croissance de l'emploi est cependant plus faible dans les métiers à fort risque d'automatisation. Voir OCDE (2021b), « What happened to jobs at high risk of automation? », *Policy brief on the future of work*, janvier.

empiète néanmoins sur certaines fonctionnalités de nature humaine, tel le contrôle visuel et l'identification de dysfonctionnements sur la base de l'expérience personnelle. De telles évolutions induisent un déplacement du rôle des employés des taches opérationnelles vers des tâches de supervision et coordination, en mobilisant les données ainsi collectées et agrégées. Cela peut conduire à une complexification des tâches puisqu'il s'agit alors de traiter et d'interpréter un nombre toujours plus élevé et plus diversifié d'informations, de pratiquer des interventions de maintenance plus fréquentes et d'avoir ainsi une responsabilité globale accrue. De telles mutations peuvent constituer des opportunités d'évolutions professionnelles pour les salariés à même de s'y conformer et accompagnés par la formation adéquate, tout en laissant ouvert le risque de décrochage d'une partie des travailleurs. De même, l'impact sur l'autonomie et sur les marges de manœuvre des salariés est ambivalent.

- Symétriquement, l'IdO peut favoriser le développement d'emplois peu qualifiés et de moindre qualité (notamment précaire, via l'intérim et les CDD) sur des processus de production toujours plus standardisés et guidés par des dispositifs d'assistance numérique (dans la logistique, par exemple).
- L'IdO pose, comme toute dimension de la numérisation, des enjeux majeurs relatifs aux compétences et à la formation. Il ouvre d'une part des possibilités nouvelles en termes de formation des travailleurs, la virtualisation des environnements de travail permettant par exemple de proposer de nouvelles formes de mise en situation en univers virtuel (simulateur). Cela facilite des démarches de formation face à des situations de crise (simulées) difficiles à créer en situation réelle. Cependant, l'adoption de nouvelles technologies basées sur l'IdO pose la question des besoins en nouvelles compétences et de la mise à niveau des compétences numériques et de l'investissement en formation à tous les niveaux mais notamment en continu sur le lieu de travail par l'employeur pour accompagner ces transformations.

2.2. Quels risques transversaux ?

Au-delà des potentialités qualitatives, peu d'éléments sur les impacts de l'Internet des objets

Les potentialités de l'IdO – qu'il s'agisse d'organisation du travail, de redéfinition des systèmes productifs dans les entreprises et les administrations ou de répercussions plus individuelles sur les travailleurs – sont assez peu quantifiées à ce jour et relèvent plus de témoignages, de cas d'usage ou de dires d'experts. L'étude d'Eurofound (2021a) identifie ainsi différents impacts potentiels de façon qualitative, sur différents registres du travail, allant de l'environnement physique aux conditions de rémunérations (voir Tableau 15), soulignant l'ambivalence de ces effets, notamment sur les compétences ou l'autonomie.

Tableau 15 – Éléments de la qualité de l'emploi potentiellement affectés par l'utilisation de l'IdO d'après Eurofound (2021a)

Environnement physique	**Exposition réduite aux risques physiques mais augmentation potentielle de l'exposition aux risques ergonomiques.**
Environnement social	La technologie peut augmenter ou diminuer les interactions sociales en fonction de l'application particulière et de la méthode de mise en œuvre.
Qualité du temps de travail	Pas de changement dans l'aménagement du temps de travail, mais utilisation plus efficace du temps de travail. Le travail de production 24 h/24 et 7j/7 reste d'application.
Intensité du travail	**Intensité de travail plus élevée dans la phase initiale de mise en œuvre de la technologie en raison de la nécessité de s'adapter à de nouvelles tâches et responsabilités, surtout si aucune formation formelle n'est dispensée.** **Au fil du temps, diminution de l'intensité du travail pour le personnel d'atelier ou opérationnel et augmentation de la pression pour les employés occupant des postes de direction chargés d'analyser des flux de données constants et plus importants.** **Dans les lieux de travail hautement numérisés où la technologie détermine le rythme de travail et l'ordre des tâches, les risques d'intensification du travail sont importants.**
Compétences et liberté d'action	**La technologie confère une plus grande liberté d'action aux employés occupant des postes de direction et d'ingénierie et favorise l'acquisition de nouvelles compétences numériques et analytiques avancées, offrant ainsi de meilleures perspectives de carrière au sein et en dehors de l'établissement.** **La technologie réduit l'autonomie professionnelle des travailleurs chargés de la production et de l'assemblage et renforce l'organisation du travail axée sur les tâches, caractérisée par une autonomie professionnelle limitée pour ceux qui travaillent sur les chaînes de montage.** **La technologie entraîne l'acquisition de compétences numériques de base pour les ouvriers et de compétences spécifiques à la technologie, qui ne sont pas nécessairement transférables à d'autres entreprises (ce qui limite la mobilité professionnelle).** **La numérisation de la plupart des tâches des ouvriers conduit à faire progresser ces profils de poste, si des formations et des montées en compétences sont proposées.**
Perspectives et salaires	Impact sur les salaires lorsque la technologie est utilisée pour contrôler les performances des employés. Amélioration des perspectives de carrière basées sur la formation ou l'expérience, en particulier pour les employés occupant des postes d'ingénierie et de direction.

Note : ce tableau est extrait (sur le seul volet IdO) et traduit d'une publication d'Eurofound (2021a), s'appuyant sur des études de cas et sur une enquête Delphi auprès d'experts en 2020-2021. Voir la publication originale pour plus de précisions sur la méthodologie et le détail des analyses de cas. Le code couleur indique dans quelle mesure les experts d'Eurofound ont jugé, sur la base d'un consensus, les impacts attendus de chaque technologie positifs (bleu), négatifs (orange) ou neutres (mauve).

Sur la base des résultats de l'enquête Delphi d'Eurofound et des études de cas, 2020-2021.

Source : éléments extraits de Eurofound (2021a), Digitisation in the Workplace*,* op. cit.*, p. 46 et p. 50*

Même les gains en efficacité ne font à ce stade pas l'objet de consensus et les déploiements observés dans les entreprises sont encore trop expérimentaux pour rendre possible toute généralisation directement liée à l'IdO. Dans l'industrie, l'Internet des objets inséré dans une digitalisation plus large des chaînes de production donne lieu à quelques estimations de gains de productivité et d'économies, qui restent des ordres de grandeur à étayer (voir cas d'usage n° 9 et n° 10). Ainsi, dans le cas des technologies de type « bureau intelligent », quelques estimations ponctuelles sont affichées par des opérateurs sur des économies de ressources permises par une meilleure gestion des présences (température, éclairage optimisés) (voir cas d'usage n° 6). Des estimations s'attachent à l'optimisation des surfaces immobilières, notamment en lien avec le télétravail, car il s'agit du coût le plus important pour de nombreuses entreprises dans les services en zone urbaine[1]. Le lien avec l'IdO est alors plus difficile à établir.

Les bénéfices pour les individus sont quant à eux encore plus difficiles à mesurer à ce jour. Les contreparties bénéfiques restent très peu documentées et ambivalentes, comme mentionné dans les Tableaux 14 et 15 recensant des avis d'experts. Il en est de même pour celles plus négatives sur le stress, l'intensification, la responsabilité, voire la santé ou la sécurité, même si la numérisation du monde du travail en général et le déploiement de certains outils connectés en particulier commencent à faire l'objet d'évaluations prospectives en matière de santé et de conditions de travail[2].

Si globalement l'IdO peut générer une réduction de certains risques physiques en prévenant des situations de danger, certains dispositifs, par exemple en matière de réalité augmentée ou virtuelle, voire des équipements de protection individuelle, peuvent susciter de nouveaux risques[3]. De façon plus générale, les risques cyber évoqués par ailleurs dans ce rapport peuvent se décliner sur le champ du travail, dès lors que certains équipements de production industriels connectés (par exemple des cobots) peuvent être exposés à des

[1] Pour une synthèse des effets économiques du télétravail, notamment sur la productivité et les coûts immobiliers, voir Batut C. et Tabet Y. (2020), « Que savons-nous aujourd'hui des effets économiques du télétravail ? », *Trésor Éco*, n° 270, Direction générale du Trésor, novembre.

[2] Voir les travaux de l'agence européenne pour la sécurité et la santé au travail (EU-OSHA), par exemple : *Foresight on New and Emerging Occupational Safety and Health Risks Associated with Digitalisation by 2025*, rapport, Luxembourg, Publications Office of the European Union, novembre 2018. Voir aussi quelques éléments statistiques issus de l'enquête européenne ESENER de 2019 menée par l'EU-OSHA qui intègre depuis peu des éléments sur la digitalisation.

[3] Sur un cas concret comme les lunettes connectées, voir Lux A., Marchal P. et Perrin N. (2021), « Lunettes connectées : de nouveaux risques pour les salariés ? » *Hygiène et sécurité du travail*, n° 264, INRS, octobre. S'agissant des équipements de protection individuelle dits intelligents, voir Marsot J. et Marchal P. (2019), « Équipements de protection individuelle et objets connectés : principaux enjeux pour la santé-sécurité au travail », communication scientifique aux journées des innovations 2019 de la FNTP, INRS.

actes de malveillance externes et devenir une source de nouveaux risques pour les travailleurs qui en sont dépendants.

Des risques d'intensification et de surveillance

La contrepartie de la capacité de rationalisation et d'une adaptation toujours plus rapide, en temps réel, des processus de production est un risque d'intensification toujours plus forte du travail, d'une prescription accrue des tâches synonyme de perte d'autonomie et d'un contrôle plus serré des employés. Comme souligné par l'INRS, les objets connectés « en traçant et traitant en temps réel un nombre important de paramètres sur l'activité, l'environnement et les contraintes physiques, ils sont les outils non plus du plus, mais de l'optimal : optimisation de l'effort, de la performance, de la satisfaction client… »[1] Se pose alors la question de la norme implicite de performance à laquelle cette optimisation est reliée.

L'intensification du travail observée dans les entrepôts de la logistique ces dernières années est ainsi en partie imputable au fort développement de technologies numériques en lien avec l'IdO tel que la guidance vocale[2]. Elle est facteur de risques physiques et psychologiques pour les travailleurs. Lorsqu'il s'agit par ailleurs d'emplois à forte rotation (interim, CDD), notamment parce que cette numérisation permet le recrutement de travailleurs peu expérimentés mais assistés, la prévention et le suivi des risques peuvent être d'autant plus difficile à exercer. C'est encore plus vrai s'agissant des travailleurs hors de la relation salariale traditionnelle, comme les travailleurs indépendants des plateformes numériques, non couverts en général par le code du travail en matière de prévention santé et sécurité.

La collecte d'informations toujours plus importante sur l'activité peut notamment être dédiée à la surveillance des personnes sur leur lieu de travail (badges, détecteurs de présence ou d'activité, caméra d'ordinateur ou autre capteur biométrique) et à l'analyse fine de chacun de leurs gestes.

L'IdO porte ainsi, sur le lieu de travail – comme dans la vie privée - un risque d'intrusion sur les données qui revêtent à la fois un caractère personnel et professionnel. La mobilisation d'outils connectés associés par exemple au contrôle de l'accès aux locaux, au suivi des horaires de travail, ou encore à la supervision du comportement des salariés (par exemple via la caméra d'un ordinateur ou le suivi des connexions à distance), constitue un potentiel fort de contrôle renforcé et continu sur les individus[3]. Si la question sous-jacente de la protection des données personnelles en matière de contrôle des employés entre dans le champ du RGPD depuis 2016, ce règlement renvoie aux

[1] INRS (2018), *Les objets connectés*, coll. « Décryptage », avril, 4 pages.

[2] Voir Malenfer M., Govaere V., Bingen A. et Trionfetti M. C. (2020), « Impact des outils numériques sur les conditions de travail : l'exemple du commerce en ligne », *Hygiène et sécurité du travail*, n° 258, INRS, mars.

[3] Eurofound (2020), *Employee Monitoring and Surveillance…*, *op. cit.*

régulations étatiques (art. 88) la responsabilité d'établir les conditions spécifiques s'appliquant au processus de traitement des données dans le cadre des relations de travail, selon les types d'usages (du recrutement à la santé et sécurité des travailleurs).

La CNIL a ainsi produit une délibération (n° 2019-001 du 10 janvier 2019) visant à réglementer la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et applications informatiques sur les lieux de travail. Elle a également élaboré une liste de 14 opérations jugées à risque et pour lesquelles une analyse d'impact relative à la protection de données (AIPD) est obligatoire. Figurent sur cette liste les traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés, ou le traitement des profils de personnes physiques à des fins de gestion des ressources humaines. La CNIL publie ainsi des fiches visant à clarifier l'état du droit sur la collecte de données en matière d'accès aux locaux, de contrôle des horaires, ou encore la géolocalisation des véhicules des salariés[1].

Reste que la portée de cette réglementation générale est continûment re-questionnée face au développement accéléré des outils d'analyse de données (notamment prédictifs), que l'IdO contribue à alimenter[2]. De nouvelles questions peuvent ainsi se poser quant à la capacité d'un employeur à imposer – et réciproquement le droit d'un salarié d'accepter ou non – l'usage de certains dispositifs dans le cadre d'une relation de travail subordonnée. Ce questionnement vaut pour des objets directement inscrits dans des logiques de performance productive ou de responsabilité de la santé et de la sécurité (par exemple pour des vêtements de travail connectés) qui incombent à l'employeur. Il est également pertinent si l'on s'intéresse à des objets connectés pouvant relever d'usages à mi-chemin entre sphère personnelle et professionnelle. Il en est ainsi des objets dits de bien-être, d'automesure (« *quantifying self* ») tels que les bracelets connectés permettant par exemple le suivi de son activité physique, de la sédentarité ou de constantes physiques, qui produisent des données plus ou moins directement relatives à la santé, et que certains employeurs peuvent proposer à leurs employés dans une logique de prévention ou de qualité de vie au travail (voire dans le cadre d'une complémentaire santé d'entreprise). Même si de tels outils sont à ce jour proposés de façon facultative, l'assimilation possible des données ainsi collectées à des données de santé et les usages qui peuvent en être fait part l'employeur (risque de discrimination, de sélection sur la base de critère physiques de santé) soulèvent différentes questions juridiques.

[1] Voir le site de la CNIL la rubrique « Travail et données personnelles ».

[2] La CNIL a ainsi produit en 2019 un référentiel pour les organismes privés et publics mettant en œuvre des traitements de gestion courante des ressources humaines. Néanmoins il ne couvre pas, du fait de leur sensibilité, les traitements RH impliquant le recours à des outils innovants tels que la psychométrie, les traitements algorithmiques à des fins de profilage, les traitements dits de Big Data et les traitements ayant pour objet ou pour effet le contrôle individuel de l'activité des salariés.

L'équilibre fragile entre respect des données personnelles des salariés et droit des employeurs à mobiliser des données liées à l'activité pour le bon fonctionnement de l'entreprise appelle un encadrement clair de l'usage de données relatives aux personnes et à leur activité par le droit du travail ou plus généralement le droit du numérique.

Face à ces enjeux, le code du travail (art. L.1121-1) pose essentiellement à ce jour un principe de proportionnalité entre les moyens technologiques déployés, les objectifs productifs visés et les conséquences pour les travailleurs[1]. Ce principe a déjà été mobilisé par la jurisprudence pour arbitrer des affaires relatives à l'usage de pointeuses biométriques ou de dispositifs de géolocalisation pour contrôler le temps de travail des salariés. S'ajoute en matière de recrutement et d'évaluation professionnelle un principe de « pertinence » édicté aux articles L.1222-3 et L1221-8 qui prévoient que les « méthodes et techniques utilisées doivent être pertinentes au regard de la finalité poursuivie ».

Dans le champ des relations de travail, le principe de consentement de l'individu n'est cependant pas une base légale valable du fait des contraintes hiérarchiques[2], et l'employeur est essentiellement tenu par une obligation d'information et de transparence sur la collecte et l'usage des données[3]. Le code du travail prévoit également différentes obligations d'information et de consultation des représentants du personnel (le comité économique et social, depuis 2018), dans les entreprises de plus de 50 salariés, notamment avant l'introduction de nouvelles technologies, tout aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail (art. L.2312-8). En outre, le comité social et économique doit être informé, préalablement à leur utilisation ou modification, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi, sur les traitements automatisés de gestion du personnel et sur les moyens ou techniques permettant un contrôle de l'activité des salariés (art. L.2312-37 et 2312-38).

Enfin, la transformation des métiers et l'imbrication croissante entre le travailleur et des équipements sous contrôle numérique – parfois hors de son contrôle et même de celui de son employeur, lorsque ceux-ci sont tributaires d'un fournisseur ou d'un tiers extérieur qui

[1] Article 1121-1 du code du travail : « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché. »

[2] Si le consentement peut être nécessaire pour la collecte de données personnelles par l'employeur, il est de façon générale admis (voir notamment l'avis du « groupe de 29 » de 2014) que du fait de la relation de subordination existante entre employeur et son salarié, on ne peut considérer le consentement de ce dernier comme une base suffisante pour légitimer tout usage des données par l'employeur.

[3] Art. L. 1222-3 du code du travail : « Le salarié est expressément informé, préalablement à leur mise en œuvre, des méthodes et techniques d'évaluation professionnelles mises en œuvre à son égard. » Art. L. 1222.4 du code du travail : « Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance. »

collecte les données – peut engendrer de nouveaux questionnements sur l'identification des responsabilités entre ces différents acteurs en cas de dysfonctionnement. Dans le cas médical, par exemple, la responsabilité du soignant à l'égard de son patient a pu être questionnée dès lors qu'interviennent dans le suivi un nombre croissants d'outils connectés. Si de premières réponses ont pu être apportées au niveau européen dans le cadre des réflexions sur l'intelligence artificielle, notamment dans une perspective assurantielle, la question peut s'étendre à d'autres activités productives. Cette hybridation, aux contours mal défini en termes de relation de subordination et de responsabilité, peut être source de stress ou à l'inverse de désengagement pour les travailleurs, voire de négligence si ce dernier, suppléé par l'outil technique, vient à relâcher sa propre attention en matière de prévention des risques, avec des conséquences néfastes sur sa santé-sécurité au travail[1].

Les potentialités comme les risques associés au déploiement massif de l'IdO sur les lieux de travail restent donc à ce jour très largement hypothétiques et leur documentation très parcellaire. Il convient d'accompagner ce déploiement par une réflexion tant juridique qu'opérationnelle, qui peut être menée à différents niveaux. Celle-ci peut venir s'inscrire dans le cadre plus général des travaux qui depuis quelques années émergent s'agissant de l'impact de la digitalisation ou de l'Intelligence artificielle, sur le monde du travail, tout en visant à identifier les spécificités de l'IdO par rapport à l'IA par exemple. De nombreux acteurs institutionnels sont susceptibles d'apporter des éclairages sur le sujet, tels que l'Agence nationale pour l'amélioration des conditions de travail (Anact) ou l'Institut national de recherche et de sécurité pour la prévention des accidents du travail et des maladies professionnelles (INRS) par exemple dans le cadre du Plan santé au travail 2021-2025. L'IdO pourrait notamment constituer un pan à part entière des travaux qui seront menés dans le cadre du laboratoire LaborIA[2], centre de ressources et d'expérimentations créé récemment par le ministère du Travail, de l'Emploi et de l'Insertion et INRIA, devant permettre mieux appréhender l'intelligence artificielle et ses effets sur le travail, l'emploi, les compétences et le dialogue social, dans l'objectif de faire évoluer les pratiques des entreprises et l'action publique.

De tels travaux doivent incorporer une réflexion juridique à l'intersection du code du travail, du code civil et du code du numérique pour tenir compte des enjeux de l'IdO sur le lieu de travail dans le cadre plus général de la numérisation des processus productifs. Cette réflexion doit se décliner dans le dialogue social. Dans un registre qui n'est pas *stricto sensu* celui de l'IdO, les syndicats européens militent pour une adaptation du cadre légal européen

[1] INRS (2018), *Les objets connectés*, *op. cit.*

[2] Ce laboratoire vient plus largement s'inscrire dans le cadre international du partenariat mondial pour l'IA (PMIA ou GPAI en anglais) qui est l'aboutissement d'une idée développée au sein du G7, sous les présidences canadienne et française, lancé en 2020 par quinze États membres fondateurs et qui compte aujourd'hui dix-neuf membres. Chaque pays membre était invité, dans le cadre du sous-groupe de travail « Avenir du travail », à déployer des observatoires dans le cadre de la Stratégie nationale pour l'IA.

et des cadres nationaux en matière de conditions de travail autour de sept dimensions[1]. À l'échelon national, le dialogue social peut être mobilisé à différents niveaux :

- au niveau interprofessionnel dans le prolongement de l'accord-cadre des partenaires sociaux européens sur la numérisation conclu en juin 2020, les partenaires sociaux français prévoient dans leur agenda autonome de mener un travail en 2022 pour décliner cet accord ;
- au niveau des filières et branches par exemple au travers d'EDEC appuyé par le ministère du Travail[2] ;
- surtout sur les lieux de travail, dans le cadre de processus d'information/ consultation/négociation entre partenaires sociaux ou dans le cadre d'une démarche de responsabilité sociétale de l'entreprise (RSE) étendue au numérique[3], ou encore directement entre travailleurs, directions et encadrement au moment de l'introduction de ces technologies, afin d'en permettre un adoption alliant confiance et efficacité[4].

Les transformations introduites par l'IdO dans les situations de travail vont renouveler les questions relatives aux droits du salarié, tant en matière de santé, de sécurité que de conditions d'emploi ou d'évolution des compétences. Les implications sont déjà visibles, mais elles font encore peu l'objet de réflexions spécifiques et sont peu présentes dans le dialogue social. Des réflexions doivent être conduites, comme c'est déjà le cas pour l'intelligence artificielle dans le monde du travail. C'est le sens de notre recommandation n° 14 : Expertiser les enjeux spécifiques de l'IdO sur les lieux de travail.

[1] Voir Ponce Del Castillo A. (2020), « Le travail à l'ère de l'IA : pourquoi la réglementation est nécessaire pour protéger les travailleurs », *op. cit.* Ces sept dimensions couvrent la protection de la vie privée des travailleurs et la protection des données ; le traitement des questions de surveillance, de suivi et de contrôle ; la transparence du but poursuivi par les algorithmes de l'IA ; le « droit d'explication » pour les décisions prises par des algorithmes ; la préservation de la santé et de la sécurité des travailleurs ; la promotion de leur autonomie dans les interactions entre l'être humain et la machine ; et enfin le développement de l'esprit critique des travailleurs envers l'IA.

[2] La question digitale a donné lieu à des EDEC (engagements pour le développement de l'emploi et des compétences) à l'échelle de secteurs ou filières ces dernières années. Voir l'Edec « Perspectives IA » signé en novembre 2019 avec la Coalition numérique française en faveur des compétences du numérique, ou l'Edec « IA Hauts-de-France ». L'enjeu principal est de mener un diagnostic prospectif pour anticiper les transformations des métiers et les besoins en emplois et compétences résultant de ces mutations technologiques.

[3] Les travaux récents de la Plateforme RSE ont ainsi débouché sur des recommandations en matière de responsabilité numérique des entreprises, en termes d'enjeux de données, environnementaux et sociétaux. Voir Plateforme RSE (2021), *Responsabilité numérique des entreprises*, synthèse, France Stratégie, mai.

[4] L'étude d'Eurofound (2021a, *Digitisation in the Workplace*, *op. cit.*) analyse l'association des salariés et des partenaires sociaux dans différents cas d'usage étudiés de déploiement de l'IoT.

3. Enjeux collectifs

3.1. De quelles données parle-t-on ?

Les données produites dans le cadre de l'Internet des objets sont des données personnelles dès lors qu'elles peuvent permettre d'identifier, directement ou indirectement, un individu. Leur collecte et leur traitement sont soumis au respect du droit fondamental des individus à la protection de leurs données et de leur vie privée. Le Règlement général à la protection des données (RGPD), adopté en avril 2016, appliqué à partir du 25 mai 2018, a remplacé la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 et permis d'harmoniser la réglementation relative à la protection des données pour l'Union européenne. Il reprend pour une large partie les dispositions de la Loi Informatique et Libertés du 6 janvier 1978.

La loi pour une république numérique (LRN) de 2016 et l'adoption du RGPD en mai 2018 ont consacré dans le droit français des dispositions essentielles relatives à la protection des données personnelles. Cette loi a également fixé un cap pour les données non personnelles (DNP) en renforçant les obligations d'ouverture des données publiques, en créant le service public de la donnée, chargé de la mise en place des jeux de données de référence[1]. Elle a également consacré la notion de données d'intérêt général (DIG)[2] en imposant l'ouverture aux délégataires de mission de service public, aux gestionnaires des réseaux publics de distribution de gaz naturel ou d'électricité, aux opérateurs bénéficiant de subventions publiques, notamment aux opérateurs des transports. Les DIG ne sont ni des données publiques, ni des données personnelles (dès lors qu'elles sont anonymisées avant ouverture), mais des données privées produites et collectées par des entreprises dont le partage et l'ouverture sont d'intérêt général.

Dans ce paysage subsiste une **catégorie orpheline, les données à caractère non personnel, massivement produites par des acteurs privés**, hors du cadre des DIG, à partir des milliards de capteurs et objets connectés qui se déploient dans toutes les branches d'activité (voir cas d'usage n° 3, 10 et 11). Si les entreprises sont concernées au premier chef, les collectivités, dans le cadre de développement de services intelligents dans les territoires (voir cas d'usage n° 10), peuvent aussi être amenées à traiter ce type de données[3].

[1] Décret n° 2017-331 du 14 mars 2017 relatif au service public de mise à disposition des données de référence.

[2] Duchesne C., Morel M., Cytermann L., Aureau T. et Vachey L. (2015), *Rapport relatif aux données d'intérêt général*, Conseil général de l'économie et IgF, septembre.

[3] Consortium Civiteo/Datactivist/Innopublica/KPMG/Parme Avocats pour le compte de la DGE, la FFTélécoms, Sycabel, InfraNum et AFNUM (2021), *De la Smart City à la réalité des territoires connectés…*, *op. cit.*

Depuis mai 2019 et l'entrée en vigueur du règlement sur le libre flux des données à caractère non personnel[1], la Commission européenne organise un marché européen de la donnée. Elle a publié en juin 2020 les lignes directrices[2] pour une libre circulation des données à caractère non personnel en portant l'idée d'un « Schengen de la donnée ».

Toutefois, ces textes ne donnent pas de précision sur le statut de ces données quand les dispositions du RGPD ne sont pas applicables. Pour lever cette insécurité juridique faudrait-il fixer un droit de propriété sur ces données ? Cette option difficile à mettre en œuvre risque de limiter les potentialités de création de valeur permises par le partage de ces données.

L'autre option, qui semble largement privilégiée par les acteurs, est d'inciter à la circulation des données. Des solutions commencent à apparaître, venant d'acteurs du marché, comme les hubs de données organisés par un secteur ou une filière[3], ou encore l'émergence de nouveaux acteurs sur le marché de la donnée, comme les data brokers, ou « orchestrateurs »[4] qui proposent des solutions techniques pour sécuriser les flux et le partage de données.

Toutefois, dans ce domaine, les pouvoirs publics pourraient contribuer à faire naître des solutions pour tous les secteurs d'activités, en favorisant notamment l'émergence d'acteurs et de plateformes dédiées au partage et à la sécurisation des échanges de données (comme ils ont pu le faire pour des plateformes de type Health Data Hub ou GaiaX). Il s'agirait de diversifier l'offre des grandes plateformes d'interface et d'agrégation de données, majoritairement extra-européennes. Les dix premiers acteurs – dont Microsoft, Amazon Web Services ou Google Cloud – détiendraient déjà près de 65 % des parts de marché, contre 44 % en 2016[5].

---

[1] Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne. Les données à caractère non personnel relèvent de deux catégories : celles qui « au départ, ne concernaient pas une personne physique identifiée ou identifiable » et celles qui « étaient initialement des données à caractère personnel, mais qui ont ensuite été rendues anonymes ». Lorsqu'un ensemble de données est composé à la fois de données à caractère personnel et de données à caractère non personnel (données « mixtes »), le règlement de novembre 2018 et le RGPD s'appliquent pour chacun en ce qui les concernent.

[2] Commission européenne (2018), *Vers un espace européen commun des données*, EUR-Lex-52018DC0232-EN-EUR-Lex SWD (2018) 125, avril.

[3] Agdatahub ou Numalim. Pour la puissance publique, on peut citer Health Data Hub.

[4] Dawex, auditionné le 14 octobre 2021, organise l'échange de données entre organisations en garantissant leur sécurité et leur inviolabilité.

[5] Xerfi et Precepta (2022), *Les marchés de l'IoT professionnel à l'heure de la maturité. Quels usages et stratégies gagnantes à l'horizon 2025 ?*, étude, décembre.

Clarifier le statut des données recueillies dans le cadre de services de l'IdO, c'est le sens de notre recommandation n° 24.

N° 24 – Définir un statut des données sensibles.

3.2. Les risques cyber

En quoi un banal grille-pain peut-il représenter une menace pour un utilisateur lambda ? En réalité, ce n'est pas l'appareil lui-même qui est visé, mais le réseau auquel il est connecté et auquel il donne accès. La cybercriminalité évolue et s'accroît au rythme des évolutions d'Internet. **L'Internet des objets va considérablement étendre les failles potentielles et la surface d'attaque**. Les objets connectés sont des tremplins qui peuvent permettre de commettre des actions beaucoup plus dommageables.

Les dispositifs IdO présentent des risques qui peuvent être qualifiés de nouveaux en raison de leur **capacité à produire des effets « physiques » en dehors des systèmes d'information**, en raison aussi de leur massification, qui rend très difficile l'organisation des mesures de protection.

Certains objets connectés sont particulièrement vulnérables, car ils sont souvent très mal configurés et protégés. Les objets disposant d'une faible capacité mémoire ou d'une autonomie énergétique limitée sont plus vulnérables. De ce fait, ils ne peuvent bénéficier de systèmes de protection (chiffrement, antivirus ou pare-feu) sophistiqués. Les jouets par exemple sont des objets particulièrement sensibles[1] (voir cas d'usage n° 1). En outre, les fabricants d'objets où sont implantés les capteurs sont rarement des spécialistes de la sécurité informatique et ils hésitent à équiper leurs produits de dispositifs de sécurité dont le coût réduirait leurs marges bénéficiaires. Ces objets constituent donc des failles de vulnérabilité importantes.

Ces risques concernent en premier lieu les entreprises ou les organismes publics (hôpitaux) mais aussi clairement et de plus en plus les particuliers. Les attaques peuvent être relatives à des **vols de données** ou à **des actes de malveillance** (rançongiciels, logiciels espions, macro-virus, etc.). Voir le cas d'usage n° 1 (et l'attaque de la société Vtech ou de la poupée Cayla).

[1] Voir les publications de la CNIL. Par exemple CNIL (2019), « Jouets connectés : quels conseils pour les sécuriser ? », décembre.

Une autre forme de risque spécifique à l'Internet des objets porte sur les **risques d'attaques systémiques** pouvant potentiellement atteindre de multiples cibles simultanément. Elles sont rendues possibles par la massification et par l'interconnexion des objets. Par exemple, les attaques en déni de services pour saturer le site web d'une victime, ou la prise de contrôle d'un système de chauffage d'un bâtiment (voir cas d'usage n° 6) ou d'un quartier, peuvent avoir un impact fort destructeur sur le réseau électrique. La prise de contrôle du système de gestion des transports, par exemple par l'attaque ciblée des capteurs dans une métropole, pourrait aussi provoquer la paralysie d'une ville entière (voir cas d'usage n° 3). Ainsi en 2016 des hackers ont attaqué le réseau du système de transport public MUNI de San Francisco et ont provoqué l'arrêt des distributeurs de tickets et d'autres infrastructures informatiques via un logiciel malveillant[1]

Si les pouvoirs publics ont pris les premières mesures[2], l'ANSSI se concentre avant tout sur la sécurisation des administrations et des opérateurs d'importance vitale, qui possèdent actuellement peu d'objets connectés. Ces risques systémiques sont encore mal évalués[3]. Il est nécessaire de se préparer à ce type d'attaques qui pour la plupart recourent à des techniques déjà développées et connues sur d'autres types de structures ou de contextes.

Il faut également préciser le partage des rôles et compétences des organismes responsables de l'organisation des mesures de protection. C'est le sens de nos recommandations n ° 4, 26, 27 et 29.

N° 4 – Mieux évaluer les risques systémiques de cyberattaques spécifiques à l'IdO.

N° 26 – Procéder aux analyses juridiques permettant de définir l'échelle des responsabilités sur la chaîne des usages.

N° 27 – Analyser l'opportunité d'une loi cyber globale.

N° 29 – Cartographier les compétences respectives des régulateurs publics sur le champ de l'IdO.

[1] Sur les risque des cyberattaques dans les systèmes de transport voir Alcatel-Lucent (2019), « L'Internet des Objets dans les transports. Créez une base solide et tirez parti de l'Iot pour améliorer l'expérience, la sécurité et l'efficacité des passagers », décembre.

[2] ANSSI (2021), *Recommandations relatives à la sécurité des (systèmes d') objets connectés*, guide ANSSI, août.

[3] Audition de l'ANSSI le 26 octobre 2021.

BRÈVES DU MONDE

L'Inde est particulièrement ciblée par les attaques cyber, en constante augmentation ces dernières années avec la numérisation grandissante de l'économie. Le Data Security Council of India estime qu'entre 2016 et 2018, l'Inde était le deuxième pays au monde le plus affecté par des cyberattaques. Au printemps 2020, au plus fort des tensions avec la Chine, l'Inde a observé une augmentation de 86 % du nombre de cyberattaques. La moitié d'entre elles utilisaient l'IdO comme porte d'entrée. Quelques mois plus tard, en octobre, la ville de Mumbai, capitale économique du pays, a subi une coupure de courant géante, causée d'après l'entreprise américaine spécialisée dans la cybersécurité Recorded Future par une cyberattaque menée par une entité liée au gouvernement chinois.

En Finlande, un rapport de 2018 sur l'état de cybersécurité montrait qu'il y avait de plus en plus d'appareils non sécurisés sur le réseau et que plus de la moitié étaient des appareils IdO, notamment des appareils d'automatisation des bâtiments[1] et de l'électronique grand public. Depuis novembre 2019, il existe un label de cybersécurité (*Finnish Cybersecurity Label*) principalement destiné aux appareils intelligents grand public : téléviseurs, bracelets et routeurs domestiques. Il est accordé aux appareils ou services intelligents connectés et aux applications répondant aux exigences de sécurité de l'information définies par le centre de cybersécurité national.

Le Chili souhaite se doter d'un système législatif et opérationnel de cybersécurité susceptible de s'inspirer notamment d'un diagnostic réalisé par la société Toca (Israël). Dans ce cadre, le Chili a signé un accord de coopération en la matière avec Israël, puis avec d'autres pays, dont l'Espagne et le Royaume-Uni.

En Chine, fin 2016, le producteur d'appareils IdO Hangzhou Xiongmai Technology a été forcé de rappeler plus de 10 000 webcams après qu'elles ont été victimes d'une attaque par le malware Mirai botnet. Les appareils Xiongmai auraient été mis sur le marché sans même être équipés de dispositif de sécurité de base, ce qui en a fait des cibles privilégiées. En 2017, il a été démontré que plus de 175 000 caméras connectées (reliées à un réseau IdO) produites par Shenzhen Neo Electronics et installées dans plusieurs pays étaient accessibles à distance en raison, là aussi, d'une insuffisante sécurité dans les protocoles d'accès des appareils. En outre, certains industriels auraient laissé volontairement des portes dérobées (*backdoors*) permettant l'accès à distance de produits IdO, à plusieurs fins (débogage ou surveillance), augmentant de fait la vulnérabilité de certains appareils. C'est notamment le cas de l'entreprise Shenzhen DblTek Technology (à fins de débogage). Enfin, un corollaire du système de surveillance chinois est de rendre possible le hacking de données et de communications dont la sécurisation est volontairement affaiblie. En août dernier, les autorités avaient interdit la dernière mise à jour du protocole TLS (utilisé pour crypter le trafic web).

[1] Ces systèmes contrôlent la ventilation, le chauffage, l'éclairage ou l'accès automatique d'un bâtiment.

Toujours **en Chine**, les recherches sur la sécurité des réseaux IdO se multiplient. Selon les données de CNKI, environ 1 229 articles sur ce thème ont été publiés[1] en 2017, contre 9 en 2009 – des chiffres à mettre en relation avec le nombre croissant d'appareils connectés. La recherche s'est principalement concentrée sur les vers IdO polymorphiques, qui ont la capacité d'infecter plusieurs appareils connectés à un réseau, une fois le premier appareil infecté. Il s'agit de modeler la manière dont un tel vers pourrait se propager[2]. De même, sont régulièrement publiées des évaluations des vulnérabilités de différents logiciels sur une banque de données nationale, afin de faciliter l'identification pour les entreprises des points de vulnérabilités dans leur architecture de sécurité. Plusieurs instituts de recherche se penchent sur la question de la sécurité des réseaux : le Beijing Key Laboratory of IdO Information Security Technology se concentre par exemple sur les systèmes de contrôle industriel.

L'élaboration de normes doit également permettre de répondre aux enjeux de sécurité et d'assurer l'interopérabilité de ce qui constitue les réseaux IdO (objets, passerelles applicatives, plateformes). En octobre 2021, le plan d'orientation pour établir un système de normes de sécurité de base pour l'IdO préconise d'élaborer au moins 10 normes industrielles IdO d'ici 2022 et 30 d'ici 2025, qui devront améliorer le niveau de sécurité dans différentes applications industrielles. Ce plan préconise l'élaboration de normes pour assurer la sécurité des terminaux IdO (objets), des passerelles applicatives, des plateformes, mais aussi pour améliorer les conditions générales de sécurité. Les recommandations sont précises (nécessité de se fonder sur des scénarios de risques, encouragement à établir dès à présent des modèles d'architecture de sécurité, à assurer la sécurité des données mais aussi de l'appareil lui-même).

En Estonie, la « Stratégie de cybersécurité 2019-2022 »[3], document cadre pour la planification de la cybersécurité nationale, fait figurer l'IdO comme l'un des facteurs technologiques de risque pour la sécurité.

Au Japon, le gouvernement a adopté le 28 septembre 2021 une nouvelle stratégie nationale en matière de cybersécurité. Une agence spécialisée (NISC) est rattachée au cabinet du Premier ministre depuis 2015 et une cellule cybersécurité est rattachée au ministère de l'Intérieur et des Communications[4]. Cette dernière cellule a notamment préparé en 2020 des recommandations sur les risques cyber liés aux technologies IdO.

Source : Direction générale du Trésor ; pour un tableau par pays et des sources détaillées, voir annexe 7

[1] SOSi (2018), *China's Internet of Things*, rapport pour la U.S.-China Economic and Security Review Commission, octobre.

[2] La modélisation de la propagation d'un ver IdO polymorphique a des applications défensives, mais aussi offensives.

[3] Ministère estonien des Affaires économiques et des Communications (2019), *Cybersecurity Strategy – Republic of Estonia, 2019-2022*, décembre.

[4] Voir le site de l'Agence, basée sur le Basic Act on Cybersecurity, et les recommandations de la cellule rattachée au MIC, en japonais.

3.3. Interopérabilité : bien au-delà des enjeux techniques

L'IdO repose sur les technologies et les protocoles de l'Internet, mais le développement massif d'objets connectés peut-il se poursuivre sans transformer profondément le socle technique de l'Internet ?

Rendre les réseaux d'objets communicants entre eux et interopérables quels que soient les technologies réseau ou les protocoles de communication partagés, ou encore disposer d'un système d'adressage commun permettant de reconnaître les milliards d'objets sur le réseau sont aujourd'hui des enjeux techniques non résolus et dont le règlement pourrait avoir des répercussions structurantes sur le fonctionnement d'Internet et de son économie.

En effet, les applications de l'IdO sont actuellement très dépendantes des technologies des verticales et des écosystèmes dans lesquelles elles opèrent, qu'il s'agisse des technologies réseaux ou logicielles.

> « Pour un projet IoT, les industriels doivent d'abord choisir la technologie d'accès, puis ajuster le choix des capteurs, des plateformes et enfin assurer l'intégration à l'architecture existante. Choisir une connectivité, c'est donc prendre un risque sur l'obsolescence, la pérennité de l'investissement, et l'utilisation simple et sécurisée des données. Face à cette complexité, le marché de l'IoT tend à se "verticaliser" autour de solutions préconfigurées (…) soutenant indirectement des écosystèmes cloisonnés par un choix limité de protocoles, de formats de données et souvent des interfaces (API) propriétaires[1]. »

Derrière le choix des protocoles et des standards, c'est la pérennité d'un Internet ouvert qui est en jeu.

L**'identification des objets sur le réseau Internet est également** une question non résolue puisqu'il n'existe pas aujourd'hui de standard unique sur le réseau. Les objets peuvent être identifiés par différents systèmes de nommage, selon les secteurs d'application dans lesquels ils sont déployés : un code barre, une adresse IP (IPV6 ou IPV4), un étiquette RFID. L'enjeu qui reste aujourd'hui à traiter est de parvenir à faire cohabiter ces différents systèmes de nommage.

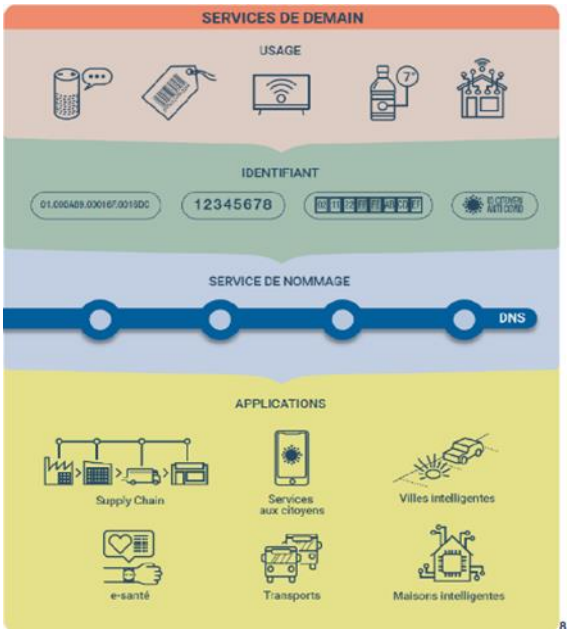
Ainsi le registre français des noms de domaines français, l'AFNIC, travaille sur l'évolution du DNS (Domain Name Service) pour le définir comme plateforme universelle de résolution des différents standards d'identification[2]. Ces enjeux ne sont pas exclusivement techniques, puisqu'ils sont déterminants pour l'avenir du fonctionnement d'Internet et ils

[1] Laurent M., Pelov A. et Toutain L. (2021), « Les protocoles de l'Internet au service de l'interopérabilité de l'Internet des objets », *Enjeux numériques*, n° 16, Annales des Mines, décembre.

[2] Audition du 9 décembre 2021.

auront des répercussions économiques importantes : faute de trouver des standards interopérables et des systèmes d'identification partagées, on risque de voir se multiplier des réseaux fermés opérés par des standards propriétaires.

Graphique 24 – Fonctionnement d'identification de l'IdO sur Internet



Source : AFNIC

Les technologies de l'IdO sont à des niveaux de maturité inégaux, il reste de nombreux domaines où la recherche doit encore progresser. Parallèlement, des enjeux importants de définition des standards structurant pour l'avenir de l'Internet sont en cours de discussion dans les instances internationales.

Maîtriser ces changements rapides nécessite de poursuivre la recherche et d'être plus présents dans les instances de gouvernance internationale de l'Internet, c'est le sens de nos recommandations n° 5, 6, 7 et 8.

N° 5 – Encourager et promouvoir les travaux de recherche relatif à l'IdO.

N° 6 – Préparer et soutenir la représentation française dans les instances internationales de normalisation et de gouvernance de l'Internet.

N° 7 – Permettre la mise ne place d'expérimentations à grande échelle.

N° 8 – Encourager le partage de données, y compris au niveau international.

BRÈVES DU MONDE

En Lettonie, selon le Plan national de numérotation, une numérotation spéciale à 10 et 12 chiffres a été réservée pour les communications M2M et IdO. Afin de favoriser l'utilisation du protocole IPv6 qui permet d'augmenter le nombre d'adresses IP individuelles et d'assurer la sécurité des services, le ministère des Transports a initié le passage du protocole IPv4 au protocole IPv6 dans tous les établissements publics et municipaux.

En Chine, le secteur de l'IdO figure à l'avant-poste des efforts en matière de standardisation à l'échelle internationale, réaffirmés dans le plan China Standards 2035. Les standards sont perçus comme un enjeu stratégique et les standards industriels notamment comme un moyen d'augmenter la compétitivité des biens et services chinois à l'international, en particulier dans les secteurs des télécommunications, de la *blockchain* et de l'IdO. Ainsi, le plan d'orientation du MIIT (janvier 2021) appelle à une coopération avec d'autres pays en matière de standards de sécurité de base pour l'IdO, tandis que le plan China Standards 2035 appelle à la standardisation de l'IdO. Le rôle des entreprises dans l'influence des normes est appelé à se renforcer. China Standards 2035 et Made in China 2025 encouragent en ce sens les entreprises chinoises, notamment les « champions nationaux ». Plus récemment, le plan pour le développement de la standardisation (octobre 2021) appelle, conformément aux axes définis par la nouvelle version (2018) de la loi sur la standardisation datant de 1988, à renforcer le rôle du marché dans la standardisation. Le 14e plan quinquennal pour les TIC (2021-2025) du MIIT abonde dans ce sens : il incite les entreprises chinoises à s'internationaliser et à participer à la définition de normes internationales dans plusieurs domaines, dont l'IdO.

Une double démarche est à l'œuvre pour influer sur les normes au niveau international : participer à leur élaboration via une activité accrue au sein d'enceintes internationales d'une part, et assurer une large adoption de produits ICT chinois par d'autres pays d'autre part. Le plan d'action pour la formulation de normes, l'un des dix segments du plan d'action pour le développement de l'IdO, appelle à s'imposer au sein d'organes tels que l'ISO/IEC et l'IUT. De même, un nombre croissant de projets dans le secteur des TIC en pays tiers, dans le cadre des routes de la soie numériques par exemple, permettent aux entreprises chinoises d'installer dans ces pays leurs propres infrastructures et de diffuser leurs propres normes, ouvrant la voie à une adoption *de facto* de ces normes et garantissant une nécessité future d'interopérabilité. Fin 2020, sur 18 normes IdO adoptées par l'ISO/IEC, 10 étaient proposées par des acteurs chinois.

Source : Direction générale du Trésor ; pour un tableau par pays et des sources détaillées, voir annexe 7

3.4. Enjeux de souveraineté et stratégie économique

La maîtrise des standards, des technologies et des brevets est le nerf de la guerre et la bataille technico-industrielle autour de l'Internet des objets va aller en s'intensifiant. La compétitivité économique de tous les secteurs de production est en jeu, bien au-delà

des entreprises du numérique et des télécoms. Tous seront potentiellement touchés, soit en raison de l'automatisation des lignes de production (cas d'usage n° 9 ou n° 10), soit parce que les produits fabriqués seront connectables (cas d'usage n° 1 ou n° 2).

À défaut de présenter ici une analyse approfondie de ces implications économiques, il convient de souligner certains points qui sont apparus clairement au cours de nos travaux.

S'il existe des acteurs européens et français, l'impact de l'Internet des objets et la transformation des chaînes de valeur qui en résulteront est difficile aujourd'hui à anticiper pour les entreprises européennes. Une enquête de Microsoft[1] souligne ainsi combien les applications IdO dans les entreprises rencontrent des difficultés techniques et sont encore souvent en phase de test. Quelles sont les capacités des entreprises françaises et européennes à s'approprier la valeur ajoutée créée par des dispositifs IdO ? Sont-elles en mesure de tirer profit de la valorisation des données ? Et disposent-elles des compétences pour maîtriser les technologies ?

L'exemple des assistants vocaux (cas d'usage n° 2) est là encore très révélateur. Le marché visé par les entreprises qui commercialisent aujourd'hui ces équipements pourrait en effet aller bien au-delà de celui de l'assistant vocal individuel. Avec les « skills », ces briques logicielles qui permettent d'ajouter de nouvelles fonctionnalités en associant par exemple des équipements domotiques ou des véhicules intelligents, l'assistant devient une télécommande universelle et disqualifie les équipements qui ne seraient pas compatibles avec sa couche logicielle. Les industriels situés en aval – par exemple, les industriels de la domotique – pourraient donc être dépendants de leur compatibilité à des dispositifs d'IdO maîtrisés par des sociétés du numérique et perdre le contrôle de leur propre marché.

L'autre enjeu relatif à la compétitivité et à l'innovation est celui des données. L'IdO est porteur de gains de productivité et d'innovation, si d'une part les données potentiellement générées peuvent être collectées et exploitées par le producteur, et si d'autre part des agrégateurs de services peuvent exploiter ces données pour produire de la connaissance ou des services à valeur ajoutée. Or cela suppose qu'il existe des régimes d'accès et d'usage des données clairement définis et permettant une juste rémunération des différentes parties prenantes impliquées dans la valorisation de ces données (cas d'usages n° 3).

À défaut, il n'y aura aucune incitation à partager ou même à produire ces données. En effet, leur valorisation nécessite des investissements importants : infrastructures de stockage, systèmes de sécurisation, qualification des données et développement de compétences *ad hoc*. Sans circulation des données, les investisseurs n'auront aucune garantie d'un retour sur investissement et d'une juste rétribution de leurs efforts. Dès lors

[1] Microsoft (2021), *IoT Signals*, *op. cit.*

le risque est double : ou bien les données seront captées par des acteurs oligopolistiques, sans partage de valeur, ou bien elles ne seront pas exploitées par défaut d'investissement, hypothéquant toute création de valeur ou d'innovation.

Selon les auteurs de l'étude récente Xerfi ces dangers sont bien réels[1] :

> « Si les concepteurs et fabricants d'objets connectés ont la mainmise sur les données issues de leurs produits, il s'agit de données isolées, qui ne présenteront qu'une faible valeur si elles ne sont pas mises en relation avec d'autres informations en provenance d'objets connectés tiers. La menace est bien réelle de voir les géants de l'IT comme Amazon, Google et IBM s'emparer de la maîtrise des données issues des services connectés en faisant de leur technologie (le système d'exploitation, le logiciel, l'assistant vocal, etc.) le(s) standard(s) de marché. »

La circulation des données doit se dérouler dans un cadre de confiance que des outils législatifs et réglementaires peuvent contribuer à définir mais qui ne suffiront pas. Le partage des données suppose aussi des coopérations entre acteurs au sein d'une même filière et entre filières (par exemple les opérateurs de télécoms pour les transporteurs ou les logisticiens). Il suppose aussi un contexte propice au développement de l'IdO, avec l'émergence de nouveaux acteurs (par exemple, les orchestrateurs de données) ou de plateformes dédiées.

La création de valeur de l'Internet des objets se situe dans la possibilité d'exploiter et de valoriser les données recueillies et de les partager pour développer de nouveaux services dans un cadre respectueux de la vie privée, de la propriété industrielle ou intellectuelle. L'absence d'un cadre adapté pourrait favoriser les grandes plateformes et leurs standards.

C'est le sens des recommandations n ° 1, 3, 23, 24, 25, 26, 29 et 30.

N° 1 – Disposer d'un outil d'observation dédié à l'IdO.

N° 3 – Faciliter la connaissance des réglementations.

N° 23 – Créer les conditions favorables au partage maîtrisé et à la valorisation des données.

N° 24 – Définir un statut des données sensibles.

N° 25 – Veiller à préserver des pratiques concurrentielles des différents maillons du marché.

[1] Xerfi et Precepta (2021), *Les marchés de l'IoT professionnel à l'heure de la maturité...*, *op. cit.*

N° 26 – Procéder aux analyses juridiques permettant de définir l'échelle des responsabilités sur la chaîne des usages.

N° 29 – Cartographier les compétences respectives des régulateurs publics dans le champ de l'IdO.

N° 30 – Procéder pour l'IdO à une analyse juridique fondée sur une approche d'analyse des risques.

3.5. Les collectivités et l'IdO

Au-delà des nombreux débats qui accompagnent le développement des villes et des territoires intelligents, on observe d'ores et déjà, dans les métropoles et les conseils départementaux, des collectivités qui choisissent de s'équiper de services connectés permettant théoriquement d'améliorer les services aux citoyens, l'efficacité de la gestion des équipements (réseaux d'énergie, d'eau, etc.) ou d'optimiser leur système de décision par l'analyse des données collectées par ces dispositifs. Les exemples sont connus (Dijon, Angers) en France et à l'étranger (cas d'usage n° 3 et n° 4). Le scénario tendanciel qui se dessine est la multiplication des expériences, impliquant de plus en plus d'acteurs et de solutions qui aujourd'hui se développent de façon indépendante. L'hétérogénéité des fournisseurs, des solutions et des standards retenus représentent un défi réel pour les collectivités qui s'engagent aujourd'hui.

Les enjeux sont de plusieurs ordres. En premier lieu, les collectivités se trouvent confrontées à des offreurs de solutions verticaux (énergie, sécurité, transports) proposant des systèmes clés en mains propriétaires, souvent fermés, sans garanties d'interopérabilité. À chaque domaine son spécialiste et son dispositif technique dédié, ce qui conduit à une prolifération d'interlocuteurs[1] et de solutions qui multiplie les marchés, les contrats et complexifient les enjeux de maintenance. L'élargissement des champs couverts (gestion des déchets, transports, etc.) par des sociétés parfois concurrentes augmentent en outre la vulnérabilité des équipements aux risques cyber. Les observations de la Fing qui a travaillé avec quinze conseils départementaux et avec l'Association des départements de France[2] ont mis en évidence que les collectivités les plus impliquées ont engagé des expérimentations sans pérennité qui pour certaines ont dû être abandonnées.

L'absence de maîtrise collective de ces déploiements présente donc un risque pour les collectivités. Sélectionner des solutions robustes, pérennes, sécures et interopérables

[1] Exemple de la ville de Nice, audition de la Fing, 30 septembre 2021.

[2] ADF et Fing (2021), *Livre blanc de l'Internet des objets*, non publié mais communiqué à l'occasion de l'audition de la Fing le 30 septembre 2021.

qui garantissent la durabilité des investissements consentis nécessite que les collectivités puissent s'appuyer sur des référentiels techniques partagés, à même de les accompagner dans leurs choix. À partir de 2025, les communes et leurs intercommunalités de plus de 50 000 habitants devront élaborer une stratégie numérique responsable (disposition de la loi du 15 novembre 2021). Les enjeux spécifiques soulevés par le déploiement de dispositifs d'IdO devront être développés dans ce cadre, notamment en permettant d'afficher plus clairement les coûts/bénéfices attendus, en tenant compte de l'ensemble de la mise en place du dispositif (CAPEX, OPEX mais aussi du cycle de vie de tous les composants).

Mettre à disposition des collectivités au bénéfice des habitants, les moyens de maîtriser leurs choix en matière IdO, c'est le sens des recommandations : n ° 7, 20, 24, 27 et 28.

N° 7 – Permettre la mise en place d'expérimentations à grande échelle.

N° 20 – Mettre à disposition des collectivités des outils de mesure d'impacts et d'aide à la décision.

N° 24 – Définir un statut des données sensibles.

N° 27 – Analyser l'opportunité d'une loi cyber globale.

N° 28 – Accompagner les acheteurs publics dans la mise en œuvre et l'achat de solutions IdO.

CHAPITRE 6

LES ENJEUX ENVIRONNEMENTAUX OU LA DIFFICILE MESURE DES COÛTS ET BÉNÉFICES

1. Bénéfices et coûts évités : de grandes incertitudes sur les chiffres

Le numérique et l'Internet des objets en particulier avec la multitude de données que ces dispositifs vont permettre de collecter, pourraient se révéler des leviers majeurs dans la lutte contre le réchauffement climatique et pour la transition écologique. Des secteurs comme l'industrie, les transports, le commerce ou l'énergie pourraient réduire leur impact environnemental par une meilleure gestion des ressources, par des mesures précises des consommations ou encore grâce aux opérations de maintenance préventive et prédictive. Les possibilités sont multiples.

Les documents fournis par les industriels sont souvent enthousiastes. Selon le rapport du GeSI[1] qui s'appuie sur les contributions d'universitaires, d'ONG et sur l'observation de plus de 500 cas d'usage, les technologies IdO, si elles sont déployées dans un souci d'impact sociétal positif, permettraient d'accélérer de 22 % les progrès vers les objectifs de développement durable ODD. Elles pourraient réduire sept fois les émissions de gaz à effet de serre produites par le secteur numérique lui-même[2].

[1] GeSI (2019), *Digital with a Purpose: Delivering a SMARTer2030*, septembre. Le Global Enabling Sustainability Initiative est un groupement international d'acteurs du secteur des technologies de l'information et de la communication qui souhaite promouvoir des pratiques numériques soutenables.

[2] Audition AFNUM.

Encadré 3 – Technologies numériques et environnement selon le World Economic Forum

« Les technologies numériques contribueraient déjà à réduire les émissions mondiales de carbone de 15 % – soit un tiers de la réduction de 50 % requise d'ici 2030 – grâce à des solutions dans les domaines de l'énergie, de la fabrication, de l'agriculture et de l'utilisation des sols, des bâtiments, des services, des transports et de la gestion du trafic. C'est plus que l'empreinte carbone actuelle de l'UE et des États-Unis réunies. Mais c'est avec la quatrième révolution industrielle – en particulier avec la 5G, l'Internet des objets (IdO) et l'intelligence artificielle (IA) – que le secteur numérique peut réellement accélérer le rythme du changement. »

World Economic Forum (2020), Exponential Climate Action Roadmap[1], traduction des auteurs

En ce qui concerne les gains de l'IdO, on trouve dans la littérature académique de nombreuses études de cas qui décrivent les apports spécifiques dus à l'installation de systèmes pilotés par de tels dispositifs : pour la gestion de l'éclairage[2], pour les systèmes d'irrigation[3], pour la collecte de données environnementales[4]. Mais ces travaux restent fondés sur des approches sectorielles, souvent étayées par des données fournies par les industriels et sur lesquelles il est peu aisé d'établir des projections plus globales.

En outre, les approches sectorielles présentent des limites importantes, comme l'illustrent deux études récentes[5]. En comparant les bénéfices du déploiement de l'IdO dans cinq secteurs, les deux études montrent que si les bénéfices sont avérés, leur ampleur présente de telles disparités qu'il convient de considérer ces résultats avec la plus grande précaution.

[1] Exponential Roadmap Initiative : https://exponentialroadmap.org/

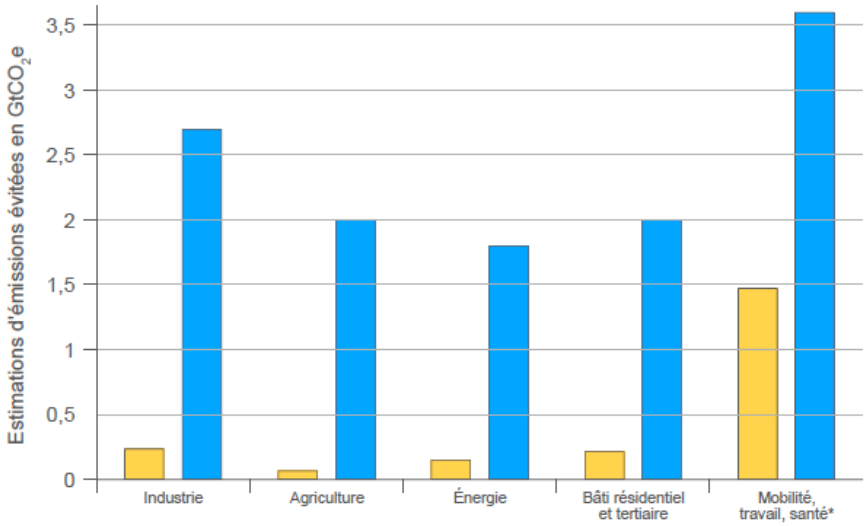
[2] Ingemarsdotter E., Jamsin E. et Balkenende R. (2020), « Opportunities and challenges in IoT-enabled circular business model implementation – A case study », *Resources, Conservation and Recycling*, vol. 162, novembre.

[3] Singla B., Mishra S., Singh A. et Yadav S. (2019), « A study on smart irrigation system using IoT », *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 5(2), avril, p. 1416-1418.

[4] Mois G., Folea S. et Sanislav T. (2017), « Analysis of Three IoT-Based Wireless Sensors for Environmental Monitoring », *IEEE Transactions on Instrumentation and Measurement*, vol. 66(8), août, p. 2056-2064.

[5] GeSi et Accenture Strategy (2015), *SMARTer 2030: ICT Solutions for 21st Century Challenges*, rapport ; GSMA et Carbon Trust (2019), *The Enablement Effect. The Impact of Mobile Communications Technologies on Carbon Emission Reductions*, décembre.

Graphique 25 – Estimation des émissions évitées par l'Internet des objets au niveau mondial, estimations en $GtCO_2eq$ évitées



Lecture : en bleu figurent les estimations de *SMARTer 2030* (GeSi et Accenture Strategy, 2015, *op. cit.*) ; en jaune les estimations de *Enablement Effect* (GSMA, 2019, *op. cit.*).

* Cette section inclut la logistique, la gestion et l'optimisation du trafic, les transports privés connectés, le télétravail, le commerce et la banque en ligne, la télémédecine, et l'enseignement à distance pour l'étude SMARter2030 et les secteurs de la ville intelligente, le travail et la santé pour le rapport Enablement.

Source : audition de Gauthier Roussilhe, CRD (ENS, Saclay, RMIT), octobre 2021

Dans le cadre de cette mission, nous avons tenté d'estimer l'ordre de grandeur des bénéfices de l'IdO. Le modèle proposé par les cabinets BCG et EY-Parthenon établit que l'Internet des objets serait globalement positif et pourrait réduire d'ici 2040 la consommation d'énergie de 12 % à 17 % dans les secteurs du transport, du bâtiment et de l'industrie. Cette projection se fonde sur l'hypothèse d'une consommation énergétique finale mondiale en 2040 de 155 000 TWh pour les secteurs des transports, du bâtiment et de l'industrie (hypothèse hors déploiement de l'IdO).

Les bénéfices attendus varient d'un secteur à l'autre. Les transports sont le secteur où les gains pourraient être les plus importants, de l'ordre de 20 %. Ces hypothèses sont fondées sur des retours d'expérience clients des cabinets[1], et sur des estimations de l'Agence internationale pour l'énergie[2]. La consommation ainsi évitée serait de l'ordre de 18 000 à 26 000 TwH.

[1] BCG (2021), « How tech offers a faster path to sustainability », 14 octobre.

[2] OCDE et AIE (2014), *More Data, Less Energy. Making Network Standby More Efficient in Billions of Connected Devices*, Paris, Publications de l'AIE, juin ; AIE (2017), *Digitalisation and Energy*, rapport technique, Agence internationale de l'énergie, novembre.

Tableau 16 – Estimation de la consommation énergétique économisée par des solutions IdO et par secteur

Industrie	Bâtiment	Transports
		
L'IdO devrait réduire la consommation énergétique des usines de 5 % à 15 % sur la base des premiers pilotes (hypothèse de travail fondée sur l'expérience de BCG et EY dans le domaine de l'industrie 4.0, aucune étude publique ou semi publique n'étant disponible)	Selon l'Agence internationale de l'énergie (AIE), la digitalisation réduirait la consommation énergétique des bâtiments résidentiels et commerciaux de l'ordre de 10 %	Selon l'Agence internationale de l'énergie (AIE), l'estimation d'efficacité énergétique pour le transport terrestre de marchandise est de 20 % à 25 % (sachant que le transport terrestre représente 80 % des émissions de CO_2 liées au transport)
Énergie consommée (% total)		
59 400 TWh (38 %)	**51 600 TWh (33 %)**	**43 900 TWh (28 %)**
Énergie économisée		
3 000-9 000 TWh	**6 000 TWh**	**9 000-11 000 TWh**
Total		
Énergie consommée (% total) 155 000 TWh (100 %)		
Énergie économisée 18 000-26 000 TWh		

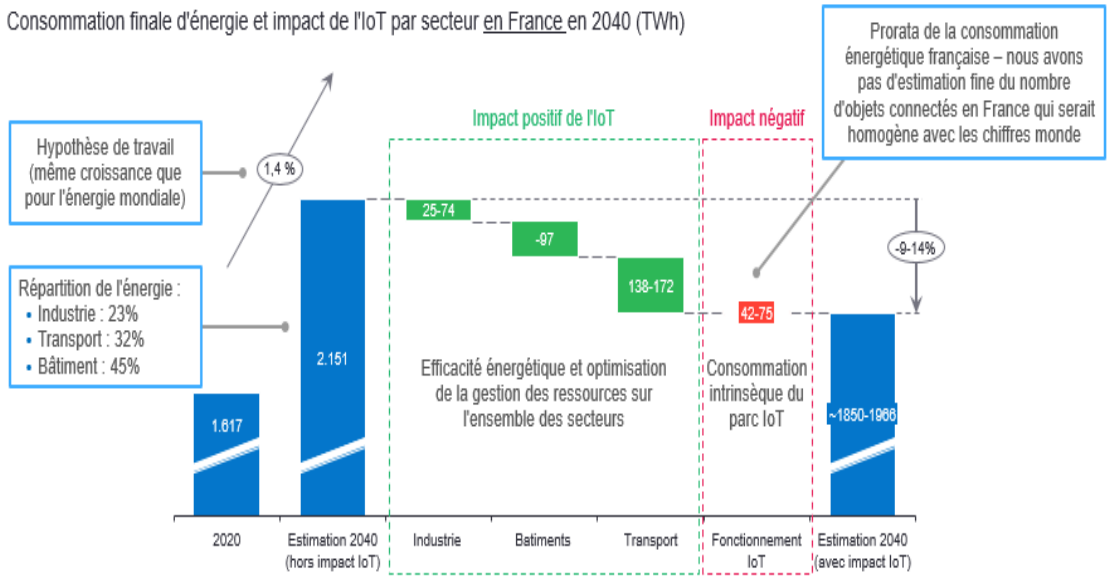
Source : analyse BCG et EY-Parthenon

Enfin, l'analyse conclut à un bénéfice net de l'IdO, puisque la consommation énergétique de ces dispositifs serait seulement de 3 000 et 54 000 TWh. Cette projection a été calculée sur la base d'une consommation moyenne de 30 kWh par objets connectés, en prenant l'hypothèse qu'il s'agit d'une consommation de bout en bout (annexe 6).

Si les mêmes hypothèses de travail étaient retenues pour la France, le déploiement de l'Internet des objets pourrait réduire la consommation finale d'énergie en France de 9 % à 14 % (voir Graphique 26). Cette hypothèse tient compte notamment d'une répartition des secteurs différentes de celle retenue dans l'hypothèse mondiale, puisque la part de consommation énergétique retenue pour chaque secteur est respectivement de 23 % pour l'industrie, 32 % pour le transport et 45 % pour le bâtiment.

Si on peut considérer que le déploiement de l'IdO apportera **des bénéfices en matière de gestion des ressources et de consommation énergétique, les hypothèses de calcul restent fragiles et ne prennent pas en compte la possibilité d'effets rebonds**.

Graphique 26 – Hypothèse des gains sur la consommation énergétique de la France après déploiement de l'Internet des objets



Source : analyse BCG et EY-Parthenon, d'après le « Bilan énergétique de la France 2019 », données du ministère de la Transition écologique

2. Les coûts environnementaux : les travaux académiques convergent en dépit des difficultés méthodologiques

2.1. Les projections au niveau mondial

La prise de conscience des impacts du numérique sur l'environnement est relativement récente mais il existe à ce jour un corpus d'études significatif. Un consensus semble se dégager pour estimer le niveau de l'empreinte environnementale actuel du numérique qui est estimé entre 2 % et 4 % de la part des émissions mondiales de gaz à effet de serre (1 000 à 2 000 M tCO_2eq)[1]. Mais de nombreux dissensus persistent sur les projections à venir en raison de difficultés relatives aux modèles utilisés et à l'insuffisance voire à l'absence de données. **Les éléments d'analyse qui concernent plus spécifiquement l'Internet des objets sont en revanche moins nombreux et présentent beaucoup d'incertitudes**[2]. Qu'il s'agisse de mesurer les effets directs ou indirects sur l'environnement, les données disponibles sont rares et parcellaires, en raison :

[1] Freitag C., Berners-Lee M., Widdicks K. *et al.* (2021), *The climate impact of ICT: A review of estimates, trends and regulations*, rapport, université de Lancaster, février.

[2] Dedryver L., Hamelin J., Couric V. et Farella-Champeix J. (2020), « Maîtriser la consommation du numérique, le progrès technologique n'y suffira pas », document de travail, n° 2020-15, France Stratégie, octobre.

– de la masse des capteurs concernés, qu'il est très difficile d'estimer. De 5 milliards d'objets connectés à plusieurs centaines de milliards, selon la définition retenue de l'IdO, ou que l'on considère les projections souhaitées par les acteurs du marché et la réalité du déploiement[1]. L'AIE[2] estime elle que le stock d'objets connectés dans le monde, incluant les objets connectés traditionnels (regroupés dans les catégories TIC et Divertissement), devrait passer **de 15 milliards en 2018 à 46 milliards en 2030**, ce qui représente une augmentation de 300 % sur cette période et un taux de croissance annuel moyen de 9,8 % ;

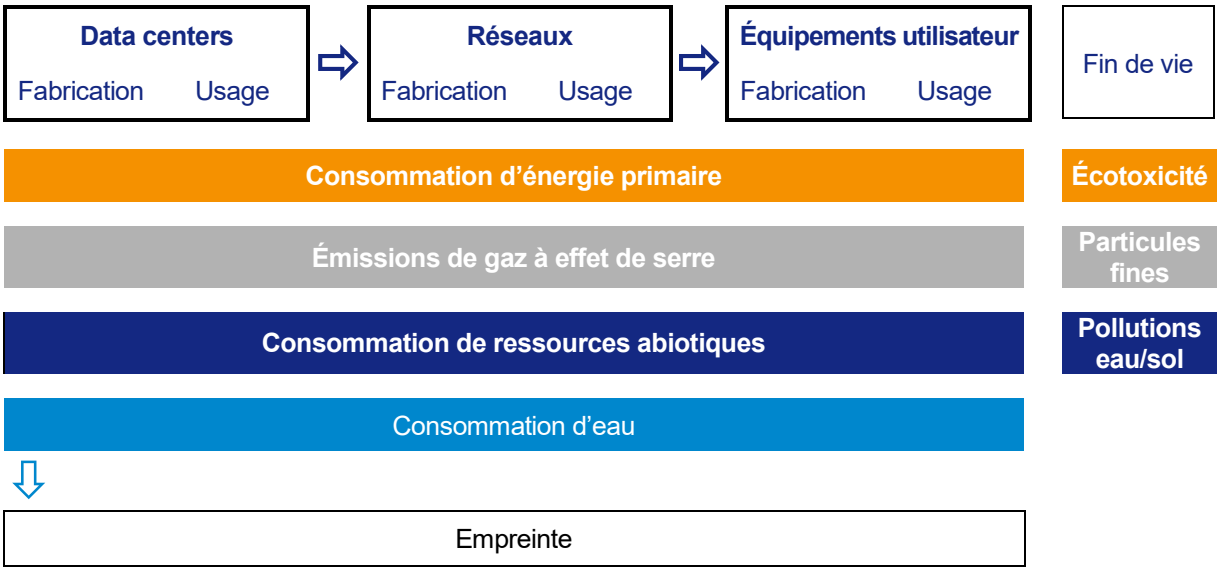
– des difficultés à estimer la durée de vie de ces objets qui présentent un double risque d'obsolescence à la fois physique (batteries notamment) et logicielle. Il existe aujourd'hui très peu d'études publiées sur l'analyse du cycle de vie de ces objets ;

– de la nature hétérogène de l'IdO et des champs d'application qu'il concerne ;

– des difficultés à estimer la diffusion des usages et des impacts qu'ils auront sur la consommation des réseaux et sur le développement des centres de calcul et de l'*edge computing* qui leur seront associés.

Définir l'empreinte environnementale de l'IdO nécessite de tenir compte de l'ensemble des segments mobilisés dans un dispositif, comme l'illustre le graphique ci-dessous.

Graphique 27 – Définir l'empreinte environnementale de l'Internet des objets



Source : Gauthier Roussilhe, audition du 28 octobre 2021

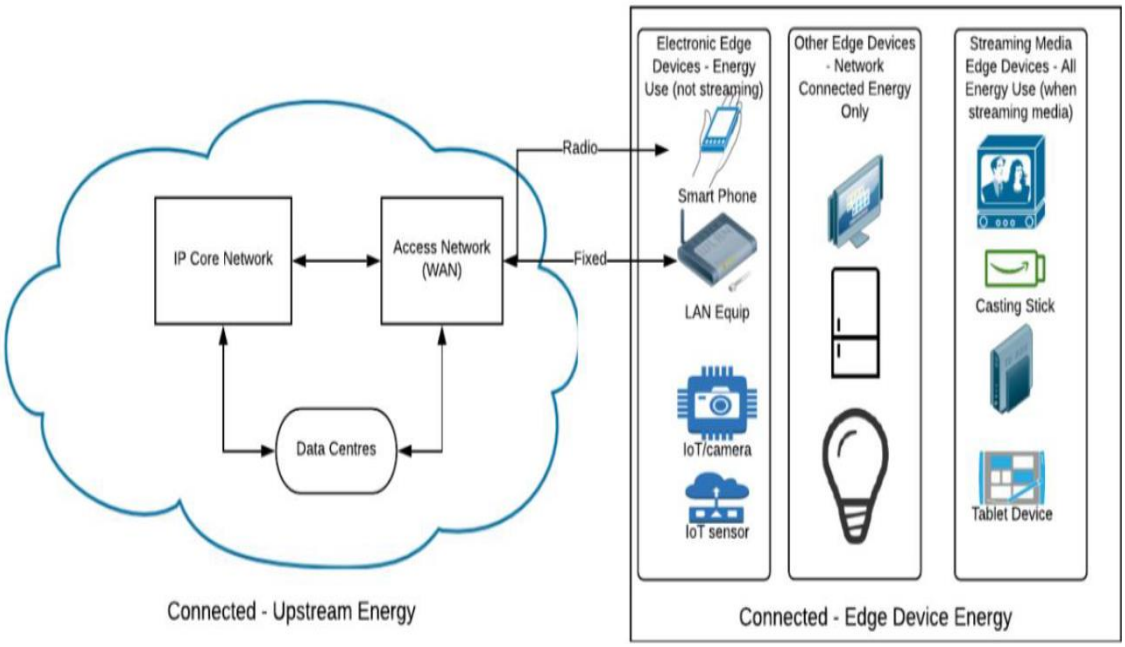
[1] Selon des sources variées : Statista (2021), Gartner (2018) ou CISCO (2020).

[2] AIE (2019), *Total Energy Model for Connected Devices*, *op. cit.*

Les éléments que nous avons pu recueillir ne concernent que les impacts relatifs à la consommation énergétique et aux émissions de gaz à effet de serre. Les données sur la consommation de ressources abiotiques ou en eau sont rares et lacunaires[1].

En 2019, l'Agence internationale de l'énergie publiait un modèle Total Energy Model (TEM 1.0) dont l'objectif est de mesurer la consommation énergétique des terminaux connectés[2]. Le périmètre du modèle ne couvre que les consommations liées à l'utilisation de dispositifs de l'IdO en couvrant un champ représentatif des objets et des technologies réseaux utilisées, mais qui ne prend pas en compte les phases de fabrication et de fin de vie des objets.

Graphique 28 – Périmètre du modèle d'estimation de la consommation énergétique de l'Internet des objets par l'Agence internationale de l'énergie



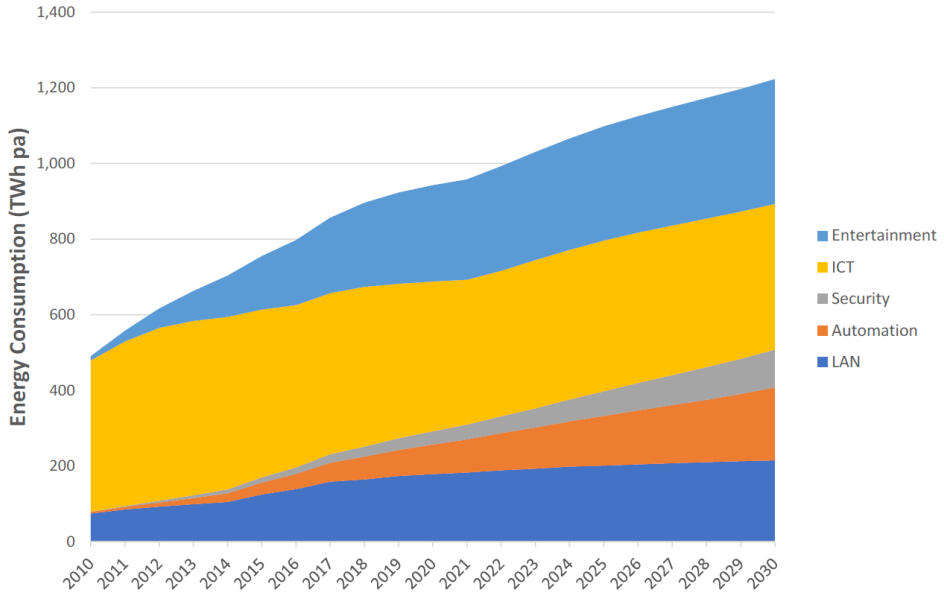
Source : AIE (2021), Total Energy Model 2.0 for Connected Devices, op. cit.*, p. 5*

Les projections du modèle de l'AIE, prévoient un triplement de la consommation énergétique, des terminaux connectés, d'ici 2030.

[1] Voir à ce sujet la publication Ademe et Arcep (2022), *Évaluation de l'impact environnemental du numérique en France…*, *op. cit.*, qui présente des indicateurs relatifs à ces ressources.

[2] Et sa mise à jour : AIE (2021), *Total Energy Model 2.0 for Connected Devices*, IEA 4E EDNA, programme de coopération technique de l'Agence internationale de l'énergie, février.

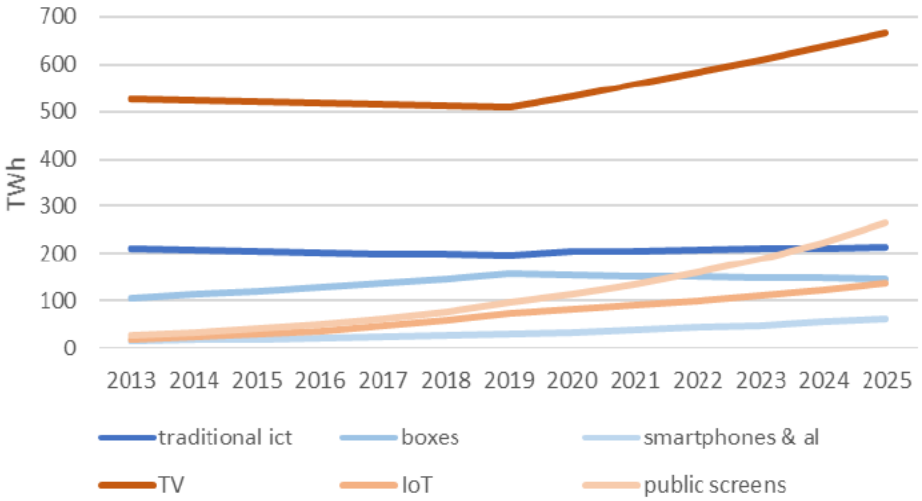
Graphique 29 – Évolution de la consommation énergétique mondiale des objets et terminaux connectés, par catégorie d'usage



Source : AIE (2021), Total Energy Model 2.0 for Connected Devices, op. cit.*, p. 24*

Le Shift Project estime quant à lui que la consommation électrique mondiale de l'Internet des objets pourrait dépasser les 200 TWh annuel pour le seul IdO[1].

Graphique 30 – Projection de la consommation électrique mondiale des terminaux en 2025



Source : The Shift Project ; Hugues Ferreboeuf, audition du 28 octobre 2021

[1] Sur une consommation globale du numérique de 2 990 TWh en 2017 selon The Shift Project, et qui devrait se situer entre 5 700 et 7 300 TWh par an en 2025.

Des études récentes permettent d'affiner ces estimations et proposent, à partir d'une approche par analyse de cycle de vie (ACV), d'établir des estimations convergentes. Deux études seulement ont permis d'établir à une échelle macro une estimation de l'empreinte carbone du déploiement massif de l'IdO dans le monde. La première[1] conclut que l'empreinte carbone de l'IdO pourrait générer entre 185 et 200 $MtCO_2eq$ (voir Tableau 17). Sa principale limite est qu'elle porte sur une période où le développement de l'IdO était encore restreint et qu'elle ne prend pas en compte les trajectoires de diffusion de l'IdO.

La seconde étude[2] montre une croissance exponentielle de l'empreinte carbone et estime à 2 000 $MtCO_2eq$ produit par l'IdO en 2025. Mais une troisième étude, la plus récente et qui émane de l'université de Louvain[3], considère cette estimation peu réaliste et présente à ce jour les résultats les plus aboutis. En étudiant plusieurs scénarios, qui tiennent compte de la complexité des objets connectés considérés, les auteurs concluent que l'empreinte carbone de l'IdO au niveau mondial à l'horizon 2027 pourrait se situer entre 22 et 1 124 $MtCO_2eq$.

Tableau 17 – Comparatif de différentes projections d'empreintes carbone de l'IdO

Estimations de l'empreinte carbone totale du numérique au niveau mondial	Projections de l'empreinte carbone mondiale de l'IdO	Référence	Période
1,8 $GtCO_2eq$ en 2017 selon The Shift Project[a]	**185 à 200 $MtCO_2eq$**	Malmodin *et al.*, 2018	2010-2015
1,4 $GtCO_2eq$ en 2019 selon GreenIT[b]	**2 000 $MtCO_2eq$**	Das, 2019	Horizon 2025
2 $GtCO_2eq$ en 2020 selon Freitag[c]	**22 à 1 124 $MtCO_2eq$**	Pirson et Bol, 2021	2020-2027
2,8 à 3,1 $GtCO_2eq$ horizon 2025 selon The Shift Project[d]			

(a) The Shift Project (2018), *Lean ICT. Pour une sobriété numérique*, rapport, octobre.

(b) GreenIT.fr (2019), *Empreinte environnementale du numérique mondial*, septembre.

(c) Freitag C., Berners-Lee M., Widdicks K. *et al.* (2021), *The climate impact of ICT…*, *op. cit.*

(d) Selon les scénarios révisés de Shift Project : « Impact environnemental du numérique : tendances à 5 ans et gouvernance de la 5G », mars 2021 ; et audition du 18 octobre 2021.

Source : France Stratégie

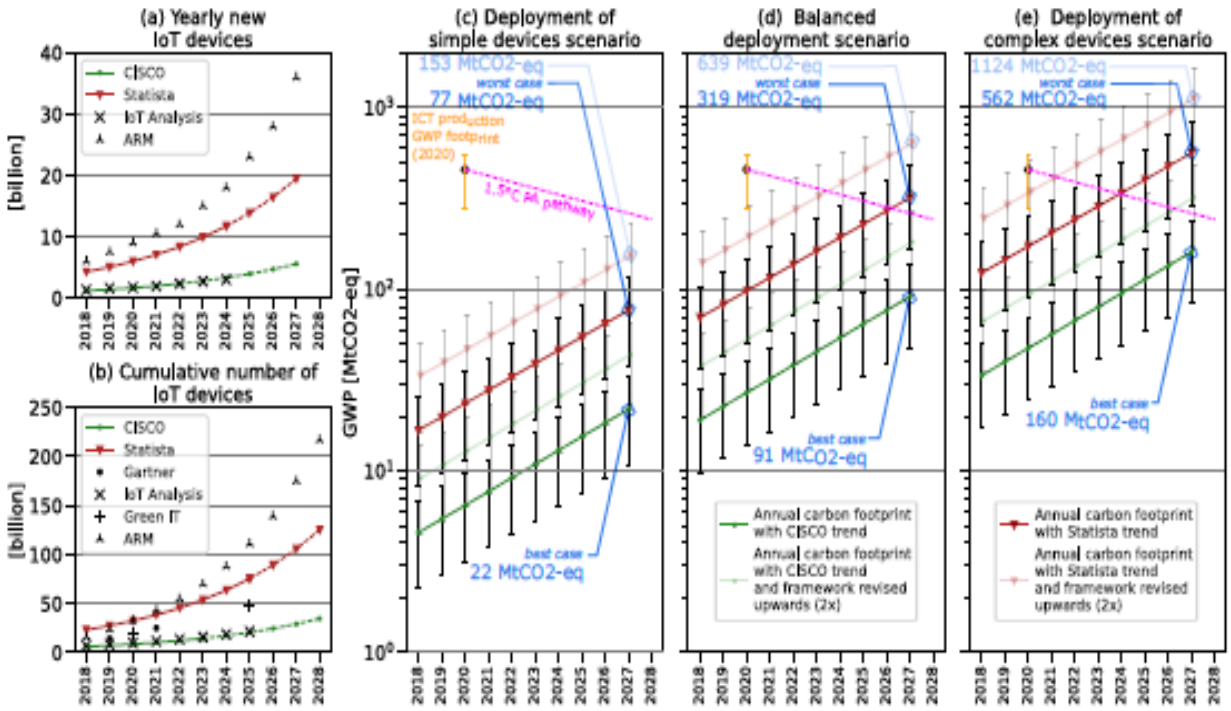
[1] Malmodin J. et Lundén D. (2018), « The Energy and Carbon Footprint of the Global ICT and E & M Sectors 2010-2015 », *Sustainability*, 10(9), mai.

[2] Das S. et Mao E. (2020), « The global energy footprint of information and communication technology electronics in connected Internet-of-Things devices », *Sustainable Energy, Grids and Networks*, vol. 24(3), décembre.

[3] Pirson T. et Bol D. (2021), « Assessing the embodied carbon footprint of IoT edge devices with a bottom-up life-cycle approach », *Journal of Cleaner Production*, vol. 322, novembre.

Ainsi l'étude de Louvain, la plus récente, présente une fourchette d'estimation très large car elle s'appuie sur un modèle tenant compte de la nature des périphériques IdO observés et de leur niveau de complexité. Dans ce modèle, les auteurs distinguent des objets aux fonctionnalités limitées (tel le capteur de présence) dont l'empreinte carbone moyenne est estimée à environ 1,4 $kgCO_2eq$ et des objets plus complexes dont l'empreinte carbone est plus importante (jusqu'à 14,9 $kgCO_2eq$ pour un assistant connecté à domicile, jusqu'à 23,4 $kgCO_2eq$ pour un drone et jusqu'à 19,5 $kgCO_2eq$ pour une montre intelligente). Le rapport entre les valeurs supérieures et inférieures de chaque résultat peut atteindre un facteur 5. Les projections s'articulent autour de trois scénarios présentant une part variable de chaque profil de matériel par rapport au nombre total d'appareils déployés à l'horizon 2025.

Graphique 31 – Projection de l'empreinte carbone de l'IdO, sur la base des projections de Pirson et Bol (2021)



(a) Déploiement annuel de nouveaux appareils IdO calculé sur la base des tendances

(b) Cumul du nombre d'appareils Id0, selon les études de marché et les prévisions les plus populaires

(c-e) Analyse macroscopique de l'empreinte carbone annuelle générée par la production d'appareils IdO pour les différents scénarios de déploiement : (c) le Scénario 1 considère le déploiement d'une majorité d'appareils simples, (d) le Scénario 2 considère le déploiement équilibré d'appareils simples et complexes et (e) le Scénario 3 considère le déploiement d'une majorité de dispositifs complexes.

Source : Pirson T. et Bol D. (2021), « Assessing the embodied carbon footprint of IoT edge devices… », op. cit.

Ces chiffres témoignent des difficultés à disposer d'outils de mesure fiables et robustes. Le périmètre retenu dans les modèles (nature des réseaux, nature des objets connectés),

la prise en compte des phases de vie de l'objet (fabrication, exploitation) ou encore la pondération des usages retenus font fortement varier les projections. S'y ajoutent les perspectives de déploiement encore très incertaines. **Mais tous ces chiffres convergent pour souligner que l'IdO aura un rôle important dans l'évolution globale de l'empreinte environnementale du numérique.** Les scénarios présentés ici, même dans leurs options les plus optimistes, et en tenant compte des éventuels bénéfices du déploiement de l'IdO, sont incompatibles avec les objectifs de réduction des gaz à effet de serre prévus par de l'accord de Paris (Pirson et Bol, 2021).

BRÈVES DU MONDE

Dans son rapport de mai 2021, l'ONG Greenpeace East Asia évalue qu'en 2020, la consommation d'électricité associée à la 5G et aux centres de données **en Chine** aurait atteint 201 TWh – équivalente donc aux consommations annuelles des villes de Pékin et de Shenzhen combinées, ou encore à 2,7 % de la consommation nationale. Plus de 60 % de l'électricité utilisée par ces infrastructures numériques provient du charbon, ce qui porte les émissions du secteur à près de 123 millions de tonnes de CO_2 en 2020. Selon les projections réalisées pour 2035, leur consommation électrique devrait exploser pour atteindre 782 TWh (+289 % par rapport à 2020), soit 5 % à 7 % du total national, dont 297 TWh pour le seul secteur de la 5G (+488 %). Au total, les émissions liées aux infrastructures numériques devraient continuer à augmenter d'ici 2035, et atteindre 310 Mt. Le rapport relève que seules deux grandes entreprises chinoises exploitant des centres de données se sont à ce jour engagées à atteindre 100 % d'énergies renouvelables d'ici 2030 (Chindata et Athub).

Greenpeace a également publié cette année son deuxième rapport annuel *Clean Cloud* pour la Chine, qui évalue les performances climatique et énergétique des 22 plus grands fournisseurs de services *cloud* et d'opérateurs de centres de données chinois.

Sur la partie amont de la chaîne de valeur, un autre récent rapport de Greenpeace réalisé avec l'Institut de l'environnement de l'université Renmin estime que les émissions liées à la production des « nouvelles infrastructures » en 2020 sont inférieures de 7,24 % à celles des infrastructures traditionnelles, soit environ 172,7 Mt contre 186,1 Mt de CO_2. Mais le potentiel des « nouvelles infrastructures » en matière de réduction d'émissions reste assez limité tant que l'ensemble de la chaîne d'approvisionnement reposera sur le bouquet énergétique chinois très dépendant du charbon. En effet, la production en amont des « nouvelles infrastructures » provoque une forte demande en produits issus des secteurs énergivores et très émissifs, notamment la métallurgie, la chimie et les produits minéraux non métalliques. Ainsi, en l'absence de normes environnementales pour l'ensemble de la chaîne d'approvisionnement, les gains en matière d'efficacité énergétique et de réduction d'émissions liées à l'exploitation de ces nouvelles infrastructures du numérique pourraient être facilement contrebalancés par les industries en amont.

Source : Direction générale du Trésor ; pour un tableau par pays et des sources détaillées, voir annexe 7

2.2. Et à l'échelle de la France ?

La France, qui vient de voter la loi n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique fait figure de précurseur en Europe sur ces questions.

La mission parlementaire d'information[1] conduite par les sénateurs Patrick Chaize et Hervé Maurey a estimé qu'à politique constante le numérique représentera en 2040 près de 7 % des émissions de gaz à effet de serre de la France (actuellement 4,7 %) et cette croissance sera principalement due à l'essor de l'IdO et aux émissions des centres de calcul. Le coût collectif de ces émissions pourrait passer d'un à douze milliards d'euros entre 2019 et 2040.

> « En 2040, si tous les autres secteurs réalisent des économies de carbone conformément aux engagements de l'Accord de Paris et si aucune politique publique de sobriété numérique n'est déployée, le numérique pourrait atteindre près de 7 % (6,7 %) des émissions de gaz à effet de serre de la France, un niveau bien supérieur à celui actuellement émis par le transport aérien (4,7 %). La part des terminaux et des équipements constitue une large partie de cette augmentation, selon cette même étude, les terminaux contribueraient à 80 % de l'empreinte carbone du numérique français, en tenant compte des phases de fabrication et de la distribution (la "phase amont") et des phases d'utilisation de ces terminaux. »[2]

Les premiers travaux conduits par l'Ademe et l'Arcep[3], produits dans le cadre de la mise en place d'un observatoire des impacts environnementaux du numérique en France, apportent une vision des impacts environnementaux du numérique en France. L'empreinte carbone du numérique y est estimée à près de 17 $MtCO_2eq$ – plus importante que le secteur des déchets (14 $MtCO_2eq$) **dont 460 000 tCO_2eq pour le seul IdO. À l'horizon 2040**, la part de l'Internet des objets pourrait s'accroître à plus de 6 $MtCO_2eq$[4], sur les **24 $MtCO_2eq$ pour le numérique dans sa globalité**[5]**.**

[1] Chaize P. et Maurey H. (2020), *Pour une transition numérique écologique*, rapport d'information fait au nom de la commission de l'aménagement du territoire et du développement durable, juin. Les chiffres présentés ci-après sont issus de Citizing, KPMG et Virtus management (2020), *Étude relative à l'évaluation des politiques publiques pour réduire l'empreinte environnementale du numérique*, *op. cit.*

[2] Chaize P. et Maurey H. (2020), *Pour une transition numérique écologique*, *op. cit.*

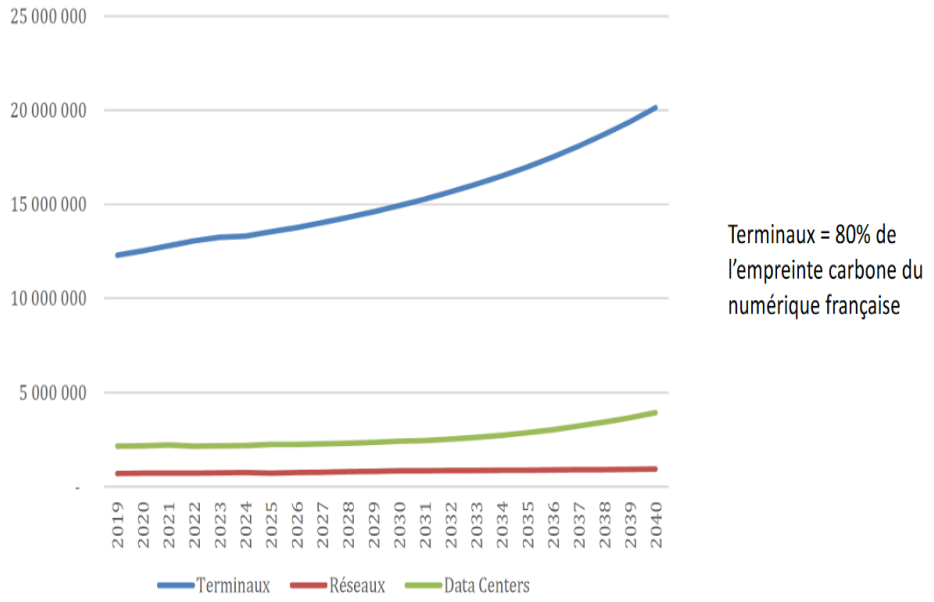
[3] Ademe et Arcep (2022), *Évaluation de l'impact environnemental du numérique en France…*, *op. cit.*

[4] Citizing, KPMG et Virtus management (2020), *Étude relative à l'évaluation des politiques publiques pour réduire l'empreinte environnementale du numérique*, *op. cit.* ; Hugues Ferreboeuf, audition du 28 octobre 2021.

[5] Citizing, KPMG et Virtus management (2020), *Étude relative à l'évaluation des politiques publiques pour réduire l'empreinte environnementale du numérique*, *op. cit.*

La consommation électrique annuelle du numérique est estimée à plus 48 TWh/an soit 10 % de la consommation électrique annuelle française[1]. Sur la base d'un nombre d'objets connectés installés en France de 244 millions, consommant en moyenne 30 KWh/an[2], la consommation électrique des objets connectés serait d'environ 7,2 TWh/an soit 15 % de la consommation électrique des biens et services numériques.

Graphique 32 – Émissions de gaz à effet de serre du numérique en tCO_2eq, à l'horizon 2040, en France



Source : Citizing, KPMG et Virtus management (2020), Étude relative à l'évaluation des politiques publiques pour réduire l'empreinte environnementale du numérique*, étude réalisée à la demande de la commission de l'aménagement du territoire et du développement durable du Sénat, juin, p. 74 – scénario central en tCO_2eq*

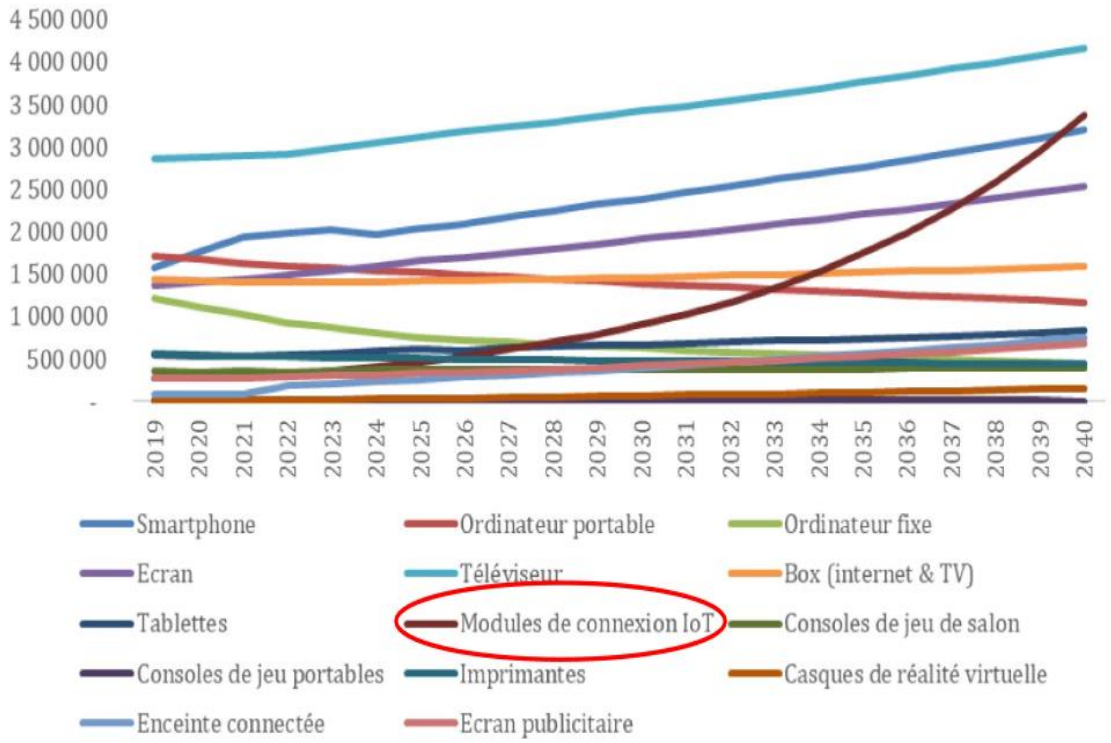
Mais que représente, plus précisément l'Internet des objets ? À l'occasion des auditions, nous avons pu obtenir des chiffres pour affiner ces premières estimations, en distinguant notamment la part des objets connectés.

Selon nos interlocuteurs, la part des terminaux de la catégorie « objets connectés » à l'horizon 2040, en tenant compte des phases amont et utilisation confondues, sera en France le deuxième poste d'émission de gaz à effet de serre après les téléviseurs.

[1] Ademe et Arcep (2022), *Évaluation de l'impact environnemental du numérique en France…*, *op. cit.*

[2] Sur la base d'une estimation d'une consommation électrique moyenne d'un objet connecté de 30 KWh fournie par le cabinet BCG, toutefois, le rapport Ademe et Arcep (2022) fournit des valeurs plus basses : 1 smartphone = 3,9 KWh/an (usage individuel), 1 tablette = 18,6 KWh/an, 1 enceinte connectée = 23 KWh/an.

Graphique 33 – Projection des émissions de gaz à effet de serre par catégories de terminaux en France en tCO_2eq, horizon 2040



Sources : Citizing, KPMG et Virtus management (2020), Étude relative à l'évaluation des politiques publiques pour réduire l'empreinte environnementale du numérique, op. cit.*, p. 60 – scénario central ; Hugues Ferreboeuf, audition du 28 octobre 2021*

Ces estimations réalisées en juin 2020 paraissent d'ores et déjà trop optimistes, au regard des résultats de l'équipe de recherche de l'université de Louvain. Elles conduisent à réviser cette estimation et à doubler les projections (voir Tableau 18).

Ces chiffres ne représentent toutefois qu'une estimation des émissions directes dues aux dispositifs IdO. Ils ne prennent pas en compte les effets relatifs aux flux de données, à l'empreinte des réseaux et des centres de calcul, ni les effets de l'*edge computing*, ni l'empreinte environnementale globale, qu'il faudrait être en mesure de calculer sur l'ensemble du cycle de vie des objets – démarche actuellement impossible à conduire en raison de l'absence de données.

Tableau 18 – Évolution de l'empreinte environnementale de l'Internet des objets, 2020-2040

Émissions de gaz à effet de serre pour les modules IdO *en milliers de tCO_2eq*	**2020**	**2030**	**2040**
Estimation juin 2020	284	903	2763
Estimation octobre 2021*	460	1 630	6 081

* Ces estimations révisées sont fondées sur une empreinte carbone embarquée moyenne de 3 kg (CO_2eq) en 2020, 4 kg en 2030 et 5 kg en 2040. Ces chiffres prennent en compte la dispersion du niveau de complexité des modules et l'hypothèse que le mix moyen va augmenter en complexité au cours du temps. Toutes choses égales par ailleurs, la valeur de référence est plutôt basée sur le chiffre moyen (« *typical* ») de l'étude Pirson et Bol (2021), *op. cit.*

Sources : Citizing, KPMG et Virtus management (2020), op. cit. *; Hugues Ferreboeuf, audition du 28 octobre 2021*

Tableau 19 – Synthèse des projections de l'empreinte carbone de l'IdO pour la France et le monde

	Horizon	**Estimation borne inférieure**	**Estimation borne haute**	**Source**
Numérique global				
GES monde	2020	1 $GtCO_2eq$	2 $GtCO_2eq$	Freitag *et al.* 2021
GES monde	2019	1,4 $GtCO_2$	Idem	GreenIT[a]
GES monde	2019	1,5 $GtCO_2eq$[b]	1,8 $GtCO_2eqc$	The Shift Project
GES France	2021	16,9 $MtCO_2eq$[d]	Idem	Ademe/Arcep
Internet des objets*				
GES IOT monde	2025	22 $MtCO_2eq$	1 124 $MtCO_2eq$	Pirson et Bol 2021
GES IOT France	2030	0,93 $MtCO_2eq$	1,6 $MtCO_2eq$	The Shift Project[e]

* Comme nous l'avons vu plus haut, ces chiffres peuvent recouvrir des périmètres relativement différents, en termes d'objets observés (PC, smartphones ou connecteurs, TV), et comprendre ou non les phases de production, d'utilisation et de reconditionnement.

(a) GreenIT.fr (2019), *Empreinte environnementale du numérique mondial*, *op. cit.*

(b) The Shift Project (2018), *Lean ICT. Pour une sobriété numérique*, *op. cit.*

(c) Selon les scénarios révisés de Shift Project : « Impact environnemental du numérique : tendances à 5 ans et gouvernance de la 5G », mars 2021.

(d) Ademe et Arcep (2022), *op. cit*.

(e) Audition de Hugues Ferreboeuf, 28 octobre 2021.

Source : auteurs

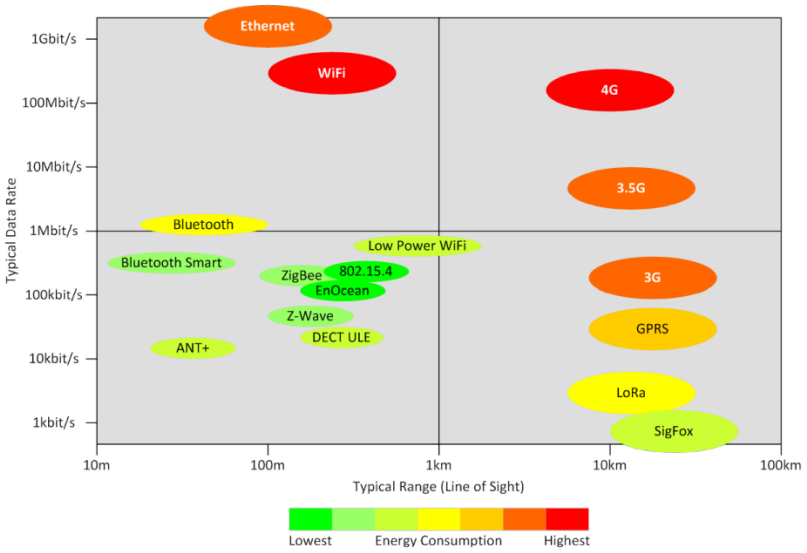
Force est donc de constater **une très grande hétérogénéité des projections de l'empreinte environnementale de l'IdO au niveau mondial et pour la France. Toutefois les ordres de grandeur convergent** pour souligner que le déploiement massif de l'IdO contribuera de façon significative à l'empreinte globale du numérique sur l'environnement. Il y a donc une réelle nécessité à disposer d'outils de mesure plus

robustes, prenant pleinement en compte les spécificités de l'Internet des objets (massification, typologie des objets, analyse du cycle de vie, etc.) qui sont encore mal appréhendées dans les modèles existants.

2.3. La consommation des réseaux et les effets rebonds

Pour avoir une vision complète des débats sur les impacts environnementaux des technologies numériques, il faut tenir compte de l'évolution des technologies et des innovations qui permettront d'améliorer les performances environnementales de ces équipements. Ainsi l'efficacité et la performance énergétiques des réseaux de télécommunications s'accroît, mais le type de réseaux sur lesquels les dispositifs vont se déployer pourrait avoir un fort impact sur la consommation énergétique globale de l'IdO et du numérique. Dès 2016, l'AIE présentait dans son rapport[1] une comparaison des différents potentiels de consommation des réseaux de télécommunications (Graphique 34).

Graphique 34 – Comparaison des réseaux, par débit, portée et consommation énergétique



Source : AIE (2016), Energy Efficiency of the Internet of Things. Policy Options*, op. cit.*

Les technologies avec de faibles émissions de données sont positionnées dans le rectangle inférieur, celles permettant des débits plus élevés sont placées dans le rectangle supérieur. L'abscisse indique la portée des réseaux, la couleur indiquant le niveau de consommation énergétique. Le graphique ne mentionne pas encore la 5G : comme les autres technologies cellulaires, elle viendra se placer dans le carré en haut à droite.

[1] AIE (2016), *Energy Efficiency of the Internet of Things. Policy Options*, document préparé pour l'IEA 4E EDNA, Agence internationale de l'énergie, juillet.

Le choix des réseaux doit également tenir compte des besoins et des fonctionnalités des dispositifs IdO qui doivent être utilisés. Comme nous l'avons vu, certaines technologies réseaux sont plus adaptées à certains usages. Dans cette même étude de 2016, l'AIE avait déjà identifié les meilleures adéquations entre les cas d'usages et les technologies réseaux, en tenant compte des effets sur la consommation d'énergie. Sur le Tableau 20, on distingue quatre catégories :

– la technologie ne correspond pas aux exigences de l'application (blanc) ;

– la technologie n'est pas recommandée, elle répond voire excède les besoins de l'application, mais est très consommatrice d'énergie (orange) ;

– la technologie correspond aux besoins de l'application et la consommation d'énergie est raisonnable (beige) ;

– la technologie est le meilleur choix, elle correspond aux besoins de l'application et présente le meilleur bilan énergétique des technologies possibles (bleu).

Tableau 20 – Technologies de réseaux adaptés aux usages de l'Internet des objets

Domaine applicatif	Application	Équipement terminal	ANT+	Bluetooth	Bluetooth smart	DECT ULE	Z-Wave	Zig-Bee	802-15-4-2011 based	EnOcean	Wifi	Low Power Wifi	Ethernet	GPRS	3G (UMTS)	3,5G (HSPA)	4G (LTE)	LoRa	Sigfox
Maison intelligente	Éclairage intelligent	Ampoules LED intelligentes	possible	recommandée	disponible	possible	possible	possible	possible	possible	recommandée	possible							
		Passerelles applicatives									possible	disponible	possible	possible	recommandée	recommandée	recommandée		
	Automatisation de la maison	Capteurs	possible	recommandée	possible	possible	possible	possible	disponible	disponible	recommandée	possible	recommandée						
		Actuateurs	possible	recommandée	possible	possible	possible	possible	disponible	disponible	recommandée	possible	recommandée						
		Caméras									possible		disponible		possible	possible	possible		
		Passerelles applicatives									possible		disponible		possible	possible	possible		
	Appareils intelligents	Appareils intelligents	possible	recommandée	disponible	possible	possible	possible	disponible	disponible	recommandée	possible	recommandée						
		Passerelles applicatives									possible	disponible	possible	possible	recommandée	recommandée	recommandée		
Mobiité intelligente	Route intelligente	Unités en bord de route									disponible								
	Éclairage public intelligent	Luminaires d'éclairage public												possible	recommandée	recommandée	recommandée	disponible	disponible

Technologie possible — Technologie disponible
Technologie recommandée — Technologie inadaptée

Source : AIE (2016), Energy Efficiency of the Internet of Things. Policy Options*, op. cit.*

Absente de cette analyse comparative, la 5G apportera des gains en matière d'efficacité énergétique au regard des autres réseaux cellulaires. Les acteurs du secteur télécom estiment que la 5G sera 10 fois plus efficace énergétiquement que la 4G à l'horizon 2025[1] grâce à l'optimisation des processeurs, aux mécanismes de partage des réseaux, aux meilleures performances des antennes (Mimo) et aux possibilités de mise en veille d'une partie du réseau. Selon une étude de l'université de Zurich, les cas d'utilisation soutenus par la 5G pourraient éviter dans un scénario optimiste 0,6 $MtCO_2eq$/an ou dans un scénario moins optimiste 0,1 $MtCO_2eq$/an, soit au total en 2030 jusqu'à 2,1 $MtCO_2eq$ à l'échelle de la Suisse[2]. Toutefois, ces éléments sont loin de faire l'unanimité (voir Encadré).

Encadré 4 – Éléments récents sur l'empreinte environnementale de la 5G

L'opérateur Huawei, dans une étude récente[3], estime que l'installation des antennes 5G en Chine va conduire à un doublement de la consommation énergétique des réseau télécoms (de 50 milliards à 100 milliards de kWh) générant près 27 $MtCO_2eq$ annuellement pour la Chine. Ces estimations ne peuvent être comparées aux projections en France ou en Europe, en raison notamment de la différence du mix énergétique propre à chaque pays, mais elles restent importantes.

En outre, la 5G qui, pour des besoins d'efficacité énergétique et de débit en zone dense, exploite des ondes d'une portée limitée, nécessitera de multiplier les antennes[4] et d'accroître logiquement la consommation électrique des réseaux.

D'autres effets, négatifs pour l'environnement, sont à craindre. Selon une étude de Qualcomm, fabricant de processeurs pour smartphones[5], les terminaux 5G conduiront à consommer plus d'énergie afin d'absorber les débits de données prévus. Enfin, les effets rebond de la 5G sont déjà observables puisque la consommation de données d'un utilisateur 5G serait de 1,7 à 2,7 fois supérieure à celle d'un utilisateur 4G, selon une étude de 2020 portant sur les premiers utilisateurs 5G dans plusieurs pays[6].

Source : Anne-Cécile Orgerie, membre du comité d'experts

[1] Conseil national de l'industrie (2020), *Contribution et éclairage du CSF Infrastructures numériques sur la question environnementale associée au numérique et à la 5G*, *op. cit.*

[2] Hischier R. et Hilty L. (2019), *The Challenges of Scaling the Internet of Things*, ETH Zurich, août.

[3] Dongxu C. et Wanxiang Y. (2020), « 5G Power: Creating a green grid that slashes costs, emissions & energy use », Huawei, juillet.

[4] Conseil national de l'industrie (2020), *op. cit.*

[5] Signals Research Group (2019), *A Global Perspective of 5G Network Performance*, octobre.

[6] Voir Rizzato F. (2020), « 5G users on average consume up to 2.7x more mobile data compared to 4G users », *Open Signal*, 21 octobre.

Les études tendent à montrer qu'il existe bien une complémentarité des technologies et quand la dimension environnementale est intégrée dans les critères de choix, cette complémentarité est encore plus pertinente.

Ces éléments nous conduisent à nous interroger sur les arguments portés par certains acteurs qui consisteraient à déployer partout la même technologie de communication. **Ainsi le déploiement de la 5G peut répondre à certains des usages de l'IdO, mais il serait incorrect de laisser penser que le développement de l'IdO serait dépendant du déploiement massif de la 5G**.

En outre, le déploiement de la 5G aura d'autres impacts sur l'environnement, au-delà de son utilisation dans des cas d'usages de l'IdO.

2.4. Risques environnementaux : interroger nos pratiques et parier sur la sobriété des usages

On voit combien il est difficile de mesurer les bénéfices nets de l'Internet des objets en matière d'empreinte environnementale. S'il existe des mesures dans certaines filières, ou pour certains cas d'usages ponctuels, il est nécessaire de disposer d'indicateurs plus fiables. Les industriels mais aussi les acteurs publics et notamment les collectivités ont besoin d'outils et de modèles pour accompagner des décisions qui engagent leurs investissements (CAPEX et OPEX).

L'Internet des objets aura un coût environnemental – consommation en énergie et en ressources – que des initiatives récentes en France vont permettre d'affiner[1]. Pour l'heure, est-il possible d'affirmer qu'un déploiement massif de l'IdO dans tous les secteurs d'activité sera bénéfique pour réduire l'empreinte environnementale de l'activité humaine ? Rien n'est moins sûr.

En revanche, une adoption raisonnée priorisant des usages où les bénéfices sont avérés (santé, sécurité, etc.) pourrait être largement bénéfique à l'ensemble de la société. Par exemple, est-il viable de déployer un dispositif de pilotage du chauffage dans un bâtiment non isolé pour un gain moyen de 20 % de la consommation énergétique, alors que le même dispositif dans un bâtiment isolé pourrait réduire la consommation énergétique de 70 %[2] ?

[1] Loi pour la réduction de l'empreinte environnementale du numérique, du 21 novembre 2021 et initiative NegaOctets.

[2] Audition d'Éric Vidalenc le 11 octobre 2021.

S'agissant de l'empreinte environnementale du numérique et de sa réduction, les premiers jalons ont été posés au niveau international[1], mais surtout européen[2] et national[3]. Ils fixent des orientations sur de nombreux points : substances utilisées, prévention et traitement des déchets, éco-conception, allongement de la durée de vie des appareils, filière de recyclage ou encore information des consommateurs sur l'empreinte environnementale des appareils.

La loi AGEC[4] a largement renforcé le principe de la responsabilité élargie des producteurs d'équipements électriques et électroniques, qu'ils soient ménagers ou professionnels. Il est établi qu'ils sont responsables de l'enlèvement et du traitement de ces produits.

Mais **l'Internet des objets fait jaillir des problématiques nouvelles comme la collecte et le recyclage d'objets initialement non connectés qui deviennent communicants et qui ne sont pas couverts par ces dispositifs** (jouets connectés, par exemple).

La première question porte sur la filière. Quelle est la filière de tri la plus adaptée pour les produits hors filières DEEE (déchets d'équipements électriques et électroniques) et qui potentiellement peuvent devenir connectés, tels que des produits textiles, mobilier, etc. Les filières sont aujourd'hui distinctes : laquelle sera la plus efficace pour le traitement de ces déchets d'un nouveau type, la filière historique ou la filière DEEE ?

Cette phase de tri de ces objets implique également l'information du consommateur qui devra être en capacité d'identifier le circuit de tri adapté.

En matière de recyclage, les composants insérés dans les objets, y compris des équipements DEEE, posent des difficultés techniques en raison de leur miniaturisation pour la séparation des composants et la récupération des matières sensibles ou stratégiques.

C'est donc un travail avec les filières actuelles et des éco-organismes concernés (notamment ceux de la filière DEEE) qu'un travail de prise en compte de ces enjeux doit

[1] Voir à ce sujet OCDE (2021a), « Recommandation du Conseil sur la connectivité à haut débit », adoptée en février 2021.

[2] La directive européenne RED (directive 2014/53/UE11) concerne la mise sur le marché des équipements radioélectriques (tout émetteur ou récepteur de radiocommunication, y compris les récepteurs de radiodiffusion et de télévision. Les équipements entrant dans son domaine d'application et disponibles sur le marché européen doivent être obligatoirement conformes à cette directive ; la directive DEEE relative à la gestion des déchets des équipements électriques et électroniques, le règlement batterie ou les réglements écodesign, etc.

[3] La loi n° 2020-105 du 10 février 2020 relative à la lutte contre le gaspillage et à l'économie circulaire et la loi n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnemental du numérique en France.

[4] *Ibid*.

être conduit[1]. La révision de la directive européenne sur les DEEE pourrait être l'occasion de maîtriser au niveau européen ces enjeux.

Développer un Internet des objets plus vertueux en termes d'impact environnemental est possible dès lors que les critères de sobriété sont envisagés dès la conception des services, depuis le choix des réseaux jusqu'à leur recyclage en passant par la conception et la fabrication des objets, dans la mesure où la nature hybride des objets connectés sera prise en compte dans les dispositifs réglementaires existants et futurs.

C'est le sens des recommandations n° 2, 7, 8, 16, 17, 18, 19, 20, 21 et 22.

N° 2 – Veiller à la prise en compte d'un volet IdO dans le nouvel observatoire des impacts environnementaux du numérique.

N° 7 – Permettre la mise en place d'expérimentations à grande échelle.

N° 8 – Encourager le partage de données, y compris au niveau international.

N° 16 – Étendre le champ de compétence de la CNDP sur les questions relatives au numérique et à l'environnement.

N° 17 – Organiser les filières de recyclage adaptées aux objets connectés.

N° 18 – Inclure les dispositifs IdO dans le référentiel général d'éco-conception des services numériques.

N° 19 – Intégrer dans la gestion du spectre des dispositifs d'incitation à des usages frugaux des réseaux.

N° 20 – Mettre à disposition des collectivités des outils de mesure d'impacts et d'aide à la décision.

N° 21 – Sensibiliser l'utilisateur des objets connectés aux impacts de ses usages sur l'environnement mais aussi sur sa sécurité.

N° 22 – Compléter la liste des produits concernés par l'indice de réparabilité.

[1] Le nouveau cahier des charges pour la filière DEE, couvrant la période 2022-2027, a été publié le 31 octobre 2021.

BRÈVES DU MONDE

En Israël, l'excès de consommation électrique en raison du développement des objets connectés ne semble pas faire l'objet de débats publics[1]. Une étude menée par ISOC-IL reconnaît cependant le risque d'augmentation de la consommation électrique qu'induiront les produits connectés mais considère en même temps que ces produits pourront entraîner des économies d'énergie s'ils permettent une régulation de la consommation (aménagement de l'éclairage public, etc.). Il souhaite à cet égard que le ministère de l'Environnement soit largement impliqué[2]. Quelques rares voix (ONG) se font entendre cependant sur le coût environnemental de la gestion du froid dans un climat désertique et chaud ou sur l'acquisition des terrains nécessaires dans un pays qui manque par ailleurs d'espaces[3].

Au Nigéria, le sujet environnemental apparaît en général loin d'être une priorité. Il semble que le recours aux technologies sobres en énergie (LoRaWan, LTE-M) soit le plus à même de faire du développement de l'IdO un phénomène bénéfique pour l'environnement dans ce pays.

L'Inde est le seul pays d'Asie du Sud à disposer d'un règlement spécifique sur les déchets électroniques. En 2016, les règles ont été élargies afin d'introduire des « organisations de responsabilité du producteur » visant à collecter et à recycler les déchets électroniques, ainsi que des programmes de rachat des déchets électroniques, de cautions et d'échanges. Une modification des règles en 2018 a introduit des objectifs de collecte annuels pour les producteurs : par exemple, à partir de 2023, les producteurs doivent collecter au moins 70 % en masse de leurs produits arrivant en fin de vie.

La fondation Shakti en lien avec PWC et l'entité semi-publique India Smart Grids Forum a publié en 2018 une étude sur l'efficacité énergétique de l'IoT. L'étude estime la consommation énergétique des objets connectés en veille pour dix cas d'usage (ampoule intelligente, système d'éclairage urbain, irrigation, prises, compteurs, thermostats, chauffe-eaux, réfrigérateurs, télévision et systèmes de domotique) et propose des recommandations pour la réduire. À l'exception de cette étude, les autres documents identifiés se concentrent principalement sur les bénéfices de l'IdO en termes de réduction de la consommation énergétique pour certains cas d'usage. On peut citer notamment une étude de l'agence publique Bureau of Energy Efficiency en

[1] Avec la transition de la production électrique du charbon vers le gaz, grâce à la production nationale *offshore*, Israël estime être dans une position plutôt vertueuse à cet égard.

[2] Selon la recommandation de l'ISOC-IL, le ministère chargé de la Protection de l'environnement devrait accompagner la mise en œuvre des technologies IdO, tout en évaluant les augmentations qui en résulteraient et en les comparant aux avantages économiques et environnementaux qu'elles sont supposées apporter.

[3] Voir l'article « Tech giants battle for data center real estate in Israel » du journal anglophone *Globe Business Israel*, 27 septembre 2021 : « *The public still perceives data centers as harmless, air-conditioned high-tech office spaces, rather than industrial plants, with most ignoring the environmental consequences brought about by this construction*. »

lien avec GIZ de juillet 2021 sur les bâtiments résidentiels intelligents et celle du think tank CEEW sur l'air conditionné.

En Estonie, tous les interlocuteurs interrogés par le service économique ont confié que l'enjeu environnemental était secondaire. L'important était l'efficacité économique. De ce fait, les régulations plus strictes envers les solutions polluantes conduisent l'IdO à se vouloir plus vertueux, mais ce n'est pas une conscience environnementale qui guide ce changement. Par exemple, la question de la consommation des centres de calcul est uniquement abordée à travers le prix de l'électricité consommée, y compris dans le monde universitaire.

En Chine, d'après les données officielles[1], la capacité de traitement annuelle des déchets DEEE (équipements électriques et électroniques) est de 160 millions d'unités (téléviseurs, réfrigérateurs, machines à laver, climatiseurs, ordinateurs), avec 2,18 millions de tonnes de déchets effectivement traités en 2019. Ce chiffre est bien en deçà de la quantité théorique de déchets DEEE (14 catégories) estimée par l'Institut de recherche sur les appareils électroménagers en Chine (CHEARI) à 6,34 millions de tonnes pour 2019, équivalent de 624 millions d'unités.

Source : Direction générale du Trésor ; pour un tableau par pays et des sources détaillées, voir annexe 7

[1] Voir le rapport annuel 2020 du ministère de l'Écologie et de l'Environnement sur la prévention et le contrôle de la pollution par les déchets solides dans les grandes et moyennes villes.

CHAPITRE 7

DES CADRES JURIDIQUES EN CONSTRUCTION

1. En France, un encadrement juridique partiel de l'IdO, qui s'appuie aussi sur la régulation européenne

Il n'existe pas de réglementation spécifique à l'Internet des objets, compte tenu de ses caractéristiques déjà évoquées : diversité des définitions, champ d'application sectorielle très large, variété des techniques et des services, etc. Le cadre juridique applicable aux objets connectés s'étend sur de nombreux champs du droit, notamment les textes qui régissent la protection des données personnelles, la cybersécurité, la consommation et la responsabilité en cas de dommage causé par un objet connecté, les télécommunications, l'environnement, etc. Dès lors, la détermination des responsabilités en cas de produits défectueux ou de dommages provoqués par les objets connectés devient difficile. D'autant plus que les producteurs d'objets connectés ne sont pas toujours propriétaires des logiciels qui y sont intégrés.

Le cadre réglementaire en France permet d'encadrer en partie l'IdO. Il s'appuie aussi sur plusieurs textes au niveau européen qui concernent différents champs (données personnelles, cybersécurité, exigences en matière environnementale, compatibilité et conformité des équipements électroniques, etc.). Malgré la richesse de ce cadre, de nombreuses questions juridiques restent posées. Elles sont liées à la très grande diversité des secteurs de diffusion et des domaines de réglementation de l'IdO (voir Tableau 21, page suivante). Elles tiennent aussi aux spécificités même des objets connectés, qui acquièrent de plus en plus d'autonomie dans leurs interactions avec l'utilisateur ou leur environnement. Enfin, l'absence d'un cadre juridique spécifique à l'Internet des objets ne permet pas toujours aux producteurs comme aux usagers de ces produits et services connectés de disposer d'informations lisibles sur les responsabilités et les exigences en matière de sécurité.

Tableau 21 – La grande variété des domaines de réglementation de l'Internet des objets

Domaines de réglementation	Objectifs
Prestation de services	Définir et spécifier des exigences claires pour la fourniture de services IdO dans un pays (y compris les logiciels, leur mise à jour, leur sécurité, etc.).
Équipement IdO	Décrire les spécifications et les exigences relatives aux équipements IdO et définir les certifications ou les classifications auxquelles ces équipements doivent se conformer.
Réseaux	S'assurer de la disponibilité du spectre et de la numérotation pour les applications IdO et encourager l'adoption d'identifiants uniques pour les objets connectés.
Protection des données et de la vie privée	Protéger la sécurité et la confidentialité des données personnelles des utilisateurs et déterminer comment les données peuvent être traitées.
Cybersécurité	Garantir la sécurité et réduire les vulnérabilités des dispositifs et des systèmes IdO (protéger les données collectées personnelles ou non : mot de passe par défaut, divulgation des vulnérabilités, mises à jour de sécurité, communication sécurisée).
Environnement	Définir des normes environnementales aux différents stades du cycle de vie d'un objet connecté, définir des exigences en matière de recyclage, de traçabilité, etc. Garantir le bon fonctionnement du marché de l'occasion des objets connectés, faire évoluer les exigences en matière d'indice de réparabilité des objets connectés.

Source : France Stratégie et étude BCG et EY-Parthenon

1.1. Différents textes ont vocation à encadrer l'Internet des objets, mais des incertitudes juridiques subsistent

En l'absence de cadre spécifique, les références aux dispositions du droit de la consommation et du droit des contrats pourraient rencontrer des limites

« En droit français, les règles spécifiques à la responsabilité liées aux faits générés par des objets connectés n'existent pas. Aussi, les analyses juridiques renvoient naturellement aux mécanismes existants portant sur les responsabilités contractuelles et extracontractuelles applicables telles qu'elles figurent dans les dispositions des codes de la consommation sur les produits défectueux ou sur la garde de la chose[1]. »

Ainsi **l'obligation d'information précontractuelle de droit commun s'applique aux objets connectés** (art. 1112-1 du code civil). Cette disposition définit des exigences du vendeur professionnel en matière d'information du consommateur. Le droit de la consommation soumet en outre le vendeur professionnel à certaines exigences s'agissant de l'information du consommateur (article 111-1 du code de la consommation). Il s'agit

[1] Cabinet Deroulez (2020), « Quel cadre pour la responsabilité du fait des objets connectés ? », 11 juin.

notamment de certaines informations qui concernent les « caractéristiques essentielles du bien ou du service, ainsi que celles du service numérique ou du contenu numérique, compte tenu de leur nature et du support de communication utilisé, et notamment les fonctionnalités, la compatibilité et l'interopérabilité du bien comportant des éléments numériques, du contenu numérique ou du service numérique, ainsi que l'existence de toute restriction d'installation de logiciel ».

De même, **dans le contexte des contrats d'adhésion, des clauses contractuelles abusives seraient frappées de nullité en application du droit des contrats (article 1171 du code civil).** En effet, toute clause non négociable d'un contrat d'adhésion qui crée un déséquilibre significatif entre les droits et obligations des parties signataires est réputée non écrite. Il en est de même pour les clauses abusives telles qu'elles sont définies par les articles L.212-1 et L.212-2 du code de la consommation qui réputent non écrite toute clause causant un déséquilibre entre les droits et obligations des parties, dans un contrat entre un professionnel et un consommateur (ou non professionnel) au détriment de ce dernier. Par ailleurs, les contrats portant sur des objets connectés ne devraient pas comporter de clauses qui videraient de sa substance l'obligation essentielle du fabricant de ces objets. L'article 1170 du code civil stipule que toute clause qui viderait de sa substance l'obligation essentielle du contrat est réputée écrite (par exemple les clauses restreignant les obligations du professionnel en matière de garantie[1]).

En outre, la question de **la responsabilité du fait des produits défectueux, prévue par l'article 1245 du code civil, s'applique dans le cas d'objets connectés**. Le producteur y est défini « lorsqu'il agit à titre professionnel, le fabricant d'un produit fini, le producteur d'une matière première, le fabricant d'une partie composante » (article 1245-5 du code civil). La responsabilité du fait des produits défectueux s'applique aux dommages causés par les produits défectueux mis en circulation.

Mais le renvoi à ces dispositions peut rencontrer des limites[2]. Les spécificités des objets connectés, notamment ceux, de plus en plus nombreux, qui ont la capacité de prendre des décisions de manière **autonome par rapport à l'intervention humaine**, peuvent remettre en cause leur application. En effet, comment appréhender la licéité du contrat et du consentement des parties dans le cas d'un objet connecté (ou d'un robot connecté) ? Comment définir précisément les responsabilités, y compris pour les objets connectés dont la production fait intervenir plusieurs fabricants de sous-produits physiques et des logiciels ?

[1] Un décret, publié le 20 mars 2009 au *Journal officiel* et intégré aux articles R. 212-1 et R. 212-2 du code de la consommation, donne la liste des clauses abusives. Pour plus d'explications, voir notamment sur le site de la Direction générale de la concurrence, de la consommation et de la répression des fraudes.

[2] Voir notamment les analyses du cabinet Deroulez (www.cabinetderoulez.com).

Par exemple, la défectuosité d'un produit est appréciée notamment au regard de la présentation du produit, des informations sur l'usage raisonnablement attendu et du moment même de mise en circulation[1]. Dans le cas d'objets connectés, l'application de ces dispositions peut s'avérer difficile. Ainsi, le défaut ne peut pas être postérieur à la mise en circulation de l'objet et **le législateur écarte la responsabilité de plein droit du producteur lorsque l'état des connaissances scientifiques et techniques au moment où le produit a été mis en circulation ne permet pas de déceler le défaut du produit par exemple (article 1245-10)**.

Deux directives européennes comblent en partie ces difficultés. Elle s'inscrivent dans le cadre d'une revue de la réglementation européenne pour tenir compte des évolutions technologiques, notamment liées à l'Internet des objets[2].

- **La défectuosité des contenus ou services numériques**. **La directive UE 2019/770 relative aux contrats de fourniture de contenus numériques et de services numériques** a été adoptée le 20 mai 2019, et sera applicable au 1er janvier 2022[3]. Elle procure une protection aux consommateurs de contenus ou services numériques si ces derniers venaient à être défectueux. Elle prévoit un droit d'obtenir réparation en demandant au professionnel de résoudre le problème, et dans le cas contraire ouvre le droit à une réduction de prix voire à une résiliation du contrat. Cette possibilité n'existait jusqu'ici au niveau européen que pour les biens matériels. En outre, **le consommateur peut faire valoir ce droit qu'il ait payé ou échangé ce service contre la fourniture de données personnelles**. Les objets connectés sont donc aussi concernés par cette directive qui offre une protection supplémentaire aux consommateurs européens. La définition des services et contenus visés par cette directive peut toutefois conduire à de réelles difficultés d'articulation avec la directive 2019/771/UE concernant les contrats de vente de bien dès lors que bon nombre d'entre eux comportent désormais des éléments numérique[4].

[1] L'article 1245-3 al. 1 du code civil énonce qu'un produit est considéré comme défectueux « lorsqu'il n'offre pas la sécurité à laquelle on peut légitimement s'attendre ».

[2] Commission européenne (2020), *Rapport sur les conséquences de l'intelligence artificielle, de l'Internet des objets et de la robotique sur la sécurité et la responsabilité*, rapport de la Commission au Parlement, au Conseil et au Comité économique et social européen, COM(2020) 64 final, 19 février.

[3] La directive UE 2019/771 abroge et remplace la directive 1999/44/CE (directive relative aux garanties des produits pour les consommateurs ou DGPC) à partir du 1er janvier 2022.

[4] Pour une analyse approfondie voir notamment Zolynski C. (2019), « Contrats de fourniture de contenus et de services numériques : à propos de la directive UE 2019/770/UE du 20 mai 2019 », *La semaine juridique – édition générale*, n° 47, 25 novembre, p. 2062-2065 et Aubert de Vincelles C. (2019), « Nouvelle directive sur la conformité dans la vente entre professionnel et consommateur : propos de la directive 2019/771/UE du 20 mai 2019 », *La semaine juridique – édition générale*, n° 28, 15 juillet, p. 1338-1342.

- **La directive UE 2019/771 relative à certains aspects concernant les contrats de vente de biens** fixe certaines règles communes sur les contrats de vente entre les vendeurs et les consommateurs, qui couvrent la conformité des biens avec le contrat, les recours en cas de défaut de conformité, les modalités d'exercice de ces recours, les garanties commerciales. **La législation s'applique à « la fourniture de contenus numériques ou de services numériques si ces derniers sont intégrés ou interconnectés avec les biens eux-mêmes, ce qui leur est nécessaire pour remplir leurs fonctions et prévus par le contrat de vente (biens comportant des éléments numériques) »**[1]. Les vendeurs doivent veiller à ce que les biens livrés au consommateur soient conformes au contrat de vente. En outre, la responsabilité des vendeurs est engagée pour tout défaut de conformité qui apparaît dans un délai de deux ans à compter de la livraison. Les vendeurs doivent respecter les dispositions contractuelles (notamment correspondre à la description, au type, à la quantité et à la qualité et présenter les caractéristiques requises par le contrat, être adapté aux finalités convenues, etc.) et les critères de conformité objectifs (être adapté aux finalités auxquelles serviraient normalement des biens de même type, « être livré avec tous les accessoires, toutes les instructions et l'emballage que le consommateur peut raisonnablement s'attendre à recevoir, présenter les qualités et les caractéristiques que le consommateur peut raisonnablement s'attendre à recevoir »[2]). Si les biens sont défectueux (« défaut de conformité »), les consommateurs disposeront d'une variété de voies de recours comme « le choix entre la réparation ou le remplacement des biens, sans frais, dans un délai raisonnable et sans aucun inconvénient majeur. Le vendeur peut proposer une autre solution si la solution choisie est impossible ou lui impose des coûts disproportionnés ; une réduction proportionnelle du prix, ou enfin la résiliation du contrat, sauf si le défaut n'est que mineur ». **Concernant spécifiquement les biens comportant des éléments numériques**, la Directive indique que :
  - « **Les vendeurs doivent informer le consommateur de toutes les mises à jour nécessaires au maintien de la conformité de ces bien**s et les lui fournir pendant une période qui est celle à laquelle le consommateur peut raisonnablement s'attendre, sauf si l'élément numérique des biens est fourni de manière continue, auquel cas des mises à jour devraient être fournies tout au long de la période de fourniture ;
  - **La responsabilité des vendeurs est engagée pour tout défaut de conformité qui apparaît dans un délai de deux ans à compter de la livraison**, sauf si

[1] Mais ne s'applique pas à tout support matériel utilisé exclusivement pour transporter le contenu numérique (par exemple les CD, les DVD, etc.).

[2] Commission européenne (2019a), « Règles relatives aux contrats de vente de biens entre les vendeurs et les consommateurs », synthèse de la directive UE 2019/771 relative à certains aspects concernant les contrats de vente de biens.

l'élément numérique doit être fourni de manière continue pendant une période plus longue, auquel cas leur responsabilité est engagée tout au long de la période de fourniture. »

La mise en circulation sur le marché d'objets connectés est régie aussi par l'obligation de conformité avec d'autres textes

- ***La traçabilité***, qui permet de suivre et donc d'identifier un produit ou un service depuis sa création jusqu'à sa destruction, est définie notamment par la norme internationale ISO 8402. D'autres normes européennes définissent des exigences de traçabilité des produits par secteurs d'activité[1] (voir également l'Acte délégué réformant la directive sur les équipements radioélectriques, RED).

- ***La norme et le marquage CE***. De nombreux produits, notamment les équipements électriques et électroniques (EEE) doivent porter la référence à la norme CE avant leur mise en circulation sur le marché. L'Union européenne a défini les conditions de mise sur le marché de ces équipements avec marquage CE dans le cadre de la **directive sur les équipements radioélectriques, RED** (mise sur le marché des équipements radioélectriques, couvrant les appareils Wifi, Bluetooth, 3G, LTE et 5G) et de la **directive sur la compatibilité électromagnétique, CEM**. Les obligations aux fabricants, aux importateurs et aux distributeurs des équipements électriques et électroniques tels que des ordinateurs, des réfrigérateurs ou des téléphones mobiles sont : enregistrement auprès des autorités nationales compétentes dans chaque pays où sont vendus ou distribués les équipements[2] ; soumission d'un rapport sur la quantité d'équipements électriques et électroniques vendus ; organisation ou financement de la collecte, du traitement, du recyclage et de la valorisation des produits. En tant que distributeur, s'y ajoute l'offre d'un service de reprise permettant aux clients de rapporter gratuitement leurs déchets d'équipements électriques et électroniques ; en tant que fabricant, le respect des dispositions de la directive relative à la limitation de l'utilisation de certaines substances dangereuses. La **directive RED** a fait l'objet de modifications significatives en octobre 2021 avec la publication d'un Acte délégué de la Commission européenne qui la réforme en renforçant notamment la dimension cybersécurité des dispositifs sans fil disponibles sur le marché européen et qui couvre les objets connectés (voir *infra*).

[1] Voir la page « Traçabilité » sur le site de la DGCCRF.

[2] Article 7 de la directive CEM (et Article R.20-12 du code des postes et des communications électroniques) : « les appareils (…) mis sur le marché portent un numéro de type, de lot ou de série, ou un autre élément permettant leur identification ». Cette identification doit apparaître dans la déclaration de conformité et sur l'appareil.

- ***La conformité en matière de niveaux d'utilisation de certaines substances chimiques***. Les produits électroniques vendus dans l'Union européenne, notamment les objets connectés, qui comprennent des substances dangereuses dont la plupart sont des métaux lourds, doivent également être conformes à la **directive RoHS** (**Restriction of Hazardous Substances**)**,** entrée en vigueur en novembre 2017, et les fabricants concernés doivent également obtenir le marquage CE spécifique pour les substances dangereuses.

La réglementation en matière environnementale comporte des textes qui encadrent, mais de manière incomplète, les phases de conception et de fin de cycle de vie des produits connectés

- La **directive 2009/125/CE (21 octobre 2009, renforcée en 2012) établit un cadre pour la fixation d'exigences en matière d'écoconception applicables aux produits liés à l'énergie**. Ce cadre porte sur les différentes phases qui concernent les matières premières utilisées, la fabrication, le conditionnement, la distribution et l'installation, l'entretien, l'utilisation et la fin de vie du produit. De plus, les fabricants ont l'obligation d'établir le profil écologique de leurs produits et de rechercher des possibilités de conception alternatives.

- La **directive européenne relative aux déchets d'équipements électriques et électroniques, DEEE**, entrée en vigueur en février 2014, impose l'étiquetage de ces produits pour les identifier sur le marché. Elle concerne spécifiquement le recyclage des déchets. Elle a été transposée en France par le décret 2014-928 (modifiant les articles du code de l'environnement).

- Par ailleurs, **la loi n° 2020-105 du 10 février 2020 relative à la lutte contre le gaspillage et à l'économie circulaire** a modifié le code de l'environnement afin d'établir des filières spécialisées par thématique de produits, responsables du recyclage et de la gestion de fin de vie de certains produits. L'intégration de composants électroniques dans des produits existants qui n'en comportaient pas auparavant pose aujourd'hui des difficultés à plusieurs filières de recyclage (voir la section sur les enjeux environnementaux).

- **Le code de l'environnement,** depuis le 15 novembre 2006, réglemente la filière de recyclage et d'élimination des déchets d'équipements électriques et électroniques. Les articles L. 541-10-20 et R. 543-172 à R. 543-206 définissent la responsabilité des entreprises en tant que producteur de déchets et, pour certains équipements

électriques et électroniques, un régime de responsabilité élargie du producteur dans la gestion des déchets des produits en fin de vie (principe du pollueur-payeur)[1].

Les spécificités des objets connectés nécessiteraient des adaptations en matière d'exigence et d'organisation des filières de traitement des déchets liés aux dispositifs d'objets connectés.

1.2. Au niveau européen : différentes familles de textes réglementaires

Sept directives présentées précédemment (RED, directive CEM, ROSH, DEEE, directive sur l'écoconception, directive contrats de fourniture de services et de contenus numériques, et directive relative à certains aspects concernant les contrats de vente de biens) encadrent les questions liées à la compatibilité, la conformité et l'environnement. D'autres textes au niveau européen définissent, d'une part, un cadre juridique concernant les données personnelles et non personnelles, d'autre part, viennent renforcer les exigences en matière de cybersécurité. En outre, des textes spécifiques ciblent certains secteurs comme la santé et le transport ou l'efficacité énergétique des bâtiments.

Le cadre juridique des données personnelles et non personnelles

Deux règlements ainsi qu'un code des communications électroniques européennes concernent spécifiquement la question des données personnelles et non personnelles :

- **Le règlement général sur la protection des données personnelles (RGPD).** Il s'agit du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Ce règlement européen s'inscrit dans la continuité de la loi française Informatique et Libertés de 1978. Il renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant. Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. En effet, l'Internet des objets présente certains risques pour les personnes concernées : manque de contrôle sur les données, asymétrie de l'information, validité du consentement, ciblage marketing ou pour d'autres usages, non-respect du principe de minimisation des données, traitement pour d'autres

[1] L'ensemble des producteurs devrait avoir un identifiant unique ou IDU. Pour l'Ademe, il facilite le suivi et le contrôle du respect des obligations qui incombent à ces producteurs. Par ailleurs, l'IDU doit figurer dans les conditions générales de vente et être communiqué à la demande de l'acheteur. En outre, les exploitants des établissements qui produisent ou expédient des déchets doivent tenir à jour un registre où sont consignés tous les déchets sortants (bordereau de déchet). Ce document est obligatoire pour toute entreprise. Il permet d'assurer de manière chronologique la traçabilité des déchets sortant de l'entreprise.

finalités, etc. Les fabricants d'objets connectés sont donc tenus de respecter ce règlement dès la conception du produit. En outre, les données personnelles recueillies, stockées ou traitées par les objets connectés sont donc régis par ce règlement. Bien que la RGPD concerne l'IdO, les objets connectés peuvent soulever des questions d'interprétation et pourraient nécessiter des précisions à apporter aux textes juridiques pour mieux les sécuriser.

- **Le règlement sur le libre flux des données à caractère non personnel dans l'Union européenne** (*Regulation on the free flow of non-personal data*), adopté et applicable depuis le 28 mai 2019. Ce règlement s'inscrit dans le cadre de la stratégie de l'Union européenne en matière de gouvernance des données, notamment en faveur de la réutilisation de données non personnelles pour le développement de l'IA. Il garantit la libre circulation des données non personnelles entre les États membres et les systèmes informatiques dans l'UE. Il supprime également les exigences de localisation des données imposées par les États et facilite le changement de fournisseur de services pour les utilisateurs. Il pourrait donc concerner notamment les données de santé et de mobilité recueillies via des dispositifs d'objets connectés.

Le code européen des communications électroniques

Tout d'abord, ce code contraint les acteurs dits de « HOFAI[1] » (*Over the top*, OTT, qui permet de transporter des flux vidéo, audio ou de données sur Internet sans l'intervention nécessaire d'un opérateur) à se conformer à des obligations de sécurité des réseaux ou encore d'interopérabilité. En ce qui concerne la protection des consommateurs, le code prévoit notamment **l'interdiction des écoutes et autres enregistrements des communications et données de trafic sans le consentement préalable des utilisateurs**. Les messageries qui seraient proposées sur les dispositifs d'objets connectés sont donc concernées. Ces opérateurs doivent également limiter l'utilisation de données de trafic et de localisation de l'expéditeur ou du destinataire, notamment pour proposer des publicités ciblées. Si cette directive cible explicitement les OTT, elle peut concerner aussi indirectement les fabricants de dispositifs et d'objets connectés.

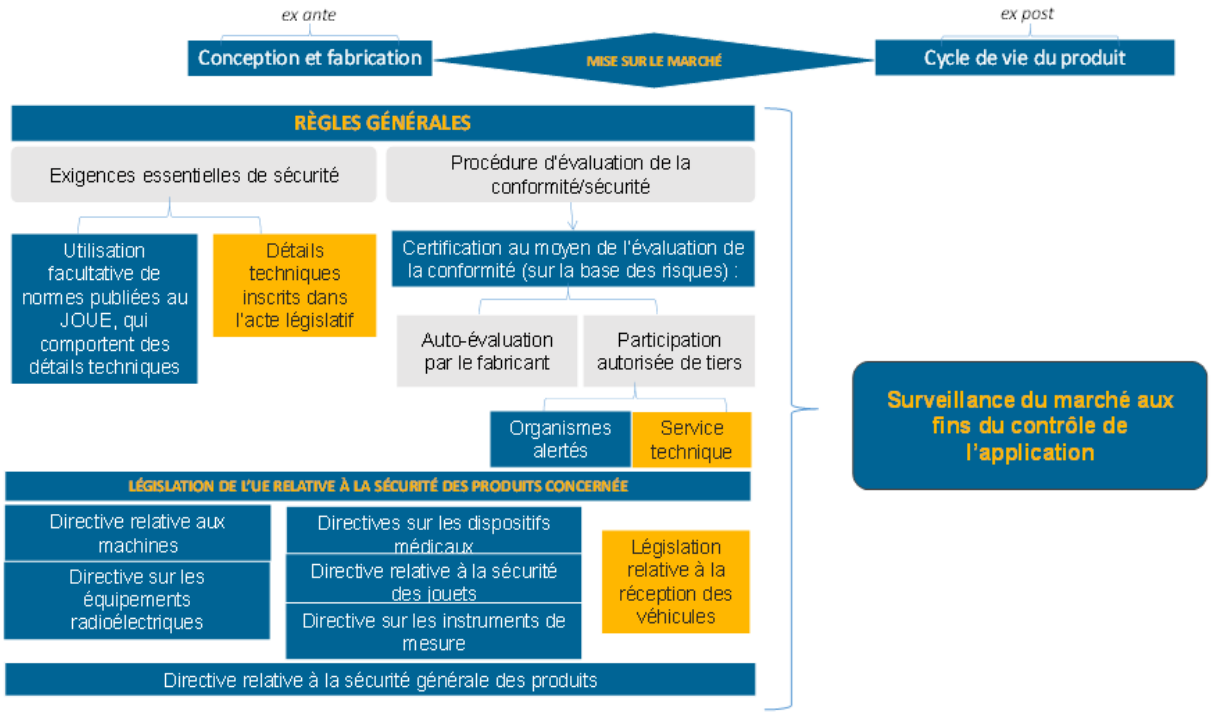
Les textes sur la cybersécurité s'appliquent aussi à l'IdO

Comme le rappelle le rapport de la Commission européenne sur les conséquences de l'intelligence artificielle, de l'Internet des objets et de la robotique sur la sécurité et la responsabilité, « la fixation de niveaux élevés de sécurité pour les produits et les systèmes intégrant les nouvelles technologies numériques et la mise en place de mécanismes solides permettant de remédier aux dommages (c'est-à-dire le cadre en matière de

[1] Hors offre du fournisseur d'accès à l'Internet.

responsabilité) contribuent à une meilleure protection des consommateurs »[1]. Le cadre réglementaire dont dispose l'Union européenne (voir Graphique 35) est complété par de nouvelles normes pour accroître sa robustesse et sa fiabilité en matière de sécurité et de responsabilité (voir notamment la question de la responsabilité du fait des produits dans les paragraphes précédents). Ces normes européennes sont complétées par des législations nationales, non harmonisées, en matière de responsabilité (voir paragraphe sur les textes en France).

Graphique 35 – Logique sous-tendant la législation de l'UE relative à la sécurité des produits



Note du rapport : « Ce schéma n'inclut pas les exigences législatives relatives au cycle de vie des produits, à savoir l'utilisation et la maintenance, et n'est présenté qu'à titre d'exemple général. »

Source : Commission européenne (2020), Rapport sur les conséquences de l'intelligence artificielle, de l'Internet des objets et de la robotique sur la sécurité et la responsabilité*,* op. cit.*, p. 6*

Dans le domaine de la cybersécurité, trois principaux textes s'appliquent dans ce domaine. Il s'agit des deux directives (Network and Information Security Directive, NIS et Cybersecurity Act), d'un Acte délégué de la Commission réformant la directive RED ainsi

[1] Commission européenne (2020), *Rapport sur les conséquences de l'intelligence artificielle, de l'Internet des objets et de la robotique sur la sécurité et la responsabilité*, rapport de la Commission au Parlement, au Conseil et au Comité économique et social européen, COM(2020) 64 final, 19 février.

que de deux normes (EN 303 645 et TS 103 701) régissant les règles, harmonisées au niveau européen, et imposant les exigences en matière de cybersécurité.

- **La directive « Network and Information Security Directive » (NIS)** de mai 2018 : les mesures juridiques qui y sont consacrées ont pour objectif de renforcer le niveau général de cybersécurité dans l'UE via des mesures de coopération et de supervision. Elle comprend notamment quatre axes : a) le renforcement des capacités nationales de cybersécurité (en France, l'agence ANSSI), b) l'établissement d'un cadre de coopération entre États membres ; c) le renforcement de la cybersécurité d'opérateurs de services essentiels ; d) l'instauration de règles européennes de cybersécurité des fournisseurs de services numériques.

- **Le Cybersecurity Act**[1] : ce règlement, entré en application le 27 juin 2019, vise à renforcer la sécurité des services en ligne et des appareils de consommation sur le marché unique numérique européen. Il définit notamment un cadre pour harmoniser les méthodes d'évaluation et les législations fragmentées en matière de cybersécurité entre les États membres. Par ailleurs, il mandate l'ENISA pour proposer un ensemble commun de normes de certification pour classifier les entreprises IdO en fonction de leur degré de sécurité selon trois niveaux (basique, substantiel, élevé) :
  - le niveau basique qui cible en particulier les produits grand public, non critiques et donc intégrant une grande partie des dispositifs et d'objets connectés ;
  - le niveau substantiel qui concerne les produits présentant un risque moyen, comme pour les « cloud » ;
  - le niveau élevé qui vise les produits ou solutions pour lesquelles les risques d'attaques par acteurs dotés de grandes compétences et des ressources significatives sont élevés.

- **L'Acte délégué relatif à la réforme de la directive RED sur les équipements radioélectriques**[2] **:** la Commission européenne vient de renforcer **la cybersécurité des dispositifs et des produits sans fil disponibles sur le marché européen**. Elle a adopté le 29 octobre 2021 un Acte délégué qui réforme la directive RED. Il doit entrer en application en janvier 2022[3], mais donne un délai de 30 mois aux fabricants pour se mettre en conformité (soit jusqu'en juin 2024). La Commission a motivé ce texte par

[1] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité).

[2] Commission européenne (s.d.), page « Radio Equipment Directive (RED) ».

[3] Si le Conseil et le Parlement ne formulent pas d'objections.

les cybermenaces qui représentent un risque croissant pour tous les consommateurs du fait de l'utilisation de différents produits sans fil, incluant donc l'IdO. Plus précisément, comme le rappelle la Commission, cet acte fixe de nouvelles exigences juridiques relatives :

– *aux garanties en matière de cybersécurité*, dont les fabricants devront tenir compte lors de la conception et de la fabrication des produits concernés. Ainsi, les dispositifs et produits sans fil devront intégrer des fonctionnalités pour éviter qu'ils ne nuisent aux réseaux de communication et empêcher qu'ils ne soient utilisés pour perturber le bon fonctionnement d'un site web ou d'autres services ;

– *à la protection des données personnelles* : les dispositifs et produits sans fil devront être dotés de fonctionnalités qui garantissent la protection des données à caractère personnel et la protection des droits de l'enfant deviendra un élément essentiel de cette législation ;

– *la protection contre le risque de fraude monétaire* **:** les dispositifs et produits sans fil devront comporter des fonctionnalités permettant de réduire au minimum le risque de fraude lors des paiements électroniques (par exemple, un meilleur contrôle d'authentification de l'utilisateur).

D'autres textes concernent l'IdO dans des domaines spécifiques

Sans viser l'exhaustivité, on peut citer ici trois textes dans le domaine du transport, deux sur les performances énergétiques et un dernier dans le domaine de la santé :

- **Deux directives sur la performance et l'efficacité énergétique[1] : la directive de 2010 sur la performance énergétique des bâtiments** (Directive 2010/31/EU on the Energy Performance of Buildings) a pour objectif global la performance énergétique de l'immobilier européen et se fixe au plus tard l'année 2050 pour disposer d'un parc immobilier à haute efficacité énergétique et décarboné. Pour atteindre cet objectif, la directive s'appuie explicitement sur le déploiement de l'IdO. On peut citer également **la directive de 2012 sur l'efficacité énergétique (**Energy Efficiency Directive 2012/27/EU)**.**
- **La directive « Intelligent Transport Systems Directive** », de 2012 : elle consacre l'application du régime des produits défectueux à tout dispositif et objet connecté dans le domaine du transport (voir paragraphe précédent sur le cadre juridique de la France).
- **Le règlement concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence européenne pour la sécurité aérienne (EU Basic**

[1] Commission européenne (2012a), « Directive 2012/27/EU du Parlement européen et du Conseil du 25 octobre 2012 relative à l'efficacité énergétique », *Journal officiel de l'Union européenne*, 14 novembre.

Regulation for Drones). Ce règlement, applicable depuis 1er juillet 2020, distingue trois catégories de drones et encadre les données collectées et traitées par les drones. Il s'agit de la catégorie dite « ouverte » pour les drones à faible risque (jusqu'à 25 kg), la catégorie « spécifique » pour ceux autorisés à voler et la catégorie « certifiée » pour les drones exploités notamment pour la livraison ou les passagers, ainsi que le survol de grandes masses de personnes. Cette réglementation est applicable depuis le 31 décembre 2020.

- **Le règlement eCall Regulation** : ce règlement rend obligatoire le système *eCall* pour tout véhicule de l'Union européenne dont la fabrication a été approuvée après le 31 mars 2018. Il permet d'appeler automatiquement et gratuitement le 112 en cas d'accident grave de la route.
- **Le règlement relatif aux dispositifs médicaux « Medical Device Regulation »** : ce règlement crée un cadre juridique et opérationnel pour assurer une coexistence sûre des dispositifs médicaux dans un environnement d'IdO. Des conseils publiés en appui au règlement soulignent la nécessité d'informer les patients et les consommateurs sur les dernières versions du logiciel, la protection de l'appareil pendant toute sa durée de vie, l'utilisation de mots de passe suffisamment complexes, la désactivation de fonctionnalités non utilisées, la sécurisation des appareils comme les ordinateurs ou les tablettes, la sauvegarde et la protection des données de santé.

1.3. Des réglementations en cours de préparation au niveau européen concerneraient directement ou s'appliqueraient à l'IdO

Sans viser ici l'exhaustivité, on peut citer ici le projet de règlement sur l'IA, le projet de règlement réformant la directive sur la sécurité globale des produits (GSPD) et les travaux de la Commission sur les ententes et les abus de position dominante sur le marché de l'Internet des objets.

Proposition d'un règlement établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'UE

Après des travaux menés par la Commission (notamment le livre blanc sur l'IA[1]), le Parlement (de nombreuses résolutions adoptées) et le Conseil, la Commission a présenté une stratégie en matière d'IA[2] qui comporte une proposition datée du 21 avril 2021 de

[1] Commission européenne (2020), *Intelligence artificielle. Une approche européenne axée sur l'excellence et la confiance*, COM(2020) 65 final, Livre blanc, 19 février.

[2] Voir CNIL (2021), « Intelligence artificielle : avis de la CNIL et de ses homologues sur le futur règlement européen », Commission nationale de l'informatique et des libertés, 8 juillet.

règlement régissant l'IA en Europe. Ce projet concernera aussi l'IdO. Comme le souligne l'exposé des motifs[1] de la proposition, « le cadre réglementaire relatif à l'IA dont les objectifs spécifiques sont les suivants :

- veiller à ce que les systèmes d'IA mis sur le marché de l'Union et utilisés soient sûrs et respectent la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union ;
- garantir la sécurité juridique pour faciliter les investissements et l'innovation dans le domaine de l'IA ;
- renforcer la gouvernance et l'application effective de la législation existante en matière de droits fondamentaux et des exigences de sécurité applicables aux systèmes d'IA ;
- faciliter le développement d'un marché unique pour des applications d'IA légales, sûres et dignes de confiance, et empêcher la fragmentation du marché. »

La **directive sur la sécurité globale des produits (GSPD)** a fait l'objet le 21 juin 2021 d'une proposition de règlement[2] modifiant celui de 2012 (UE n° 1025/2012, et abrogeant la directive GSPD 87/357/CEE de 2001). Comme le souligne l'étude d'impact, ce projet répond au constat selon lequel « l'apparition de certains nouveaux risques liés à la connectivité, l'applicabilité de la directive aux mises à jour et aux téléchargements de logiciels ainsi que l'évolution des fonctionnalités des produits intégrant l'IA soulèvent la question de savoir si la DSGP est suffisamment claire pour offrir une sécurité juridique aux entreprises et protéger le consommateur ». En effet, les travaux menés en amont, notamment ceux publiés dans l'avis de décembre 2020 du sous-groupe sur l'intelligence artificielle, les produits connectés et autres nouveaux défis en matière de sécurité des produits du réseau pour la sécurité des consommateurs, concluent que les textes actuels ne permettent pas de garantir la couverture de ces risques[3].

Ce projet de règlement, s'il est adopté, apportera des modifications substantielles dans le champ de l'IdO. Cinq points peuvent être soulignés :

- **La définition d'un « produit » intégrerait désormais l'IdO** : l'article 3 du projet de règlement définit ainsi un produit comme « tout élément, interconnecté ou non avec

[1] Commission européenne (2021b), *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union*, 21 avril.

[2] 2021/0170 (COD), Projet de règlement relatif à la sécurité générale des produits, modifiant le règlement (UE) n° 1025/2012 du Parlement européen et du Conseil et abrogeant la directive 87/357/CEE du Conseil et la directive 2001/95/CE du Parlement européen et du Conseil.

[3] https://ec.europa.eu/safety/consumers/consumers_safety_gate/home/documents/Subgroup_opinion_final_format.pdf

d'autres éléments, fourni ou mis à disposition, à titre onéreux ou gratuit, dans le cadre d'une activité commerciale – y compris dans le cadre de la prestation d'un service –, qui est destiné aux consommateurs ou qui peut, dans des conditions raisonnablement prévisibles, être utilisé par les consommateurs même s'il ne leur est pas destiné » ;

- **Le filet de sécurité intègre aussi les risques liés à l'IdO** : la proposition de règlement inclut les nouvelles technologies et les risques qui leur sont liés afin de garantir que ces risques relèvent du champ d'application du filet de sécurité. Elle complète les dispositions prévues pour les risques liés à l'IA.
- **La cybersécurité est prise en compte parmi les exigences pour considérer un produit comme « sûr »**.
  - Le projet de règlement précise que les risques liés à la cybersécurité qui ont une incidence sur la sécurité des consommateurs sont couverts par la notion de sécurité des produits (telle qu'elle est définie dans la proposition de règlement). **Ce projet complète ainsi le règlement sur la cybersécurité de 2019**. En effet, **si ce dernier introduit, à l'échelle de l'UE, un cadre de certification de cybersécurité pour les produits, services et processus TIC, il ne prévoit pas d'exigences légales minimales en matière de cybersécurité pour les produits TIC**.
  - **Le projet complète également la directive NIS** : en effet, cette directive crée des obligations pour tous les États membres en ce qui concerne l'adoption d'une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, en vue de renforcer la cybersécurité dans l'ensemble de l'UE. Or, cette directive ne prévoit pas d'exigences minimales en matière de cybersécurité pour les produits de consommation. L'objectif du projet de règlement est de combler cette lacune en fournissant une base juridique qui permet aux autorités publiques de prendre des mesures contre les produits présentant de tels risques.
- **La sûreté d'un produit est liée aux normes européennes et, en l'absence de celles-ci, par les législations nationales**[1]. Selon l'article 5, les opérateurs économiques mettent sur le marché de l'Union uniquement des produits sûrs. Le projet énonce qu'**un produit est présumé conforme à l'obligation générale de sécurité dans les cas suivants** :
  - s'il est conforme aux normes européennes pertinentes (dont les références ont été publiées au *Journal officiel de l'Union européenne* conformément à l'article 10,

[1] Le projet prévoit que la « sécurité des produits devrait être évaluée en tenant compte (…) des besoins et des risques spécifiques des catégories de consommateurs susceptibles d'utiliser les produits, en particulier les enfants, les personnes âgées et les personnes handicapées ».

paragraphe 7, du règlement UE n° 1025/2012, ou aux parties pertinentes de celles-ci, en ce qui concerne les risques et les catégories de risques couverts) ;

– en l'absence de normes européennes, telles que visées au point précédent, s'il est conforme aux exigences nationales en matière de santé et de sécurité prévues par la législation de l'État membre où le produit est mis à disposition sur le marché.

- Si les dispositions prévues par cet article 5 ne s'appliquent pas, le projet énonce qu'il convient de tenir compte de **plusieurs éléments pour évaluer si un produit est sûr, dont trois critères concerneraient les produits intégrant des dispositifs IdO**[1] :

  – l'effet du produit sur d'autres produits dans les cas où on peut raisonnablement prévoir l'utilisation du premier avec les seconds, y compris l'interconnexion des produits ;

  – les caractéristiques de cybersécurité appropriées nécessaires pour protéger le produit contre les influences extérieures, y compris les tiers malveillants, lorsqu'une telle influence peut avoir une incidence sur la sécurité du produit ;

  – les fonctionnalités évolutives, d'apprentissage et prédictives d'un produit.

Par ailleurs**, en matière de droit de la concurrence, on peut citer les travaux récents de la Commission européenne qui se sont traduits par une enquête sectorielle sur l'IdO** dont les premières conclusions ont été publiées le 9 juin 2021. Si le rapport souligne la croissance rapide de ces marchés liés à l'IdO, il met en lumière aussi les préoccupations exprimées par les personnes interrogées dans le cadre de l'enquête sectorielle. Cette enquête intègre différents objets connectés, en particulier les assistants virtuels[2].

Enfin, en parallèle de ces réglementations, de nombreux organismes et organisations professionnelles publient des recommandations (CNIL et ANSSI par exemple en France, ENISA en Europe, etc.) ou proposent des certifications (au niveau européen ou international comme l'ETSI, ISO, IoXT, CTIA, Eurosmart, etc.)[3].

L'analyse du cadre réglementaire susceptible d'affecter le développement et l'usage de l'IdO ne prétend pas être exhaustive. Seuls les principaux registres réglementaires,

[1] Dans le respect du plan d'action pour une économie circulaire, ce projet énonce « qu'il convient de privilégier la mesure la plus durable, c'est-à-dire celle qui a le moins de répercussions sur l'environnement, à condition qu'elle n'entraîne pas une baisse du niveau de sécurité ».

[2] Selon la terminologie de la Commission européenne.

[3] Pour une présentation exhaustive des organismes et des types de certifications, voir notamment les travaux publiés par l'ETSI (European Telecommunications Standards Institute) dans le rapport ETSI (2016), *SmartM2M. IoT Standards Landscape and Future Evolutions*, rapport technique, European Telecommunications Standards Institute.

susceptibles d'affecter l'IdO de façon transversale, dans ses multiples registres de déploiement sont évoqués (comme produit, comme réseau, etc.).

Des pans de réglementation plus spécifiques peuvent aussi l'affecter de façon indirecte. Il en va ainsi par exemple de la réglementation relative à la santé et à la sécurité au travail, qui pourrait encadrer le déploiement et surtout les usages d'objets connectés sur les lieux de travail au même titre que d'autres technologies. La directive-cadre européenne 89/391 sur la santé et la sécurité au travail du 12 juin 1989 a été déclinée depuis en une vingtaine de directives thématiques, dont certaines portent sur les lieux de travail (89/654), les équipements de travail (89/655), les équipements de protection individuels (89/656) ou les équipements à écran de visualisation (90/270). Ce cadre européen trouve une transcription plus détaillée dans le droit français au travers du code du travail. Cette législation, dans son état actuel, constitue un cadre général définissant notamment la responsabilité des employeurs dans la prévention de risque pour les travailleurs en lien avec leur équipement de travail (machines et équipements de protection personnels), leur environnement (exposition à des polluants, etc.) ou leur lieu de travail. Cette réglementation est pour partie assez « ancienne » puisque remontant aux années 1990, avant le déploiement massif d'Internet, des réseaux sociaux et aujourd'hui de l'IdO et de l'IA. Elle ne s'adresse pas spécifiquement à ces technologies numériques et n'a que peu évolué à cet égard, exception faite en matière d'exposition aux risques pour la santé et la sécurité résultant ou susceptibles de résulter d'une exposition à des champs électromagnétiques. La directive de 2004 revue en 2013[1] est ainsi déclinée en France par le décret n° 2016-1074 du 3 août 2016 relatif à la protection des travailleurs contre les risques dus aux champs électromagnétiques[2]. Ce décret définit les règles de prévention contre les risques biophysiques directs des ondes et leurs effets indirects connus. Il prévoit une approche graduée des moyens de prévention et du dialogue interne à mettre en œuvre en cas de dépassement des « valeurs d'action » et des « valeurs limites ». Cette réglementation prend sens au regard de l'IdO qui induit – notamment dans l'industrie 4.0 où la 5G offre de

[1] Une directive européenne particulière a été édictée en 2013 (2013/35/UE) pour fixer les prescriptions minimales de sécurité et de santé relatives à l'exposition des travailleurs aux risques dus aux agents physiques (champs électromagnétiques) (vingtième directive particulière au sens de l'article 16, paragraphe 1, de la directive 89/391/CEE). Cette directive a abrogé celle initialement éditée en 2004 (2004/40/CE). Les dispositions du code du travail modifiées par le présent décret peuvent être consultées, dans leur rédaction résultant de cette modification, sur le site de Légifrance.

[2] Abstraction faite des réformes du code du travail qui depuis 2016 ont introduit le droit à la déconnexion, facilité le télétravail et commencé à encadrer l'emploi sur les plateformes de mise en relation, dans la livraison ou le transport. Mais ces modifications, liées à des enjeux de numérisation de l'économie, ne sont pas nécessairement en lien direct avec l'IdO et visent des enjeux de protection sociale, de relations contractuelles, de contrôle du temps de travail ou de conciliations vie privée/vie professionnelle.

nombreuses perspectives – l'augmentation des ondes magnétiques pour la transmission de données à distance toujours plus nombreuses.

Depuis quelques années, la dimension numérique des conditions de travail fait par ailleurs l'objet d'une attention croissante. L'UE a ainsi ouvert en 2021 une proposition de réglementation sur l'intelligence artificielle et, dans le cadre de son plan stratégique en matière de santé et sécurité au travail pour la période 2021-2027, elle prévoit de « moderniser le cadre législatif en matière de SST en rapport avec la numérisation par une révision de la directive sur les lieux de travail et de la directive relative aux équipements à écran de visualisation d'ici 2023 ».

À noter que cette réglementation porte essentiellement sur les relations de travail salarié, laissant de plus en plus ouverte, avec le développement de formes d'emplois hybrides ou indépendantes liées aux plateformes numériques d'intermédiation, la question de la responsabilité des donneurs d'ordre ou intermédiaires en matière de santé et sécurité, mais aussi d'utilisation des données collectées via et sur les travailleurs.

Si les objets connectés soulèvent des enjeux de protection des consommateurs[1] et de responsabilité du fait des produits, ils posent aussi de nombreuses questions sur la protection des données personnelles et non personnelles et sur la sécurité. Favoriser une meilleure lisibilité et donc une meilleure application de ce cadre juridique très fragmenté et envisager des enrichissements éventuels, c'est le sens des recommandations n° 3, 13, 26, 27, 29 et 30.

N° 3 – Faciliter la connaissance des réglementations.

N° 13 – Adapter le cadre réglementaire actuel pour un bon niveau de protection des personnes vulnérables.

N° 26 – Procéder aux analyses juridiques permettant notamment de définir l'échelle des responsabilités sur la chaîne des usages.

N° 27 – Analyser l'opportunité d'une loi cyber globale.

N° 29 – Cartographier les compétences respectives des régulateurs publics dans le champ de l'IdO.

N° 30 – Procéder pour l'IdO à une analyse juridique fondée sur une approche d'analyse des risques.

[1] Il existe un système européen d'échange rapide d'informations sur les dangers découlant de l'utilisation des produits de consommation, nommé RAPEX. En France, la DGCCRF a par exemple alerté sur les risques en matière de montres connectées pour enfants (notice RAPEX en 2019).

2. Aux États-Unis, en l'absence d'un cadre juridique fédéral, certains États sont à l'initiative

Au niveau fédéral, il n'existe pas aujourd'hui aux États-Unis de cadre général et structuré de la réglementation de l'IdO. Toutefois, compte tenu des enjeux qui lui sont liés, différents textes législatifs et réglementaires ont été adoptés et d'autres sont au stade de projets. Les textes traduisent, en partie, une vision stratégique construite de développement de ce secteur tout en tenant compte de questions clés telles que la cybersécurité.

2.1. Une réglementation favorable pour une vision stratégique

Un soutien à l'IdO avec l'objectif d'être le leader mondial du secteur

Dès 2015, le Sénat américain a adopté à l'unanimité une résolution appelant à une **stratégie nationale pour le développement de l'Internet des objets**[1]. En 2017, la National Telecommunications and Information Administration du Département du Commerce a produit un livre vert pour le développement de l'IdO[2]. Ce ministère y a défini quatre principes, déclinés en propositions d'actions :

- **Veiller à ce que l'IdO soit inclusif et largement accessible aux consommateurs, aux travailleurs et aux entreprises** ; notamment permettre la disponibilité et l'accès à l'infrastructure et au spectre nécessaires pour soutenir la croissance et l'avancement de ces technologies ;
- **soutenir un environnement IdO stable, sécurisé et digne de confiance** : notamment éliminer les obstacles et encourager la coordination et la collaboration entre les acteurs, influencer, analyser, concevoir et promouvoir des normes et des pratiques qui protégeront les utilisateurs de l'IdO tout en encourageant la croissance, l'avancement et l'applicabilité des technologies de l'IdO ;
- **défendre un environnement IdO ouvert et interopérable à l'échelle mondiale**, fondé sur des normes consensuelles axées sur l'industrie : veiller à ce que les normes techniques nécessaires soient élaborées et mises en place en garantissant une interopérabilité mondiale ;

[1] GPO (2015), « S. RES. 110 – Expressing the sense of the Senate about a strategy for the Internet of Things to promote economic growth and consumer empowerment », U.S. Government Publishing Office, 24 mars.

[2] National Telecommunications and Information Administration (2017), *Fostering the Advancement of the Internet of Things*, Green Paper, janvier.

- **favoriser la croissance et l'innovation de l'IdO en encourageant l'expansion des marchés** : application et utilisation novatrice des technologies, réduction des obstacles à l'entrée et mobilisation de tous les acteurs pour relever les défis de politique publique.

En 2015 également, deux rapports de la Federal Trade Commission ont souligné les risques liés à la sécurité et à la vie privée[1], suivis de deux autres rapports du National Institute of Standards and Technology (NIST, Département du Commerce) sur l'identification et le management de ces risques[2].

Dans le prolongement de ces travaux et de la mise en œuvre de cette stratégie, le **Developing and Growing the Internet of Things Act (DGIT Act)** a été adopté par le Sénat le 8 janvier 2020. Ce texte institutionnalise, sous l'égide du Département du Commerce, la création d'un groupe de travail qui mobilise différentes agences fédérales pour formuler des recommandations concernant l'IdO, en lien avec cinq missions[3] :

- Identifier les lois et réglementations fédérales, les pratiques en matière de subventions, les défis budgétaires ou juridictionnels et d'autres politiques sectorielles qui entravent le développement de l'IdO ;
- Concevoir des politiques ou des programmes qui encouragent et améliorent la coordination entre les agences fédérales ayant des responsabilités pertinentes ;
- Explorer les pistes et le cas échéant mettre en œuvre les recommandations du comité directeur (composé d'experts extérieurs au gouvernement fédéral) ;
- Examiner comment les agences fédérales peuvent bénéficier, utiliser, préparer et sécuriser l'IdO ;
- Consulter les parties prenantes non gouvernementales.

Par ailleurs, la National Security Commission on Artificial Intelligence (NSCAI), une commission indépendante chargée de faire des recommandations stratégiques au gouvernement pour que progresse le développement de l'intelligence artificielle, intègre aussi dans ses travaux les questions liées à l'IdO (voir notamment le rapport 2021[4]).

---

[1] FTC (2015b), *Internet of Things: Privacy and Security in a Connected World*, Federal Trade Commission Staff Report, janvier ; et FTC (2015a), « What's the security shelf-life of IoT? », Federal Trade Commission, février.

[2] National Institute of Standards and Technology-NIST (2015), *De-Identification of Personal Information*, par Simson L. Garfinkel, octobre ; et NIST (2018), *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, par Katie Boeckl, Michael Fagan, William Fisher *et al.*, septembre.

[3] Voir le texte du « Developing Innovation and Growing the Internet of Things Act » or « DIGIT Act » (2019).

[4] Dont le secrétariat est assuré par le département de la Défense. NSCAI (2021), *Final Report*, National Security Commission on Artificial Intelligence. Une première partie est consacrée aux mesures à prendre face aux menaces extérieures que fait peser l'intelligence artificielle (IA) sur le pays et ses intérêts. La seconde s'intéresse aux leviers actionnables pour promouvoir l'innovation et la compétitivité américaines en matière d'IA : investissements,

Des nouveaux projets de loi ont été déposés au Congrès sur différents sujets liés à l'IdO. Par exemple, la proposition du 27 avril 2021 cible « l'agriculture de précision »[1] et vise à orienter certains programmes de recherche de la National science fondation (NSF) et à engager des travaux d'évaluation technologique sur six axes de l'IdO. S'y ajoute la proposition très récente « IoT Readiness Act of 2021 » qui imposerait à la Commission fédérale des communications (Federal Communications Commission, FCC) de **collecter et de gérer les données sur l'évolution du marché de l'IdO, en particulier sur le marché des objets connectés via les technologies cellulaires de la 5G pour déterminer les besoins en matière de spectre.**

Une vision stratégique de la construction des standards et des certifications, sous l'égide de la NIST

La vision stratégique s'appuie aussi sur une réflexion approfondie en matière de normes, de standards et de certifications, sous l'égide du National Institute for Standards and Technology (NIST), consacré dans son rôle de coordination des travaux au niveau fédéral. C'est sur la base de son second rapport *Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline*, publié en janvier 2020, et fruit de la coordination de réflexions inter-agences, que les travaux sur les standards par secteurs et produits ont été lancés. Ces standards définis par la NIST en concertation avec les industriels et d'autres parties prenantes se voient consacrés dans la loi fédérale DGIT Act notamment en matière d'exigence pour les agences fédérales.

2.2. Au niveau fédéral, une législation renforcée en matière de cybersécurité de l'IdO acquis ou géré par les agences

Une législation qui cible aujourd'hui les achats publics et la gestion d'objets connectés par les agences fédérales

La question de la cybersécurité est considérée comme une des principales difficultés qui pourraient freiner le développement de l'IdO. Dans son rapport d'évaluation technologique en 2017, le GAO (*United States Government Accountability Office*, organisme rattaché au Congrès) a dressé la liste des principaux types de cyberattaques qui pourraient affecter l'IdO (voir Tableau 22).

formations, accords de visas, cartes vertes aux étudiants étrangers hautement qualifiés. Les secteurs agricole et alimentaire sont identifiés comme pouvant bénéficier des avancées de l'IA afin d'améliorer leur productivité tout en minimisant les impacts sur l'environnement (l'agriculture de précision).

[1] Voir GPO (2021a), « S. 2750: Precision Agriculture Loan Program Act of 2021 », U.S. Government Publishing Office, 15 septembre.

Tableau 22 – Exemples de cyberattaques qui pourraient concerner l'Internet des objets

Types d'attaques	Description
Déni de service	Attaque qui empêche ou compromet l'utilisation autorisée de réseaux, de systèmes ou d'applications en épuisant les ressources.
Déni de service distribué	Variante de l'attaque par déni de service qui utilise de nombreux hôtes pour réaliser l'attaque.
Logiciel malveillant	Un logiciel malveillant (ou malware) est un programme inséré dans un système, généralement de manière clandestine, dans le but de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation de la victime, ou de l'importuner ou de la perturber d'une autre manière. Les bombes logiques, les chevaux de Troie, les rançongiciels, les virus et les vers sont des exemples de logiciels malveillants.
Écoute passive	Surveillance ou enregistrement de données, telles que des mots de passe transmis en clair, au moment de leur transmission par une liaison de communication, et ce sans altérer ni affecter ces données.
Injection SQL	Attaque qui consiste à altérer une recherche de base de données dans une application web dans le but d'obtenir un accès non autorisé à des informations sensibles dans une base de données.
Wardriving	Méthode consistant à parcourir les villes en voiture avec un ordinateur équipé d'un système sans fil (parfois avec une antenne puissante) à la recherche de réseaux sans fil non sécurisés.
Exploit zero-day	Exploitation d'une vulnérabilité de sécurité jusqu'alors inconnue du grand public. Dans de nombreux cas, le code de l'exploit est écrit par la personne qui a découvert la vulnérabilité. En créant un exploit pour une vulnérabilité précédemment inconnue, l'attaquant crée une menace puissante, car il est difficile de se protéger étant donné le laps de temps très court entre la découverte de la vulnérabilité et de l'exploit par le grand public.

Source : GAO (2017), Internet of Things. Status and Implications of an Increasingly Connected World*, U.S. Government Accountability Office, mai, p. 27.*

Ces différents travaux se sont traduits notamment par l'adoption en décembre 2020 d'une loi sur la cybersécurité de l'IdO, l'**Internet of Things Cybersecurity Improvement Act**[1]. Cette loi donne une définition juridique des objets connectés excluant les ordinateurs, les tablettes et les smartphones. Le texte indique que cette exclusion s'explique par le fait que l'identification et le traitement des questions de cybersécurité les concernant sont bien connues. Cette loi interdit aux agences fédérales l'acquisition et l'usage des objets connectés qui ne respectent pas les standards définis par la NIST (voir *supra*). Ces standards, définis par ailleurs selon des orientations en référence aux niveaux d'exigence des standards internationaux de l'ISO (voire d'autres standards étrangers

[1] Voir le texte complet sur le site du Congrès américain.

considérés comme pertinents), doivent être respectés autant par les fournisseurs que par les sous-traitants. Cette loi exige aussi que la révision de ces standards soit réalisée au moins une fois tous les cinq ans.

Toutefois, trois exceptions sont prévues à cette interdiction : l'objet connecté pourrait être acquis ou utilisé par l'agence fédérale s'il constitue un intérêt pour la sécurité nationale, ou s'il est nécessaire pour la conduite de recherches scientifiques ou technologiques, ou enfin s'il existe des alternatives appropriées pour sécuriser l'objet en question.

Enfin, en mai 2021, l'initiative du président Biden « Executive Order on Improving the Nation's Cybersecurity » renforce les systèmes d'information et la modernisation de la cybersécurité ainsi que la sécurisation de la chaîne d'approvisionnement des logiciels au sein du gouvernement fédéral, avec des décisions spécifiques à l'IdO. Ce texte oblige aussi les fournisseurs à signaler les incidents de cybersécurité et à partager les informations avec le gouvernement.

2.3. Des réglementations adoptées par huit États, dans le sillage de celle initiée depuis 2017 par la Californie

Au niveau fédéral, la réglementation de la protection des données personnelles est aujourd'hui limitée au secteur public et à certains domaines du secteur privé

Au niveau fédéral, de nombreuses propositions de loi des deux côtés de l'échiquier politique ont cherché à introduire la protection des données personnelles, par exemple la proposition des Démocrates « Democrats' Consumer Online Privacy Rights Act » et celle portée par les Républicains « Republicans' United States Consumer Data Privacy Act of 2019 ». Il s'agit dans les deux cas de renforcer la législation existante. En effet, les États-Unis disposent depuis 1974 d'une loi qui protège les données à caractère personnel (Privacy Act de 1974). Toutefois, cette loi, qui garantit cinq grands principes – la transparence, l'accès, la correction, la sécurité des données et la limitation des finalités – est limitée aux seules données détenues par le secteur public et n'a donc pas le caractère universel que procure le RGPD.

En ce qui concerne les données privées détenues par le secteur privé, les lois sont peu nombreuses et concernent des secteurs ou des publics spécifiques : la santé avec le Health Insurance Portability and Accountability Act, les données financières avec le Gramm-Leach-Bliley Act, la protection des données concernant les enfants avec le Children's Online Privacy Protection Act. En ce qui concerne les données personnelles, seules celles qui font l'objet de finalités commerciales donnent lieu dans certains États à une réglementation.

Plusieurs États se sont dotés de réglementations spécifiques à l'IdO

L'État de Californie est le premier à avoir introduit une loi protégeant les données personnelles, en janvier 2020 (California Consumer Privacy Act, CCPA[1]). Cette loi renforce le droit à la vie privée et la protection des consommateurs résidents en Californie : elle s'appliquera aux dispositifs IdO. Les particuliers ont ainsi le droit de connaître les données personnelles détenues par les entreprises (avec critères des entreprises concernées établis par la loi) et peuvent en demander la suppression. En outre, les entreprises peuvent se voir interdire par les particuliers la vente à des tiers de leurs données personnelles. Cette loi californienne est assez large dans la définition du mode de connexion à Internet puisqu'elle s'applique à tout appareil qui se connecte « directement ou indirectement » à Internet. Leur fabriquant sont tenus de prévoir des dispositifs de sécurité qui permettent de protéger les données personnelles contre tout accès, modification, ou diffusion non autorisés.

D'autres États ont adopté une loi ou construit une proposition en cours de discussion pour réglementer en matière de protection des données privées, comme celles des États de l'Oregon et de Washington (Washington Privacy Act)[2]. Au total, neuf autres États, qui représentent 30 % de la population américaine, auraient ainsi introduit des lois s'inspirant de celle initiée par l'État de Californie. Les données privées y sont réglementées, avec des exceptions pour les données qui sont déjà couvertes par des textes au niveau fédéral (les données de santé notamment).

Enfin, différents projets de textes législatifs sur l'Internet (reconnaissance faciale, données de santé, etc.) pourraient s'appliquer à l'IdO. Ils montrent aussi que les débats dans ce domaine ne sont pas encore clos aux États-Unis[3].

2.4. Une stratégie globale qui prend forme

Au travers des éléments que nous venons d'examiner, on voit se déployer une stratégie des États-Unis consistante avec leur doctrine d'« *information dominance* ».

[1] Un autre texte de loi « The California Privacy Rights Act (CPRA) », qui entrera en application en janvier 2023, complète le CCPA, avec la création de droits nouveaux, notamment sur les informations sensibles tels que l'ethnie ou la religion.

[2] Voir Gloss K. (2021), « Navigate IoT regulations at local and global levels », *IoT Agenda*, 27 septembre.

[3] Voir la note du cabinet Deroulez (2020), « Droit applicable à l'IoT – La "discontinuité des normes" est un facteur de complications mais également d'insécurité juridique pour les acteurs de l'IoT », 11 juin.

3. Au Royaume-Uni, la diffusion des bonnes pratiques sera-t-elle suivie de l'adoption d'une loi ?

Le gouvernement britannique a pris des initiatives pour répondre aux préoccupations en matière de cybersécurité liées à l'IdO, nées notamment de la médiatisation d'incidents de cybersécurité et de violation de la protection des données.

Dès 2018, un code de bonnes pratiques pour protéger les consommateurs a été publié (*Code of Practice for Consumer IoT Security*) par le département Digital, Culture, Media et Sport. Ce code, non contraignant, est destiné aux entreprises impliquées dans le développement, la production et la vente de produits connectés. Il comporte treize bonnes pratiques en matière de sécurité des objets connectés :

– ne pas proposer de mot de passe par défaut ;
– mettre en œuvre une politique de divulgation des vulnérabilités ;
– maintenir les logiciels à jour ;
– stocker en sécurité les informations d'identification et les données sensibles ;
– communiquer en sécurité (cryptage des données) ;
– réduire au minimum les surfaces d'attaque exposées ;
– assurer l'intégrité des logiciels ;
– assurer la protection des données personnelles (selon les normes du RGPD) ;
– rendre les systèmes résilients aux pannes ;
– surveiller les données de télémétrie du système ;
– rendre facile la suppression des données personnelles pour les consommateurs ;
– faciliter l'installation et la maintenance des dispositifs ;
– valider les données d'entrée pour éviter les cyberattaques ;

Ce code ainsi que d'autres travaux complémentaires ont fait l'objet de consultation en 2019 avec le National Cyber Security Center (NCSC) et les parties prenantes au Royaume-Uni (entreprises et associations). En janvier 2021, le département Digital, Culture, Media et Sport a présenté de nouvelles propositions pour introduire une législation visant à réduire les risques de cyberattaques auxquels les appareils connectés pourraient être soumis. Ces propositions visent à garantir que tous les appareils connectés à Internet vendus aux consommateurs britanniques satisferont aux trois exigences de sécurité suivantes :

- tous les mots de passe des appareils connectés à Internet doivent être uniques et non réinitialisables selon les paramètres d'usine ;

- les fabricants d'appareils connectés grand public doivent fournir un point de contact public afin que tout individu ou entreprise puisse signaler une vulnérabilité et que celle-ci puisse être traitée rapidement ;
- les fabricants d'appareils connectés grand public doivent indiquer explicitement la durée minimale pendant laquelle l'appareil pourra recevoir les mises à jour de sécurité, que ce soit au point de vente, en magasin ou en ligne.

Si le gouvernement britannique a déclaré son intention de légiférer en la matière, aucune échéance n'a été fixée pour mettre en œuvre ce projet de loi.

BRÈVES DU MONDE

En Inde, la protection de la vie privée est actuellement réglementée par l'Information Technology Act (ITA) de 2000, et les Information Technology (Reasonable Security Practices and Procedures and Sensistive Personal Data or Information) Rules de 2011. Toutefois, l'ITA a été jugé inadéquat par un jugement de la Cour suprême en 2017 érigeant la vie privée comme un droit fondamental et demandant le développement d'un cadre réglementaire spécifique à la protection des données.

En Finlande, il n'y a pas de législation spécifique dédiée à l'IdO. Selon Traficom, il n'est pas nécessaire de réglementer les technologies individuelles, mais leurs effets et leurs utilisations doivent être réglementés.

Au Japon, s'il n'existe pas de régulation spécifique à l'IdO, on peut citer les réglementations relatives aux technologies radio, sur lesquelles s'appuient les solutions IdO, édictées par l'Association of Radio Industries and Businesses (ARIB)[1] et par le ministère des Affaires internes et des Communications (MIC), et plus largement, les réglementations relatives à la protection des données personnelles[2].

En Chine, s'il n'existe pas de réglementation spécifique sur les données générées par les réseaux IdO à ce jour, des réglementations sectorielles en cours d'élaboration et à venir préciseront progressivement ce cadre. Les données considérées comme importantes ou essentielles verront leur collecte, stockage et flux régulés. Ainsi la gestion des données générées par un réseau IdO donné dépendra du type de données générées. Des réglementations sectorielles se dessinent, notamment dans le domaine automobile : deux réglementations (avril et mai 2021) prévoient ainsi de restreindre très fortement la nature et le volume de données, notamment personnelles, pouvant être collectées et de limiter celles pouvant être stockées dans le cloud. Le texte

[1] Les technologies LPWA susmentionnées respectent généralement le standard ARIB STD-T108.

[2] L'Act on the Protection of Personal Information de 2003 (dernière version en vigueur amendée en 2017, la version amendée en 2020 prenant effet en avril 2022) que la Personal Information Protection Commission passe en revue tous les trois ans depuis un amendement en date de 2015.

mentionne en outre explicitement que les données issues des véhicules connectés doivent être stockées en Chine. Le nombre de normes IdO élaborées et mises en œuvre a sensiblement augmenté depuis 2016. En janvier 2021, le pays compterait ainsi 76 normes nationales adoptées, dont 30 dans l'IdO industriel et 62 adoptées au niveau local. Plus de 30 comités techniques, affiliés à la SAC et/ou au MIIT, auraient participé à leur élaboration. Le secteur de l'IdO figure à l'avant-poste des efforts de la Chine en matière de standardisation à l'échelle internationale, réaffirmés dans le plan China ZolynsStandards 2035.

Source : Direction générale du Trésor ; pour un tableau par pays et des sources détaillées, voir annexe 7

TROISIÈME PARTIE

CONSTATS, DÉFIS ET PISTES DE PROPOSITIONS

CHAPITRE 8

CONSTATS ET DÉFIS : L'IDO EST BIEN PLUS QU'UNE SIMPLE ÉVOLUTION TECHNOLOGIQUE

Dans un premier temps, nous faisons ici une synthèse des principaux constats et défis issus de l'analyse conduite dans le rapport, pour présenter dans un second temps nos pistes de recommandations (chapitre 9).

Cette synthèse est structurée en cinq thèmes :

- l'IdO a et va avoir un impact majeur sur la société, les citoyens et les entreprises ;
- l'IdO va être une composante importante de l'impact environnemental du numérique ;
- l'IdO accroît les surfaces de vulnérabilité ;
- les développements l'IdO se jouent largement hors de nos frontières géographiques ;
- l'IdO se base sur un cadre de régulation déjà riche mais fragmenté.

1. Un impact majeur sur la société, les citoyens et les entreprises

1 – Le premier constat que nous sommes amenés à faire concerne le développement majeur de l'IdO dans tous les aspects de nos vies et de nos activités. L'IdO est bien plus qu'une simple évolution technologique : il va transformer nos rapports au numérique et en particulier les interactions humain-machine.

2 – L'omniprésence et la relative invisibilité de l'IdO vont avoir des conséquences sur la vie privée ainsi que sur le travail et son organisation.

3 – Si les chiffres actuellement disponibles ne permettent pas de caractériser facilement le phénomène, tous montrent au minimum un accroissement majeur de l'IdO en termes de nombre d'objets concernés, de marché et d'impact.

4 – Le développement massif de l'IdO pour les usages grand public va s'opérer rapidement et à très grande échelle. L'impact de l'IdO sur les marchés et sur leur organisation va induire de nouvelles opportunités et changer les équilibres actuels.

5 – Il existe un déficit d'informations et d'outils de mesure sur l'évolution de l'IdO au niveau local, national et mondial.

DÉFIS

- Maîtriser et le cas échéant s'approprier l'Internet des objets et ses usages dans toute la société, avec leurs conséquences sociales, environnementales mais aussi éthiques et économiques.
- Améliorer nos connaissances et nos outils de mesure pour suivre le développement de l'IdO, en tant que composante spécifique du numérique, au niveau national et européen et construire des outils d'information performants pour la puissance publique, les citoyens et les entreprises.
- Accompagner les usages de l'IdO dans l'entreprise, tant dans la production, l'évolution des missions et des tâches que dans l'organisation du travail.

2. Une composante importante de l'impact environnemental du numérique

6 – Les outils pour mesurer les bénéfices et les coûts environnementaux de l'IdO à l'échelle de l'ensemble du cycle de vie des produits manquent actuellement de données, de robustesse et de reproductibilité.

7 – La massification des usages et des infrastructures (réseaux, edge, cloud, équipements) conduit à une augmentation significative de la consommation énergétique et de l'empreinte carbone, une augmentation qu'il faut mettre en regard des bénéfices potentiels sur la maîtrise des autres dépenses énergétiques et des engagements de l'accord de Paris.

8 – La 5G sera utile pour certains cas d'usages spécifiques de l'IdO mais elle peut être interrogée pour d'autres cas d'usage qui peuvent être opérés par des réseaux différents présentant des avantages techniques et environnementaux avérés.

DÉFIS

- Disposer de résultats de recherches plus nombreux, qu'il s'agisse de la mesure des impacts environnementaux, des évolutions techniques (protocoles, efficacité énergétique, protection des données personnelles, impact de l'IdO dans les organisations professionnelles, etc.).
- Concevoir et mettre en place des usages sobres et soutenables de ces technologies pour l'ensemble des acteurs (industriels, opérateurs, grand public) et inciter à leur adoption.
- Prendre en compte les enjeux spécifiques à l'IdO dans les mesures de réduction de l'empreinte environnementale du numérique sur tout le cycle de vie des produits (conception, fonctionnement, fin de vie).

3. Un accroissement considérable des surfaces de vulnérabilité

9 – L'IdO présente des risques renouvelés en matière de cybersécurité, car les objets connectés accroissent les surfaces d'attaques, notamment du fait de leurs capacités de calcul souvent moindre et des difficultés intrinsèques de mise à jour. Les situations sensibles se trouvent multipliées, de mêm que les victimes potentielles (citoyens, entreprises, organisations).

10 – Aux risques déjà connus de vol de données ou d'actes de malveillance s'ajoute le risque d'attaques systémiques à grande échelle menées depuis des dispositifs IdO. Ces attaques ont des impacts difficiles à évaluer et pour lesquels les dispositifs de protection sont souvent mal adaptés.

11 – Les compétences en matière de cybersécurité et de menaces spécifiques sont actuellement assurées par l'ANSSI dans le cadre de ses missions régaliennes. Ni la DGCCRF, ni l'ARCEP ne disposent des moyens d'intervenir sur ces sujets.

DÉFIS

Viser à renforcer la confiance dans les dispositifs IdO et permettre de meilleurs niveaux de protection contre les cyberattaques, en particulier contre des attaques systémiques rendues possibles via les dispositifs mal sécurisés.

4. Un développement qui se joue largement hors de nos frontières

12 – La perception des enjeux de l'IdO est complexe. Les technologies sont de maturité inégale et des incertitudes techniques restent à lever (identification, portabilité, interopérabilité, itinérance).

13 – Ces enjeux ne sont pas seulement techniques mais aussi géopolitiques, car les États et les entreprises internationales du numérique cherchent à imposer leurs standards et leurs solutions. Pourtant la France et l'Europe disposent de nombreux atouts (un cadre juridique en construction, des acteurs, des technologies).

14 – L'hétérogénéité des réglementations peut constituer un frein à l'adoption de protocoles en particulier basés sur les technologies LPWAN.

15 – Les enjeux de souveraineté sont nombreux et concernent autant la maîtrise des données et des technologies que la prise de contrôle de marchés ou de secteurs stratégiques.

DÉFIS

- Faire valoir les atouts européens et français en matière d'Internet des objets.
- Considérer l'IdO comme une filière industrielle stratégique et viser à organiser les industriels français et européens pour constituer une approche continentale à la mesure des enjeux.

5. Un cadre de régulation déjà riche mais fragmenté

16 – Au-delà des bénéfices directs des dispositifs IdO, la valorisation des données recueillies par ces dispositifs constitue une création de valeur importante. Les marchés qui s'organisent autour de ces données constituent un enjeu stratégique à l'échelle mondiale.

17 – De nombreuses dispositions existantes au niveau européen et national encadrent l'IdO. Mais on observe une fragmentation des dispositions qui relèvent selon les cas de la protection de la vie privée, du droit de la consommation ou de réglementations sectorielles. Ce cadre réglementaire est peu lisible et contribue à l'insécurité juridique des acteurs.

18 – En matière de protection des données personnelles, le cadre juridique actuel fondé sur le RGPD couvre la majorité des situations d'utilisation de l'Internet des objets. Mais certaines applications ne permettent pas actuellement la mise en œuvre d'un consentement libre et éclairé.

19 – Il reste des incertitudes sur le statut des données non personnelles produites dans le cadre d'application de l'IdO et sur les conditions de leur utilisation.

20 – Les contours des marchés fondés sur l'IdO sont encore très incertains, en raison de la multiplicité des acteurs. Se côtoient ici les entreprises du numérique, des télécoms et des acteurs sectoriels (bâtiment, santé, transport, jouets/jeux, habillement, agriculture, etc.) qui ont tous vocation à prendre part à la définition des marchés en devenir. Dans ce contexte, les acteurs de l'IdO pourraient être amenés à jouer un rôle de « *gatekeeper* », en imposant leurs standards technologiques et leur modèle économique, ce qui pourrait conduire à une « *plateformisation* » de certaines filières, par exemple en domotique et équipement de la maison.

DÉFIS

- Améliorer notre cadre de régulation avec des compétences mieux définies et des moyens d'intervention accrus.
- Organiser les conditions pour un partage sécurisé et équitable des données pour tous les acteurs de la chaine de valeur, y compris la puissance publique.

CHAPITRE 9

ORIENTATIONS ET PISTES DE RECOMMANDATIONS

À partir des constats et des défis résumés dans le chapitre précédent, nous formulons ici des propositions qui découlent de l'analyse menée dans le rapport. Ces propositions visent à éclairer le législateur mais aussi les citoyens pour leur permettre – dans leurs rôles respectifs – de s'approprier nos travaux et de mieux maîtriser leur environnement numérique. Elles ont aussi vocation à anticiper les sujets sur lesquels une action publique pourrait être nécessaire, au regard des points sensibles qui ont émergé au cours des auditions et de nos analyses.

Les propositions sont structurées en cinq thèmes.

- Donner les moyens de développer une vision stratégique de l'IdO : observer, mesurer, comprendre, protéger.
- Développer la recherche et intensifier la présence française dans les instances de gouvernance de l'Internet.
- Permettre le développement d'un IdO éthique et respectueux des utilisateurs.
- Soutenir le développement d'un IdO sobre et responsable.
- Concevoir un IdO de confiance pour les entreprises, les citoyens et les acteurs publics.

Le comité d'experts a par ailleurs noté l'intérêt qu'il y aurait à **impliquer davantage la représentation nationale sur les enjeux du numérique** au sein d'une commission parlementaire dédiée aux enjeux du numérique, en particulier à l'Internet des objets et aux problématiques dites d'intelligence artificielle.

1. Donner les moyens de développer une vision stratégique : observer, mesurer, comprendre et protéger

1 – **Disposer d'un outil d'observation dédié à l'IdO** portant sur les technologies, le niveau de déploiement, les acteurs et les usages afin de favoriser l'émergence d'une vision stratégique du développement de l'IdO, tant pour la puissance publique que pour les acteurs du marché.

2 – **Intégrer systématiquement au sein du nouvel Observatoire des impacts environnementaux du numérique**, prévu au titre de la loi REEN du 15 novembre 2021, un volet IdO en prenant en compte l'ensemble des dispositifs impliqués dans son fonctionnement (capteurs, réseaux, usage et stockage) sur tout le cycle de vie des équipements.

3 – **Faciliter la connaissance des réglementations**, normes, certifications, et animer une veille sur les évolutions des cas d'usage et des législations étrangères pour l'information des entreprises.

4 – **Mieux évaluer les risques systémiques de cyberattaques spécifiques à l'Internet des objets** (impacts, coûts, mesures de résilience) et mieux articuler les compétences des organismes en charge de la prévention et de la lutte contre ces menaces, notamment dans le cadre de la stratégie cyber définie au niveau européen.

2. Développer la recherche et intensifier la présence française dans les instances de gouvernance de l'Internet

5 – **Encourager et promouvoir les travaux de recherche** notamment ceux qui favorisent **l'interopérabilité et la portabilité** des solutions IdO tout en soutenant les initiatives des acteurs français et européens (organismes de recherche, entreprises) quand elles existent (système d'exploitation tel que RIOT, adoption d'identifiants uniques et travaux de l'AFNIC, par exemple).

6 – **Préparer et soutenir la représentation française dans les institutions internationales** et européennes et dans les instances de normalisation et de gouvernance de l'Internet (UIT, 3GPP, W3C, IETF, IGF)[1] en privilégiant (comme les Américains et les Chinois, par exemple) des représentations mixtes (diplomates, scientifiques, parties prenantes).

[1] Voir le glossaire en annexe 4.

7 – **Permettre la mise en place d'expérimentations** à grande échelle visant à valider des propositions techniques et à évaluer leur impact environnemental et social.

8 – **Encourager la coopération internationale, en particulier sur le partage des données** environnementales recueillies par les objets connectés, notamment celles relatives aux risques climatiques.

3. Permettre le développement d'un Internet des objets éthique et respectueux des utilisateurs

9 – **Informer le citoyen sur la protection de ses données personnelles,** de sa vie privée et de ses libertés et droits fondamentaux ainsi que sur la protection de sa sécurité et de la confidentialité de ses données, par une information disponible sur les produits ou par des campagnes d'informations publiques associant différentes parties prenantes.

10 – **L'utilisation de l'IdO dans les interventions médicales doit faire l'objet d'une déclaration explicite aux professionnels de santé et aux patients.** Explorer la possibilité d'étendre cette démarche à d'autres cas d'usage considérés comme critiques.

11 – **Consolider la mise en œuvre d'une information claire** et, lorsque cela est nécessaire, **d'un consentement « libre, spécifique, éclairé et univoque »** pour les services de l'IdO, dans le respect du RGPD.

12 – **Informer les usagers de la présence de capteurs** et de la possibilité de traçage de leurs objets connectés personnels notamment dans les espaces publics qu'ils fréquentent (rues, espaces commerciaux, lieux de loisirs, etc.), à l'image des dispositions relatives à la vidéosurveillance. Introduire un droit à l'arrêt ou à la déconnexion d'un dispositif IdO.

13 – **Adapter le cadre réglementaire actuel pour permettre un bon niveau de protection des publics vulnérables** (attention particulière pour les personnes mineures, âgées, en perte d'autonomie, etc.).

14 – **Expertiser les enjeux spécifiques de l'IdO sur le lieu de travail** (santé et sécurité, emploi et conditions de travail, droits des données et surveillance du travail) à différents niveaux (réglementation, dialogue social, pratiques des entreprises) notamment dans le cadre des travaux menés par l'observatoire **LaborIA**. Ces travaux doivent s'accompagner d'une réflexion juridique à l'intersection du droit du travail, du droit civil et du numérique.

15 – **Confier au Comité national pilote d'éthique du numérique** l'organisation d'une réflexion, associant la CNIL, le Défenseur des droits et la Commission nationale consultative des droits de l'homme sur les enjeux d'éthique et la protection des libertés et droits fondamentaux relative à la conception et à la mise en œuvre des usages de l'IdO.

16 – **Étendre le champ de compétence de la Commission nationale du débat public (CNDP)** aux questions et aux enjeux du numérique, conformément à la recommandation de cette commission du 21 février 2021, sur les projets de révision de l'article R 121-2, afin notamment de lui donner les outils lui permettant d'intervenir sur l'ensemble des questions relatives à l'environnement.

4. Soutenir le développement d'un IdO sobre et responsable

17 – **Mieux organiser les filières de recyclage pour qu'elles s'adaptent aux objets connectés**, y compris les produits hors filière électronique et électrique qui deviendront connectés (textiles, électroménagers, petits équipements), depuis les filières de tri jusqu'au recyclage, dans la perspective notamment de la révision de la directive européenne sur les DEEE (déchets des équipements électroniques et électriques).

18 – **Inclure les dispositifs IdO dans le référentiel général d'écoconception des services numériques,** prévu au titre de la loi REEN du 15 novembre 2021**.**

19 – **Intégrer dans la gestion du spectre radioélectrique des dispositifs d'incitation** à des choix d'implémentation frugaux (énergétique, données, ressources, algorithmes).

20 – **Mettre à disposition des acheteurs publics et des prescripteurs, en particulier auprès des collectivités, des outils d'aide à la décision** (bonnes pratiques, simulateurs indépendants) pour mesurer l'efficacité et les bénéfices environnementaux du déploiement d'une solution IdO (coûts/bénéfices, proportionnalité, finalité, transparence, etc.) afin notamment de nourrir les stratégies territoriales pour un numérique responsable prévues au titre de la loi REEN du 15 novembre 2021. Cette disposition pourrait également être appliquée dans le cadre de la mise en œuvre de l'article 36 de la loi n° 2021-1104 du 22 août 2021 portant sur la lutte contre le dérèglement climatique et le renforcement de la résilience face à ses effets.

21 – **Intégrer dans les certifications ou labels existants à l'attention du grand public des mentions spécifiques relatives aux objets connectés** et aux services associés permettant de s'informer sur l'impact de leurs usages mais aussi sur le niveau de confiance de ces dispositifs (fiabilité, *privacy by design*, transparence, proportionnalité, éthique, etc.) ou encore sur les risques cyber.

22 – **Intégrer explicitement les objets connectés grand public dans la liste des produits concernés par l'indice de réparabilité** prévu au titre de l'article 16 de la loi n° 2020-105 du 10 février 2020 relative à la lutte contre le gaspillage et à l'économie circulaire, dite loi AGEC.

5. Concevoir un IdO de confiance pour les entreprises, les citoyens et les acteurs publics

23 – **Créer les conditions favorables au partage maîtrisé et à la valorisation des données** qui vont être massivement recueillies par les dispositifs IdO, en favorisant l'émergence d'acteurs en capacité d'offrir aux entreprises et aux personnes publiques des garanties sur la sécurité des échanges, leur confidentialité et l'intégrité des données échangées.

24 – **Définir un statut de données sensibles** au-delà des données personnelles ou médicales pour les données industrielles ou celles qui, recueillies dans le cadre de déploiement massif de dispositifs d'observation (caméras, capteurs) pourraient présenter des risques stratégiques ou de sécurité nationale (certaines données d'urbanisme ou d'équipement des collectivités ou dans le domaine de l'agriculture).

25 – **Veiller à préserver des pratiques concurrentielles sur les différents maillons du marché** de l'IdO, y compris pour les dispositifs palliant l'absence d'interopérabilité (assistants conversationnels notamment).

26 – **Procéder aux analyses juridiques permettant notamment de définir l'échelle des responsabilités sur la chaîne des usages** afin de clarifier les niveaux de responsabilité entre les différents intervenants dans la mise en œuvre d'une solution IdO (les fabricants de capteurs, les opérateurs de réseaux et de plateformes, les entreprises qui commercialisent le service).

27 – **Analyser l'opportunité d'une loi cyber globale** compte tenu de l'étendue du champ des usages de l'IdO et du caractère interministériel des administrations concernées à l'occasion de l'adoption du Cyber Security Act européen.

28 – **Accompagner les acheteurs publics** (collectivités, hôpitaux, universités, etc.) dans la mise en œuvre et l'achat de solutions incluant des objets connectés, en mettant à leur disposition des ressources, (guide d'achat, bonnes pratiques) réalisées en collaboration avec l'ANSSI, la CNIL, l'Ademe, l'ANSES.

29 – **Cartographier les compétences respectives des régulateurs publics** susceptibles de couvrir le champ de l'IdO (télécom, données, concurrences, droit des consommateurs, etc.) afin d'identifier les lacunes existantes (par exemple,

compétences Arcep sur d'autres acteurs que télécom pour le recueil des données relatives à l'Observatoire des impacts environnementaux du numérique) mais aussi afin de mesurer les moyens à mettre à leur disposition pour l'exercice de leur mission.

30 – **Procéder pour l'IdO à une analyse juridique fondée sur une approche d'analyse des risques,** complémentaire de la démarche engagée à l'occasion de la proposition européenne d'Artificial Intelligence Act qui définit les typologies de risques (inacceptable, élevé, limité et minimal). Cette approche permettrait d'élaborer des protocoles de conformité pour les entreprises et les collectivités.

ANNEXES

ANNEXE 1

LETTRE DE SAISINE

GOUVERNEMENT
Liberté
Égalité
Fraternité

France Stratégie
Courrier arrivé le : 04/06/2021
N° : 708

Paris le 27 MAI 2021

Monsieur le Commissaire général,

Le Gouvernement porte depuis plusieurs mois une feuille de route pour mettre le numérique au service de l'environnement. Cette stratégie d'actions concrètes répond à des préoccupations légitimes de la société, relayées notamment par la Convention Citoyenne pour le Climat. Elle s'articule autour de trois grands axes de travail :

- connaitre pour mieux agir grâce à l'identification et la collecte de données précises, claires, objectives, sur les impacts réels, positifs et négatifs du numérique sur l'environnement ;
- soutenir un numérique plus sobre et plus responsable en réduisant son empreinte environnementale, des terminaux jusqu'aux usages et aux services numériques ;
- innover pour mettre le numérique au service de la transition écologique.

Dans le cadre du premier axe, nous travaillons à soutenir et appuyer des travaux d'experts afin d'objectiver l'empreinte environnementale du numérique et outiller l'action. C'est dans cette dynamique que, en parallèle de plusieurs études actuellement menées, une étude globale sur le développement des objets connectés notamment permis par les technologies nouvelles comme la 5G, va être lancée afin de mieux prendre en compte leurs effets.

Le Gouvernement souhaite confier le pilotage de cette étude à France Stratégie. Véritable projection dans un futur où la maison, la ville, l'agriculture, les machines et outils de production seront connectés, **cette étude vise à analyser les principaux impacts des technologies de l'internet des objets, et notamment à partir de la 5G, sur** :

- **l'environnement**, tant par leur empreinte écologique directe et indirecte que par leur contribution à la réduction des émissions de gaz à effet de serre en France ;

Monsieur Gilles de MARGERIE
Commissaire général
France Stratégie
Commissariat général à la stratégie
et à la prospective
20 avenue de Ségur
75007 PARIS

- **la vie quotidienne des Français**, tant par leur **impact social** sur le développement des usages que par les **enjeux sociétaux** qu'ils soulèvent, notamment au regard de leur acceptabilité et de leurs conséquences sur les données personnelles et sur la vie privée.

En matière de livrables pour cette étude exigeante et ambitieuse, il sera attendu de vos travaux, qui devront être réalisés majoritairement **sur la base de l'état des connaissances disponibles** :

- un état de l'art des applications et des principaux usages identifiés à venir ainsi que de leur état de maturité à date, et ce dans une approche prospective à 5 ans ;
- un panorama des opportunités, des risques et des impacts potentiels de ces technologies dans la vie quotidienne des Français, dans les territoires et pour les entreprises, et sur l'environnement ;
- un panorama des différentes positions argumentées des parties prenantes et des représentants de la société civile sur ces technologies et leurs usages actuels et à venir ;
- une analyse et une synthèse des principales demandes d'action à destination du Gouvernement à l'aune des évolutions contextuelles prévues (régulation, législation, etc.) notamment pour identifier celles en passe d'être mises en œuvre ou qui pourront l'être ;
- des pistes d'action pour les décideurs publics permettant de mieux prendre en compte les futurs effets sociaux, sociétaux et environnementaux des objets connectés.

Pour mener à bien votre mission, vous êtes invités à vous appuyer sur un **comité d'experts spécifiquement créé dont la composition devra garantir la pluralité des points de vue** et l'impartialité de l'étude, que vous aurez la charge d'animer. Ce comité, pluridisciplinaire, composé de personnalités qualifiées de tous horizons, pourra notamment organiser des auditions d'experts pour alimenter son analyse. La Présidence du Comité sera assurée par une personnalité de votre choix qui sera le garant de l'impartialité des travaux.

Nous vous serions reconnaissants de nous faire part de vos résultats et des pistes d'action que vous proposerez, d'ici la fin d'année 2021, afin que le Gouvernement en tienne le plus grand compte dans les modalités de déploiement des futures technologies.

En vous assurant de notre totale confiance pour le pilotage de cette étude, nous vous prions de croire, Monsieur le Commissaire général, à l'assurance de notre considération distinguée.

Barbara POMPILI

Ministre de la Transition écologique

Cédric O

Secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques

ANNEXE 2

COMPOSITION DU COMITÉ D'EXPERTS

Le comité d'experts est présidé par **Claude Kirchner**, directeur du Comité national pilote d'éthique du numérique et directeur de recherche émérite d'Inria.

Gilles Babinet, co-président du Conseil national du numérique

Didier Baichère, parlementaire, membre de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPESCT)

Valérie Beaudouin, professeure au département SES à Télécom Paris, Institut polytechnique de Paris

Éric Brousseau, professeur d'économie et de management, université Paris-Dauphine-PSL

Lucien Castex, président du comité scientifique, Internet Society (ISOC) France, membre de la CNCDH

Régis Chatellier, responsable d'études prospectives au pôle usage, innovation et prospective, laboratoire d'innovation numérique de la CNIL

Vincent Courboulay, maître de conférence en informatique, université de La Rochelle et directeur scientifique, Institut du numérique responsable

Alexia González Fanfalone, économiste analyste des politiques de télécommunication à la Direction de la science, de la technologie et de l'innovation de l'OCDE

Nathalie Mitton, directrice de recherche, Inria

Anne-Cécile Orgerie, chargée de recherche en informatique, CNRS, IRISA, EcoInfo

Kavé Salamatian, professeur d'informatique, université de Savoie

Francky Trichet, adjoint au maire et conseiller métropolitain, Ville et Métropole de Nantes, membre de l'association les Interconnectés

Célia Zolynski, professeur de droit, université Paris 1 Panthéon-Sorbonne

ANNEXE 3

LISTE DES PERSONNES RENCONTRÉES

Le comité d'experts a mené 28 auditions, de septembre 2021 à novembre 2021.

Audition du 23 septembre 2021

- **Régis Chatellier**, responsable d'études prospectives au pôle usage, innovation et prospective, laboratoire d'innovation numérique de la CNIL

Auditions du 30 septembre 2021

- **Jacques-François Marchandise**, directeur de la FING, et **Matthieu Brient**, chargé de mission du programme #RESET 2022 « Transformer le numérique » à la FING
- **Bernard Benhamou**, secrétaire général de l'Institut de la souveraineté numérique

Auditions du 7 octobre 2021

- **Olivier Beaujard**, *senior director*, LoRa ecosysteme, SEMTECH
- **Raphael Guastavi**, chef de service adjoint au service produits et efficacité matières, direction Économie circulaire et déchets, Ademe

Auditions du 14 octobre 2021

- **Dominique Boullier**, professeur de sociologie à l'Institut d'études politiques de Paris
- **Laurent Lafaye** et **Fabrice Tocco**, co-CEO de Dawex
- **Bastien Le Querrec**, membre bénévole de La Quadrature du Net

Audition du 21 octobre 2021

- **Catherine Rolin**, chargée de mission gestion prévention des déchets, France Nature Environnement

Audition du 26 octobre 2021

- **Renaud Labelle**, sous-directeur expertise à l'ANSSI

Auditions du 28 octobre 2021

- **Daniel Kofman**, professeur à Telecom ParisTech, co-fondateur et directeur de LINCS (Laboratory of Information, Networking and Communication Sciences)
- **Hugues Ferreboeuf**, directeur du projet Lean ICT du Shift Project
- **Gauthier Roussilhe**, chercheur au Centre de recherche en design, ENS Saclay, ENSCI

Audition du 2 novembre 2021

- **Sophie Quinton**, chargée de recherche à l'Inria

Auditions du 4 novembre 2021

- **Jeremy Prince**, directeur de Sigfox, et **Christophe Fourtet**, co-fondeur de Sigfox et *chief scientist officer*
- **Michel Van Den Berghe**, président, Campus Cyber
- **Bernard Ourghanlian**, directeur technique et sécurité, Microsoft
- **Stella Morabito**, déléguée générale, **Caroline Marcouyoux**, responsable environnement RSE et communication, et **Philippe de Cuetos**, directeur des affaires techniques et réglementaires, AFNUM

Audition du 5 novembre 2021

- **Louis Laurent**, directeur des études et recherches à l'INRS, et **Agnès Aublet-Cuvelier**, adjointe

Audition du 10 novembre 2021

- **Éric Vidalenc**, directeur régional adjoint à l'Ademe Hauts-de-France

Auditions du 18 novembre 2021

- **Henri Verdier**, ambassadeur du numérique
- **Éric Stefani**, Numeum, président du comité IoT, **François Lhemery**, Numeum, directeur délégué aux affaires publiques et à la communication, **Valentin Hueber**, Numeum, délégué en charge des comités Industrie du futur, IoT, intelligence artificielle, data et cloud, **Thierry Leboucq** membre de Numeum, président de Greenspector
- **Serge Abiteboul**, membre du collège de l'Arcep, **Adrien Haidar**, chef de l'unité Analyse économique et intelligence numérique, Arcep et **Anne-Lise Thouroude**, chef de l'unité Fréquences et technologie, Arcep
- **Alexandre Monnin**, directeur scientifique d'Origens Media Lab

Audition du 3 décembre 2021

- **Pierre Montagnier**, statisticien, direction de la Science, de la technologie et de l'innovation de l'OCDE

Audition du 6 décembre 2021

- **Patrick Chaize**, sénateur, référent numérique au Sénat et président de l'Avicca

Audition du 7 décembre 2021

- **Emmanuel Baccelli**, chercheur à l'Inria

Audition du 9 décembre 2021

- **Benoît Ampeau**, directeur partenariat et innovation, **Pierre Bonis**, directeur général et **Sandoche Balakrichenan**, responsable recherche et partenariat, AFNIC

●●●

Nous remercions également **Michel Combot** (FFT) et les représentants de l'AFNUM pour l'envoi d'une contribution écrite. Nous remercions également **Denis Berthault**, président du GFII, pour l'envoi du rapport d'activité 2020-2021.

Dans le cadre des auditions, nous avons souhaité rencontrer des représentants de la société Google, qui n'ont pu répondre positivement à notre proposition.

ANNEXE 4

GLOSSAIRE

3GPP	3rd Generation Partnership Project
AFNIC	Association française pour le nommage Internet en coopération
AioT	*Artifical intelligence of things* (« intelligence artificielle des objets ») : combinaison des technologies d'intelligence artificielle (IA) avec l'infrastructure Internet des objets pour réaliser des opérations IoT plus efficaces
API	*Application Programming Interface* (« interface de programmation applicative »)
AUF	Autorisation d'utilisation de fréquences
Bluetooth	Technologie de réseau personnel sans fil, noté WPAN (*Wireless Personnel Area Network*)
Cloud computing	Informatique en nuage, accès à des services informatiques via internet (le cloud)
DEEE	Déchets d'équipements électriques et électroniques
DECT	*Digital Enhanced Cordless Telecommunications* (« télécommunications améliorées sans fil »)
DIG	Données d'intérêt général
DNp	Données non personnelles
DNS	*Domaine Name Service* (« système de noms de domaine »)
Edge computing	Informatique en périphérie de réseau : stratégie qui consiste à traiter les données à la périphérie du réseau, près de la source des données.
eMBB	*enhanced Mobile Broadband* (« haut débit mobile amélioré »)
IdO/IoT	Internet des objets / *Internet of Things*

IETF	*Internet Engineering Task Force* : élabore et promeut des standards Internet, en particulier ceux qui composent la suite de protocoles Internet (TCP/IP).
IGF	*Internet Governance Forum*
IPV4	*Internet Protocol* version 4
IPV6	*Internet Protocol* version 6
ISO	*International Organization for Standardization* (« Organisation internationale de normalisation »)
LAN	*Local Area Network* (« réseaux avec une étendue spatiale limitée »)
LEO	*Low Earth Orbit* (« orbite terrestre basse »)
LoRaWAN	Protocole de télécommunication permettant la communication à bas débit par radio, d'objets à faible consommation électrique communiquant selon la technologie LoRa et connectés à l'Internet via des passerelles, participant ainsi à l'Internet des objets
LPWAN	Liaison sans fil à faible consommation énergétique
LTE-M	*Long Term Evolution for Machine* : cette extension du réseau 4G/LTE est une technologie particulièrement flexible, adaptée pour gérer des cas d'usage très variés comme les compteurs électriques (*Smart Grid*), les panneaux d'information sur la voie publique ou les voitures connectées
M2M	*Machine to machine* (« communication de machine à machine)
mMTC	*massive Machine Type Communications* (« communications de machine à machine massive »)
NFC	*Near-Field Communication* (« réseau de proximité, courte distance »)
NB-IoT	*Narrowband Internet of Things* (« réseau de communication à bande étroite pour IdO »)
QoS	*Quality of service* (« qualité de service »)
Ransom-wares	Rançongiciel : logiciel malveillant prenant en otage des données
RFID	*Radio Frequency IDentification* (« radio identification »)
RGPD	Règlement général sur la protection des données personnelles
Stand alone	Infrastructure autonome
UIT	Union internationale des télécommunications

URLLC *Ultra Reliable Low Latency Communications* (« réseau à très faible latence »)

Wifi Ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11.

W3C *World Wide Web Consortium* : organisme de standardisation à but non lucratif chargé de promouvoir la compatibilité des technologies du *World Wide Web*

ZigBee Protocole de haut niveau permettant la communication d'équipements personnels ou domestiques équipés de petits émetteurs radios à faible consommation

Z-Wave Protocole standardisé

ANNEXE 5

DESCRIPTION DÉTAILLÉE DE CAS D'USAGE

Une partie des travaux conduits par les cabinets BCG et EY-Parthenon a consisté à produire une analyse détaillée de dispositifs d'objets connectés, déjà déployés ou en cours de déploiement. Cette démarche a permis d'illustrer les réflexions du comité d'experts par des cas concrets.

Chacun des exemples retenus (voir les critères de sélection présentés au chapitre 4) a donné lieu à une analyse approfondie de quatre thèmes : maturité technologique, maturité économique, impacts sociaux et environnementaux. Selon les exemples présentés, des compléments d'information – sur le cadre juridique ou sur les conditions d'acceptation du public, par exemple – ont pu être ajoutés.

Il n'était pas possible de présenter toute la richesse des informations recueillies dans le corps du rapport, c'est pourquoi pour les lecteurs qui le souhaitent l'intégralité du document est accessible sur le site de France Stratégie.

ANNEXE 6

CALCUL DES BÉNÉFICES DE L'INTERNET DES OBJETS

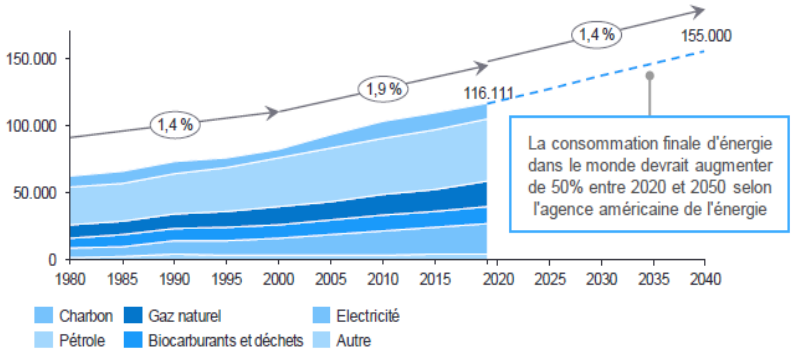
Base de calcul retenue par les cabinets BCG et EY-Parthenon pour le calcul d'une estimation des bénéfices de l'Internet des objets dans trois secteurs : industrie, transports, bâtiments.

1 La consommation finale d'énergie dans le monde pourrait atteindre 155 000 TWh / an en 2040

ANALYSES PRELIMINAIRES

La consommation finale d'énergie dans le monde a cru de ~2% p.a. entre 2000-2020 pour atteindre ~116.000 TWh et pourrait atteindre 155.000 TWh en 2040

Consommation finale d'énergie dans le monde entre 1980 et 2040 (TWh)



Principaux éclairages

En prenant une hypothèse de linéarité, une croissance de 50% entre 2020 et 2050 correspond à une croissance de ~33% entre 2020 et 2040

Ainsi en 2040, la consommation finale d'énergie dans le monde pourrait atteindre 155.000 TWh

Cette croissance se justifie principalement par la croissance démographique et économique dans les pays hors OCDE

Note : Consommation finale comme étant la consommation totale d'énergie (incl. électricité, gaz, pétrole, etc.) les données initiales ont été converti de l'"exajoule en Tera Watt heure (1 EJ= 277,77TWh)
Source : "Final consumption – Key World Energy Statistics 2021" IEA (Agence international de l'Energie) https://www.iea.org/reports/key-world-energy-statistics-2021/final-consumption, "International Energy Outlook 2021" EIA (US Energy Information Administration) https://www.eia.gov/outlooks/ieo/pdf/IEO2021_ReleasePresentation.pdf , analyse BCG et EY-Parthenon

Page 24

BCG EY Parthenon

2 La diminution des déplacements et l'exploitation de la donnée grâce à l'IoT réduiraient la consommation mondiale d'énergie de 18 à 26k TWh (soit 12-17%)

ANALYSES PRELIMINAIRES

	Industrie	Bâtiments	Transport	Total
	L'IoT devrait réduire la consommation énergétique des usines de 5 à 15% sur la base des premiers pilotes (hypothèse de travail basée sur l'expérience de BCG[1] et EY dans le domaine de l'industrie 4.0 - aucune étude publique ou semi publique n'étant disponible)	Selon l'agence international de l'Energie (IEA) la digitalisation réduirait la consommation énergétique des bâtiments résidentiels et commerciaux de l'ordre de 10%	Selon l'agence international de l'Energie (IEA), l'estimation d'efficacité énergétique pour le transport terrestre de marchandise est de 20 à 25% (sachant que le transport terrestre représente 80% des émissions de CO2 liées au transport)	-
Energie consommée (% total)	59.400 TWh (38%)	51.600 TWh (33%)	43.900 TWh (28%)	155.000 TWh (100%)
Energie économisée	3.000-9.000 TWh	6.000 TWh	9.000-11.000 TWh	18.000-26.000 TWh

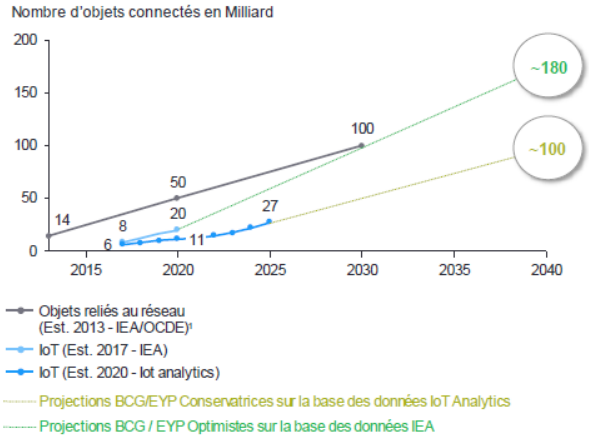
1. https://www.bcg.com/publications/2021/how-technology-helps-sustainability-initiatives
Source: "More Data, Less Energy" IEA (Agence International d'Energie) 2013 https://iea.blob.core.windows.net/assets/3fadb2cb-c2c7-4775-947f-0b8f38be0a19/MoreData_LessEnergy.pdf , "Digitalisation and Energy" IEA 2017 https://www.iea.org/reports/digitalisation-and-energy, Expérience BCG et EY-Parthenon

Page 25

3A Le nombre d'objets connectés en 2040 est estimé entre 100 et 180 milliards …

ANALYSES PRELIMINAIRES

Le nombre d'objets IoT dans le monde est estimé entre 11 et 20 milliards en 2020 et pourraient atteindre 100-180 Md en 2040



Explication de la méthodologie et principales hypothèses

Nous avons triangulé 3 sources d'information :
- Une projection faite par l'IEA en 2013 qui porte sur les objets connectés aux réseaux incluant les téléphones et les ordinateurs (courbe grise)
- Une projection faite par l'IEA en 2017 sur les objets IoT (courbe bleu clair)
- Une projection faite par IoT analytics en 2020 allant jusqu'à 2025 sur les objets IoT (courbe bleu foncé)

Nous avons ensuite extrapolé ces courbes :
- Scénario conservateur pour la courbe jaune en se basant sur la croissance d'IoT analytics 2023-2025
- Scénario optimiste (avec accélération de la pente) pour la courbe verte, en se basant sur le nombre d'objets connectés 2030 de l'IEA/OCDE (incluant les portables et ordinateurs)

Ainsi en 2040, nous estimons que le nombre d'objets IoT serait entre 100 et 180 milliards

1. Inclut les téléphones et les ordinateurs
Source: "More Data, Less Energy" IEA (Agence International d'Energie) 2013 https://iea.blob.core.windows.net/assets/3fadb2cb-c2c7-4775-947f-0b8f38be0a19/MoreData_LessEnergy.pdf, IoT analytics Sept. 2021 https://iot-analytics.com/wp/wp-content/uploads/2021/09/Global-IoT-market-forecast-in-billion-connected-iot-devices-min.png, analyse BCG et EY-Parthenon

Page 26

Source : BCG/EY-Parthenon

3B … consommant entre 3 000 et 5 400 TWh en 2040

ANALYSES PRELIMINAIRES

La consommation énergétique de 100-180 Md objets connectés serait de 3.000 à 5.400 TWh

Données de l'agence Internationale de l'Energie

Année	Nombre d'objets (Md)	Consommation énergétique (TWh/an)	Consommation énergétique / objet (kWh/an)
2013	14	616	44
2020	50	900	18

Moyenne

Extrapolation

2040	180	5.400	~30
	100	3.000	~30

Explication de la méthodologie et principales hypothèses

- Nous nous sommes basés sur les chiffres de l'IEA concernant les nombres d'objets connectés en 2013 et 2020 et leurs consommations énergétiques respectives afin de calculer la consommation par objet connecté (soit 44 et 18 kWh). Les deux nombres étant différents, nous avons considéré leur moyenne (30kWh) dans notre extrapolation en 2040
- A noter que 30 kWh comprend très certainement la consommation de bout en bout (e.g., lignes de transmission, stockage en data center, etc.) car un titre indicatif un téléphone portable consomme seulement 5kWh/an
- En combinant l'estimation de consommation énergétique par objet et le nombre d'objets connectés en 2040, nous aboutissons à une consommation IoT qui se situerait en 3 et 5,4k TWh
- A noter que notre estimation est conservatrice puisque l'IEA estime que la consommation des objets connectés pourrait être réduite de 65% grâce à une meilleur efficience des systèmes (e.g., optimisation des flux de données)
- Nous soulignons que notre calcul exclut le scope d'émissions 4 (liés à la production des objets connectés)

Source: "More Data, Less Energy" IEA (Agence International d'Energie) 2013 https://iea.blob.core.windows.net/assets/3fadb2cb-c2c7-4775-947f-0b8f38be0a19/MoreData_LessEnergy.pdf, IoT analytics Sept. 2021 https://iot-analytics.com/wp/wp-content/uploads/2021/09/Global-IoT-market-forecast-in-billion-connected-iot-devices-min.png, analyse BCG et EY-Parthenon

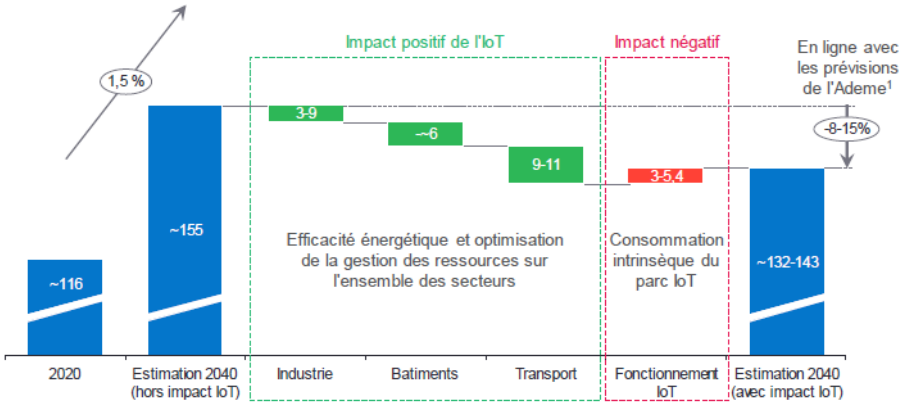
Page 27

BCG EY Parthenon

Annexe | Selon les premières analyses, le déploiement de l'IoT à l'échelle réduirait la consommation finale d'énergie dans le monde de 8-15%

ANALYSES PRELIMINAIRES

Consommation finale d'énergie et impact de l'IoT par secteur dans le monde en 2040 (1000 TWh)



Comment transposer ce raisonnement à l'échelle de la France ?

L'estimation de l'impact de IoT sur la consommation mondiale d'Energie peut être transposée à l'échelle de la France en première approximation car les prévisions en matière d'efficacité énergétique par secteur sont universelles.

En revanche, ce qui diffère c'est la répartition de la consommation énergétique par secteur (i.e., industrie, bâtiment, transport). Ainsi pour raffiner cette estimation à l'échelle de la France, il convient de considérer la répartition de la consommation énergétique par secteur en France (cf. page suivante).

1. Article cité l'Ademe : https://www.lesechos.fr/2014/02/lenergie-fer-de-lance-de-la-maison-connectee-272216
Source: IEA : "More Data, Less Energy" IEA (Agence International d'Energie) 2013 https://iea.blob.core.windows.net/assets/3fadb2cb-c2c7-4775-947f-0b8f38be0a19/MoreData_LessEnergy.pdf, IoT analytics Sept. 2021 https://iot-analytics.com/wp/wp-content/uploads/2021/09/Global-IoT-market-forecast-in-billion-connected-iot-devices-min.png, https://www.bcg.com/publications/2021/how-technology-helps-sustainability-initiatives, analyse BCG et EY-Parthenon

Page 28

BCG EY Parthenon

Source : BCG/EY-Parthenon

ANNEXE 7

ÉTUDE COMPARATIVE DANS HUIT PAYS

PAR LA DIRECTION GÉNÉRALE DU TRÉSOR

France Stratégie a bénéficié des contributions du réseau des services économiques (Direction générale du Trésor) à travers une enquête comparative conduite auprès de huit pays : le Chili, la Chine, l'Estonie, la Finlande, l'Inde, Israël, le Japon et le Nigéria. Ces derniers ont été sélectionnés avec le comité d'experts sur la base de critères tenant compte de la maturité technologique et numérique du pays, de ses caractéristiques socioéconomiques et de la nature de son cadre institutionnel et politique, afin d'appréhender les différentes approches pour encadrer ces technologies. Ces pays, en dépit des dimensions variées de leurs marchés intérieurs, présentent une maturité technologique certaine qu'illustrent des cas d'usages de l'IdO particulièrement intéressants à explorer.

Chili	• Maturité technologique et numérique
	• Une réforme constitutionnelle en cours prévoit des dispositions spécifiques au numérique
	• Enjeux géostratégiques : présence de mines de lithium
Chine	• Maturité technologique
	• Caractéristiques socioéconomiques
	• Massification des usages numériques
Estonie	• Maturité technologique
	• Environnement sociolégislatif innovant sur le numérique
Finlande	• Présence d'un opérateur européen majeur (Nokia)
	• Modèle politique
Inde	• Caractéristiques socioéconomiques
	• Démographie
	• Secteur numérique dynamique
	• Enjeux environnementaux
Israël	• Maturité technologique : cybersécurité
	• Écosystème d'innovation dynamique : start-up
Japon	• Maturités technologique et numérique
	• Caractéristiques socioéconomiques : démographie : vieillissement de la population
	• Enjeux géostratégiques : proximité avec la Chine et la Corée
Nigéria	• Caractéristiques socioéconomiques
	• Démographie
	• Enjeux environnementaux

Questionnaire de l'étude comparative internationale (ECI)

Éléments locaux de contexte du pays questionné :

1. **Quelle est l'ampleur du développement de l'Internet des objets (IdO),** destiné aux professionnels (B2B) et aux particuliers (B2C) ? Plus précisément, donner quelques indicateurs chiffrés (nombre d'objets ou de produits connectés, marchés et secteurs les plus avancés en la matière, etc.) ? Quelle est la tendance dans le pays depuis les 5 ou 10 dernières années ? Et s'ils existent, fournir des éléments sur les perspectives à moyen et long termes de développement de l'IoT dans le pays.
2. **Existe-t-il une politique publique dédiée portant sur l'IdO ? Si oui :**
   a. Quels en sont les objectifs et les moyens affichés ?
   b. Quels sont les dispositifs de soutien ou d'accompagnement des pouvoirs publics à l'égard des industriels et des acteurs de ces technologies (soutien à la R & D, développement d'infrastructures, dispositifs d'incitation à l'investissement, etc.) ?
   c. Au-delà des moyens, l'IdO bénéficie-t-il aujourd'hui d'un cadre spécifique de régulation ? Des évolutions sont-elles envisagées prochainement et de quelle nature ? (Merci de donner le cas échéant les références aux textes législatifs et réglementaires, les noms et missions des instances en charge de ces questions, etc.)
3. **Le développement de l'IdO dans le pays a-t-il fait ou va-t-il faire l'objet de débats publics ? Si oui, précisez les termes des débats, notamment sur les points suivants :**
   a. Quels enjeux autour des données de l'IdO ? Quels sont les risques majeurs identifiés en matière de libertés individuelles ? Données étant entendu ici comme données personnelles et données non personnelles.
   b. Quels sont les impacts potentiels de transformation sociale de l'Internet des objets mis en avant dans le contexte national ? Notamment, quels bénéfices directs/potentiels ou déjà identifiés pour l'usager et pour la collectivité ? Quels impacts sur l'emploi et l'organisation du travail ? Quels sont les termes des enjeux d'acceptabilité dans la société et quelles enceintes de débat public/citoyen pour aborder ces enjeux ?
   c. Quel est l'impact environnemental de ces technologies ? En particulier, quelles mesures ou chiffrages de ces impacts ? Quels sont les principaux résultats des études produites dans le pays (institutions académiques, organismes gouvernementaux, ONG) qui permettent de mesurer les impacts de l'IdO en termes de consommation énergétique, consommation de ressources, analyse du cycle de vie mais aussi en termes de gains attendus : réduction de la consommation énergétique ou de ressources (eau par exemple) ?
   d. Existe-t-il d'ores et déjà des politiques d'incitation à une meilleure prise en compte des enjeux environnementaux, par ex. amélioration des circuits de recyclage, garanties aux consommateurs ?
4. **Quelle est la prise en compte des dimensions cybersécurité et enjeux géostratégiques ? En particulier :**
   a. Quels sont les risques cyber majeurs identifiés et les dispositifs de protection mis en œuvre ?
   b. Quels enjeux internationaux géostratégiques de l'IdO pour le pays en termes notamment de normalisation, standard, portabilité ?

NB : Si possible, fournir pour les différents points les références aux études et rapports publics existants et textes législatifs et réglementaires ainsi que les liens vers les sites de débats publics organisés par les pouvoirs publics.

Étude de cas : le Chili

Service économique régional pour le Cône Sud Novembre 2021

Questionnaire : Internet des objets (IdO) – Chili

1. Quelle est l'ampleur du développement de l'Internet des objets ?

D'après le sous-secrétariat d'État aux Télécommunications chilien (Subtel[1]), le Chili recense, en novembre 2021, entre 50 et 60 millions d'objets connectés à Internet (sur 11,3 milliards d'objets connectés au niveau mondial en 2020[2]) pour 19 millions d'habitants. L'IdO en est à ses débuts et devrait se développer de façon dynamique dans le secteur minier, l'élevage du saumon, le secteur forestier et les services des « villes intelligentes ».

Le groupe d'audit et de conseil britannique Deloitte a réalisé une étude en 2018 qui montre que le Chili est le pays d'Amérique latine qui serait le mieux adapté pour le développement du marché de l'IdO[3], sur la base d'une comparaison de 33 variables appliquées aux pays appartenant à l'OCDE et à l'Amérique latine et relatives à l'infrastructure, la régulation, la capacité d'innovation, la stabilité politique et économique, l'adoption de technologies par les entreprises et le niveau de formation des ressources humaines. Cette estimation est cohérente avec des données publiées par le groupe de conseil et d'études sur les marchés des technologies de l'information, IDC, dans le cadre d'une étude financée par la BID, qui anticipe que les trois pays qui connaîtront la plus forte croissance des dépenses en matière d'IdO entre 2017 et 2022 se trouvent en Amérique latine : ce sont le Mexique, la Colombie et le Chili[4].

En 2017, un projet pilote a été mis en place, « Smart City in a box »[5], cofinancé par la BID (860 000 dollars) et le gouvernement chilien (2,4 millions de dollars) dans la ville de Temuco (localisée à 670 km au sud de Santiago). Il a pour objectif de soutenir les développeurs de logiciels pour créer des solutions sur une plateforme technologique dans les quatre domaines suivants : la surveillance de la qualité de l'air, la mise en place d'arrêts de bus virtuels, la gestion des déchets solides urbains et la gestion des incidents dans la ville. Le projet, qui devait arriver à échéance en 2021, a été retardé en raison de la crise sanitaire liée au Covid-19.

[1] Site web : https://www.subtel.gob.cl/

[2] IoT Analytics (2021), « State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion », 22 septembre.

[3] Deloitte (2018), *IoT para el sector empresarial en América Latina*, *op. cit.*

[4] Pérez R., Sergio C. et Terry E. (2019), *IoT in LAC 2019*, *op. cit.*

[5] Détails du projet : https://www.iadb.org/en/project/CH-T1195

2. Existe-t-il une politique publique dédiée portant sur l'IdO ?

Actuellement, il n'existe pas de stratégie spécifique ou de mesures ou règlementation spécifiques à l'IdO.

En revanche, des dispositifs d'appui aux entreprises peuvent être mises en place via, par exemple, des financements, des formations ou des appels à projets du ministère de la Science, de la Technologie, de la Connaissance et de l'Innovation et de CORFO[1] (*Corporación de Fomento de Chile*), agence publique de promotion de l'entrepreneuriat et l'innovation dépendante du ministère de l'Économie. Ces dispositifs d'appui sont toutefois généraux, portant sur plusieurs domaines à la fois, comme par exemple le programme de soutien au développement des entreprises qui travaillent sur des technologies telles que l'intelligence artificielle, l'Internet des objets et la réalité augmentée[2], ou l'appel à projets du programme « Net Zero » pour l'accélération de projets dans le secteur *cleantech* auquel participent des start-up du domaine de l'énergie et de l'IdO. Ainsi que le soulignait la Subtel, le secteur de l'IdO n'est pas abordé en tant que tel par le gouvernement : il s'insère dans une politique plus générale de développement technologique du pays.

À Santiago par exemple, un programme d'accompagnement aux entreprises qui produisent des produits et des services de « ville intelligente », dont l'IdO, appelé « Sé Santiago »[3] a été mis en place par CORFO et Fundación Pais Digital, association d'entreprises qui a pour but la promotion de la technologie au Chili.

Les autorités chiliennes estiment que les infrastructures de télécommunications existantes sont suffisantes pour répondre à la demande existante de connexions internet. Le développement du réseau mobile 5G n'est envisagé par le gouvernement chilien que sur le long terme. Il existe aujourd'hui cinq projets pilotes pour évaluer l'utilisation de la 5G, mis en place dans le cadre du programme « Observatorio 5G »[4], piloté par Subtel avec l'appui de la BID. Un appel à projets a été lancé par Subtel pour sélectionner une entreprise qui sera chargée de la création d'un « Centre d'expansion des entreprises et opportunités d'affaires autour de la technologie 5G[5] » qui aura pour objectif notamment de mettre en place un laboratoire de recherche et de développement de technologies afin de promouvoir la transformation numérique liée à la 5G dans les secteurs productifs des entreprises établies au Chili.

---

[1] Site web : www.corfo.cl

[2] Inria (2020), « Ministerio de Ciencia y Corfo lanzan Startup Ciencia », Institut national de recherche en sciences et technologies du numérique, 25 mai.

[3] Site web : http://www.sesantiago.cl/

[4] Site web : https://www.subtel.gob.cl/observatorio5g/ (en espagnol).

[5] Source : https://www.corfo.cl/sites/cpp/convocatorias/centro_escalamiento_y_tecnologias_5g

3. Le développement de l'IdO dans le pays a-t-il fait ou va-t-il faire l'objet de débats publics ?

Le développement de l'IdO ne fait pas l'objet d'un débat public, d'une part parce qu'il est à un stade préliminaire de son développement, d'autre part parce que le pays s'inscrit dans un modèle économique libéral, construit dans les années 1970 suivant la pensée de l'école de Chicago, notamment de Milton Friedman. L'amélioration des conditions économiques et technologiques du pays est privilégiée, sans forcément s'interroger sur les dimensions d'éthique ou de souveraineté (à titre illustratif, l'expédition des passeports et des cartes d'identité ainsi que la mise en place de systèmes d'identification pourrait être confiée prochainement, sans soulever de réel débat de société, à un consortium dirigé par le géant technologique chinois, Aisino Corporation).

4. Quelle est la prise en compte des dimensions cybersécurité et enjeux géostratégiques ?

En réponse à la multiplication des attaques informatiques, le Chili souhaite se doter d'un système législatif et opérationnel de cybersécurité susceptible de s'inspirer notamment d'un diagnostic réalisé par la société Toca (Israël ; les principaux acteurs israéliens ayant par ailleurs aussi proposé leurs services et solutions au gouvernement chilien). Dans ce cadre, le Chili a signé un accord de coopération en la matière avec Israël, puis avec d'autres pays, dont l'Espagne et le Royaume-Uni. La France avait également été sollicitée, mais l'ANSI n'a pas souhaité donner suite et le projet de protocole de coopération entre nos deux pays est finalement resté lettre morte.

En parallèle, dès avril 2017, le Chili s'est doté d'une *Politique nationale de cybersécurité* qui avait pour objectif à l'horizon 2022 : (1) d'obtenir une infrastructure d'information solide et résiliente, (2) de garantir les droits des individus dans le cyberespace, (3) de développer une stratégie de cybersécurité fondée sur l'éducation, les bonnes pratiques et la responsabilité dans la gestion des technologies numériques, en établissant des relations de coopération en matière de cybersécurité avec d'autres acteurs, et (iv) de promouvoir le développement d'une industrie de la cybersécurité pour l'atteinte de ses objectifs stratégiques.

Le document ne mentionne pas spécifiquement l'IdO. Toutefois, en novembre 2017, le gouvernement chilien a publié également un document de Politique nationale de cyberdéfense[1], en application des objectifs définis dans la Politique nationale de cybersécurité. Ce document vise à répondre aux « nouveaux » et « croissants risques et menaces » liés à la « massification de l'Internet des objets, le Big Data, l'automatisation des processus industriels et les systèmes d'armes létaux autonomes ».

[1] Source : https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf (en espagnol).

La BID appuie le gouvernement en la matière à travers des programmes d'assistance technique, notamment le programme de renforcement de la gestion stratégique de la sécurité publique au Chili, qui possède une composante dédiée au renforcement de la Politique nationale de cybersécurité[1]. La BID a par ailleurs proposé à l'État chilien de financer à 50 % la mise en place d'un système complet de cybersécurité qui dépendrait du ministère de l'Intérieur et dont l'appel d'offres, après avoir été reporté plusieurs fois, pourrait être publié début 2022.

Sur le plan législatif, le président de la République Sebastián Piñera a annoncé, fin 2021, la transmission au Congrès d'un projet de loi visant à créer l'Agence nationale de cybersécurité, qui aurait pour but principal de protéger la sécurité publique dans le cyberespace, en anticipant et en combattant la cybercriminalité pour protéger les actifs numériques du pays.

[1] BID et OEA (2020), *Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe*, rapport, juillet.

Étude de cas : la Chine

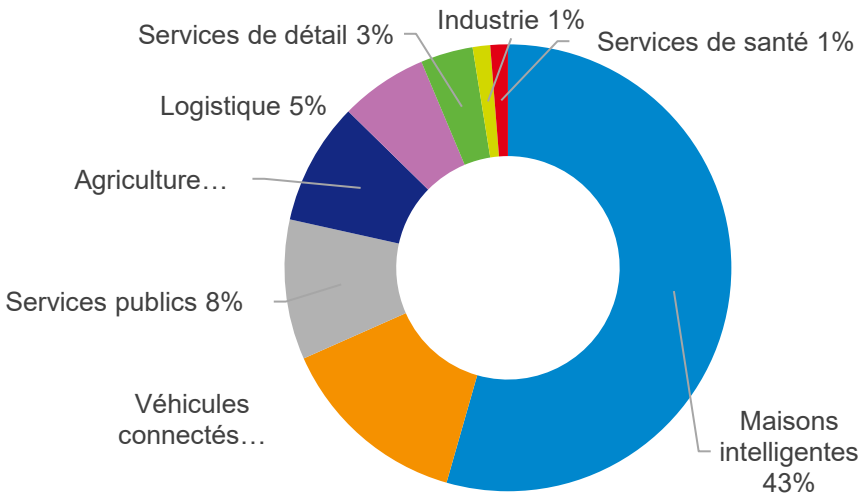
Ambassade de France en Chine

Service économique régional de Pékin

Questionnaire : Internet des objets (IdO) – Chine

1. Quelle est l'ampleur du développement de l'Internet des objets ?

Selon le CAICT[1] s'appuyant sur les données de GSMA[2], la Chine comptait 3,6 milliards d'objets connectés en 2020, soit 30 % des connexions mondiales. Le pays présente un développement avancé en IdO, Shenzhen et Pékin faisant partie des cinq premières villes accueillant les sièges sociaux d'entreprises de plateformes IdO (Tuya, Alibaba Cloud, Baidu IdO Core et Huawei Connection Management Platform). Toujours selon le Livre blanc 2020 du CAICT, le secteur de l'IdO a crû de 20 % annuellement sur la période 2016-2020, et représentait en 2020 une industrie de l'ordre de 1 700 milliards de yuans (236 milliards d'euros). L'IdO en Chine est d'abord employé pour les solutions de « maisons intelligentes » (43 %) – présence notamment de Xiaomi (30 % de son chiffre d'affaires en 2019 est généré par le secteur des produits IdO selon l'entreprise). Viennent ensuite les solutions de véhicules connectés (11 %), de services publics (8 %), d'agriculture intelligente (7 %), de logistique (5 %), de services de détails (3 %), tandis que les parts dans l'industrie et les soins de santé ne représentent chacune qu'1 %.



Source : CAICT (2020), Livre blanc sur l'IdO (物联网白皮书)

[1] Think tank affilié au ministère de l'Industrie et des technologies de l'information (ou MIIT).

[2] Global System for Mobile Communications Association.

Si la plupart des applications concerne des solutions de « maisons intelligentes », d'autres émergent dans les secteurs des services publics, de la ville intelligente mais aussi dans l'industriel (« *smart manufacturing* »). S'agissant des transports intelligents et des solutions permettant l'émergence de villes intelligentes, plusieurs plateformes sont en cours d'élaboration. Par ailleurs, plusieurs entreprises proposent des solutions d'IdO industriel : c'est le cas de RootCloud (mise en réseau des équipements de production grâce à des capteurs et à un traitement de l'information en temps réel), qui revendique 560 000 objets connectés dans 81 industries, ses plateformes utilisant par ailleurs la *blockchain* pour assurer la confidentialité et la traçabilité des données échangées ; de son concurrent direct Xreacloud[1], ou encore de Hanyun (plateforme d'internet industriel développée par XCMG, Huawei et China Unicom). L'un des exemples les plus saillants de mise en œuvre de l'internet industriel est celui de Haier, dont la plateforme COSMOPLAT compte 26 millions de machines connectées et pour laquelle deux de ses usines figurent dans la liste des usines *lighthouse* leaders dans le déploiement d'IdO industriel[2].

S'appuyant sur une certaine avance dans le déploiement d'infrastructures de télécommunications, plusieurs projets locaux voient le jour. Mi-2020, la ville de Shenzhen a annoncé avoir réalisé une couverture complète avec 46 000 stations de bases 5G standalone[3], une avance qui pourrait favoriser le déploiement de l'IdO[4]. Des projets de *smart cities* d'envergure, à l'instar du City Brain d'Alibaba à Hangzhou voient le jour. En particulier, la ville de Wuxi (province du Jiangsu) cherche à se positionner sur l'ensemble des maillons nécessaires à l'IdO (puces, capteurs, réseaux de communications), pour des applications dans les véhicules connectés, les transports intelligents et les villes intelligentes[5]. Elle accueille ainsi depuis 2009 une zone de démonstration de réseau de capteurs, dont le développement a dès 2012 fait l'objet d'un plan 2012-2020 du MIIT, ainsi que la ville IdO Hongshan[6], lancée en 2017 avec Alibaba (plateforme Feifeng 飞凤平台, solution PAAS). En ligne avec la politique industrielle chinoise, l'objectif est de s'appuyer sur l'écosystème de Wuxi pour faire émerger le secteur IdO d'abord à Wuxi puis au niveau national[7]. D'autres zones tentent de se positionner sur

[1] Yi H. (2019), « Industrial Internet Prospect XreaCloud Raises CNY 300 Mn in Series A », *EqualOcean.com*, 16 décembre.

[2] Onag G. (2020), « Haier gets its second "lighthouse" for advanced manufacturing », *FutureIoT.tech*, 17 janvier.

[3] Tomás J. P. (2020), « Shenzhen becomes first Chinese city with full 5G coverage », *RCRWireless.com*, 19 août.

[4] Lee J. (2021), « The Connection of Everything: China and the Internet of Things », art. cit. ; *Shenzen Daily* (2020), « National 5G application to speed up », 13 mai.

[5] Source : http://www.bizwnd.com/2020-05/08/c_482512.htm

[6] Source : https://finance.sina.com.cn/roll/2019-08-30/doc-iicezzrq2256336.shtml (en chinois).

[7] Le Wuxi IoT Research Institute coopère étroitement avec les grands groupes télécoms chinois. Il a à ce titre été labellisé comme une plateforme nationale pour le projet national « Perceive China » (感知中国中心) par le Premier ministre Wen Jiabao dès 2009. L'Académie chinoise des sciences, en charge de ce projet, le

l'IdO (Yangzi River Delta), un développement à nouveau encouragé le plan triennal 2021-2023 du MIIT. Enfin, la Chine privilégie, pour son LPWAN, le NB-IoT. Plusieurs projets de China Unicom, China Telecom et Huawei déploient le NB-IoT pour leurs solutions de villes intelligentes – une technologie de plus en plus utilisée, notamment en Chine[1] (90 % des connexions utilisant le NB-IoT[2]).

S'agissant des perspectives à moyen et long termes, le CAICT prévoit que le nombre de connexions en Chine atteindra 8,1 milliards en 2025. La GSMA estime que sur 14 milliards de connexions IdO dans le monde d'ici 2025, un tiers sera situé en Chine. L'IdO pourrait ajouter 196 milliards d'euros au PIB cumulé des industries manufacturières au cours des 15 prochaines années, selon un rapport d'Accenture[3]. L'industrie manufacturière bénéficiera vraisemblablement le plus du développement de l'IdO, devant les services publics. Au contraire, les secteurs de la santé, de l'éducation et des transports génèreront des bénéfices moins importants. L'utilisation de la *blockchain* (certification, traçabilité) et de l'IA (traitement des données) est par ailleurs amenée à croître pour traiter la quantité croissante de données[4]. Ainsi, dans la continuité des politiques publiques ayant permis le développement rapide de l'IdO en Chine, le plan triennal du MIIT appelle à renforcer certains maillons (puces, capteurs), à intégrer davantage l'IA et la *blockchain* dans les solutions IdO, mais aussi à élaborer davantage de normes. S'agissant des infrastructures permettant les télécommunications enfin, la Chine a annoncé en mai 2020 avoir lancé deux satellites pour la mise en place d'un réseau dédié aux applications IdO, là où la couverture par l'infrastructure terrestre est insuffisante.

2. Existe-t-il une politique publique dédiée portant sur l'IdO ?

a. Identifié comme stratégique par le MIIT, l'IdO voit son développement promu dans plus de 24 plans entre 2010 et 2020[5], dont certains sur des segments spécifiques (NB-IoT par le MIIT en 2017). Le plan *Made in China 2025* et l'initiative « Internet Plus » (2015) lui ont donné une impulsion supplémentaire. Plus récemment, l'IdO a été mentionné dans le quatorzième plan quinquennal (2021-2025) général, ainsi que dans sa déclinaison pour

présente comme une « zone de test pour un réseau mondial » devant permettre de déployer un IoT aux « caractéristiques chinoises ». Dans un premier temps, ce projet aurait conduit à peu de résultats mais la localité aurait depuis contribué à l'élaboration du standard international ISO/IEC30141 et au développement de la technologie NB-IoT et continuerait à bénéficier du soutien du gouvernement central (voir l'article « Wuxi's IoT industry cluster wins national support » de *WuxiNews.com*, mis à jour le 26 mars 2021).

[1] Goled S. (2021), « Explained: The Factors Behind China's IoT Ascendancy », *AnalyticsIndiaMag.com*, 21 janvier.

[2] Clark R. (2020), « China crosses 100M NB-IoT connections but still short of target », *LightReading.com*, 24 avril.

[3] Accenture (2015), « Internet of Things to Boost China's Economic Growth by US$1.8 trillion by 2030, Finds Accenture », communiqué de presse, 9 septembre.

[4] Voir le *White Paper 2020* du CAICT (en chinois).

[5] Lee J. (2021), « The Connection of Everything: China and the Internet of Things », art. cit.

les technologies ICT (mentionné 36 fois). L'accent est notamment mis sur le développement de l'IdO cellulaire et l'intégration avec les réseaux LTE/5G.

En septembre 2021, le MIIT et huit autres administrations publient le plan triennal pour l'établissement des infrastructures pour l'IdO (2021-2023). Celui-ci fixe plusieurs objectifs principalement nationaux (voire liste complète en annexe) : création de 10 entreprises IdO dont la valeur de la production doit excéder 10 milliards de yuans d'ici 2023 ; amélioration du système de standardisation (et de la sécurité des réseaux) ; développement d'applications dans les villes intelligentes et applications industrielles ; promotion à grande échelle d'IPv6[1].

Les efforts de développement de l'IdO s'inscrivent dans un effort national plus large d'accélérer le développement de plusieurs secteurs technologiques, de volonté d'innovation et de montée en gamme industrielle. Ils doivent ainsi s'appréhender non seulement comme un effort de développement sectoriel, mais aussi comme faisant partie d'un ensemble de technologies identifiées comme stratégiques à l'avenir. Ainsi, le Plan de développement de nouvelle génération de l'intelligence artificielle (IA) (2017) préconise de développer des capteurs intelligents et des puces permettant de soutenir la nouvelle génération d'IdO. De même, les projets d'investissements dans les « nouvelles infrastructures » (5G, cloud, internet satellitaire, etc.) permettront de rendre plus efficaces et rapides les communications entre appareils constituant un réseau IdO. Le plan triennal pour l'établissement des infrastructures pour l'IdO du MIIT (2021-2023) promeut d'ailleurs l'intégration de la 5G, du Big Data, de l'IA et de la *blockchain* au développement de l'IdO. En ce sens, la volonté de développement de l'IdO en Chine peut même être comprise, du moins partiellement, comme un effort de développement d'un secteur pluriel, dont le développement viendra de fait compléter, voire irriguer celui d'autres secteurs identifiés comme prioritaires.

L'IdO permettra des applications pour optimiser la gestion urbaine et l'industrie. La plupart des plans élaborés par les autorités mettent fortement l'accent sur le développement de l'internet industriel. Plusieurs objectifs sont fixés en ce sens. Notamment, le plan d'action de développement de l'internet industriel du MIIT (janvier 2021) fixe un objectif de 30 usines entièrement connectées par la 5G dans 10 industries différentes d'ici 2023[2]. Il préconise également de créer 10 entreprises IdO, de porter le nombre d'objets connectés à 2 milliards d'ici 2023 ou encore de promouvoir l'application (industrielle) à grande échelle d'IPv6[3] (protocole succédant à IPv4 et permettant d'identifier un nombre d'objets bien plus grand) – un objectif conforme au plan triennal pour

[1] De l'anglais « Internet Protocol version 6 », qui permet d'identifier les appareils sur internet et de les localiser, chaque appareil étant identifié par son adresse IP (analogue à une adresse postale par exemple).

[2] *China Daily* (2021), « China to build 30 "fully connected" 5G factories by 2023 », 24 janvier.

[3] Borak M. (2021), « China hatches a plan to lead in the adoption of new internet protocol as Beijing eyes internet of things », *South China Morning Post*, 31 juillet.

l'établissement des infrastructures pour l'IdO du MIIT (septembre 2021). De même, le plan *Made in China 2025* (2015) appelle à accélérer la recherche et les applications IdO ; l'une de ses composantes clefs est l'initiative « Internet Plus » pour l'internet industriel.

b. Ces impulsions politiques et ces objectifs s'accompagnent d'investissements et de mesures de soutien importantes. L'annexe sur l'IdO du plan de développement de l'industrie de l'information et des communications (2016-2020) préconise un **soutien fiscal** pour l'IdO[1], un soutien à la R & D et à la commercialisation de technologies IdO, et encourage les autorités locales à créer davantage de **fonds de soutien** à l'IdO. Dès 2011, des fonds sont mis en place à cet effet : le MIIT et le ministère des Finances ont créé un fonds spécial de projets pour le développement de l'IdO. De 2011 à 2015, ce fonds a investi en moyenne 500 millions de yuans (80 millions de dollars) par an, en soutenant plus de 500 projets de R & D liés à l'IdO. D'autres fonds, parfois non dédiés spécifiquement à l'IdO, ont également permis de financer plusieurs projets : le *China Internet Investment Fund* (CIIF) a par exemple investi près de 100 milliards de yuans (14,6 milliards de dollars) IdO. De la même manière, plusieurs programmes opérés par le MOST et la fondation nationale pour les sciences naturelles (programme 863 par exemple) permettent de financer des projets IdO. Une étude de l'*US-China economic and security review commission* (2018) montre qu'entre 2008 et 2017, plus de 2 000 publications liées à l'IdO ont été le fruit de recherches soutenues par l'un de ces programmes.

Si certains fonds existent à l'échelle nationale, les fonds promouvant le développement de l'IdO sont plus importants à l'échelle locale (subventions pour des projets d'internet industriel[2] ; projets communs entre municipalités et entreprises[3] ; ou encore zone de test dédiée[4] aux scénarios de communications entre véhicules et infrastructures routières). Le gouvernement provincial du Jiangsu prévoit dès 2010 des subventions d'un montant de 180 millions de yuans (26,3 millions de dollars) pour la R & D dans les technologies liées à l'IdO[5]. De même, des fonds ont été mis en place dans l'Anhui et le Fujian pour soutenir les efforts en R&D dans ce secteur. Le fonds d'investissement entrepreuneurial IdO de Shanghai est doté de 408,5 millions de yuans (62 millions de

[1] Aucune incitation fiscale spécifique ne semble cependant s'appliquer au secteur de l'IdO. Cependant, de même que pour l'ensemble des secteurs innovants, les entreprises considérées comme « high-tech » voient leur impôt sur les sociétés abaissé de 25 % à 15 %.

[2] Sheehan M. (2021), « Remaking "Made in China": Beijing's Industrial Internet Ambitions », *MacroPolo.org*, 22 février.

[3] GSMA (2018), *Air Quality Monitoring Using IoT and Big Data. A Value Generation Guide for Mobile Operators*, février.

[4] Source : https://baijiahao.baidu.com/s?id=1699061037285919308&wfr=spider&for=pc (en chinois).

[5] SOSi (2018), *China's Internet of Things*, rapport pour la U.S.-China Economic and Security Review Commission, octobre.

dollars). En 2017, Wuxi a annoncé la formation d'un fonds industriel pour l'IdO doté de 5 milliards de yuans (766 millions de dollars).

Au total, les investissements dans l'IdO industriel en Chine pourraient atteindre près de 27 milliards de dollars entre 2020 et 2030, contre 14 milliards de dollars entre 2017 et 2019 selon des estimations de Morgan Stanley[1]. Au niveau local, 4,6 milliards de yuans ont été investis pour faire du district de Hongshan (Wuxi) une zone-test des infrastructures NB-IdO en 2016. Enfin, de manière générale, d'importants mécanismes sont en place pour soutenir la R & D, dont notamment des préférences fiscales.

c. Les divers plans promouvant l'IdO (susmentionnés) portent davantage sur les moyens et objectifs stimulant son développement que sur sa régulation. Néanmoins, ces plans préconisent généralement une élaboration croissante de normes IdO (pour favoriser l'interopérabilité mais aussi pour assurer la sécurité des réseaux et appareils connectés – *voir par ailleurs*), tandis que les données générées par les appareils connectés, présentes sur les plateformes et transmises au sein d'un réseau IdO donné font l'objet de réglementations strictes et désormais en vigueur (*voir par ailleurs*).

3. Le développement de l'IdO dans le pays a-t-il fait ou va-t-il faire l'objet de débats publics ?

a. Les enjeux autour des données de l'IdO portent davantage sur la sécurité des données et la protection des données personnelles des utilisateurs chinois que sur les risques identifiés en matière de libertés individuelles, du fait du contexte politique propre au régime chinois. En matière de données, la Chine s'est récemment dotée d'un cadre réglementaire qui continue de s'étoffer, d'abord avec la loi sur la cybersécurité (2017), puis avec la loi sur la sécurité des données et la loi sur la protection des données personnelles, entrées en vigueur en 2021.

Identifiées comme un facteur de production économique au même titre que le capital, la main-d'œuvre, le foncier et la technologie, les données sont encadrées et leurs flux régulés : il s'agit, pour les données considérées comme peu sensibles, de favoriser la valorisation et le partage de ces dernières, en promouvant notamment la création de plateformes d'échanges afin d'en libérer le potentiel économique. Dans l'industrie, des plateformes d'échanges de données sont déjà mises en place, liant les machines et équipements de production entre eux afin d'optimiser la production. En amont des lois cadres et réglementations sur les données, des entreprises comme Haier ont ainsi développé des solutions permettant de telles connexions (COSMOPLAT). Il s'agit d'une tendance impulsée politiquement, dès 2015 avec l'initiative

[1] Stanley M. (2020), « China has a new $1.4 trillion plan to overtake US in Tech », *Bloomberg.com*, 20 mai.

« Internet Plus », ou encore avec une injonction de la part des autorités à ce que les entreprises publiques partagent leurs données[1].

À l'inverse, d'autres données considérées comme « importantes » (重要数据) et « essentielles » (核心数据) voient leur gestion, stockage et transfert strictement encadrés. Comme prévu par la loi sur la cybersécurité (2017) et rappelé par la loi sur la sécurité des données (2021), ces données générées en Chine doivent être protégées via des mesures de cybersécurité strictes, que ce soit au niveau technologique ou opérationnel. Les données ainsi générées doivent en outre être stockées sur le territoire chinois, et leur transfert est conditionné à l'obtention d'une licence de l'Administration du cyberespace (CAC) selon des conditions qui se précisent et se déclinent en fonction des secteurs[2]. En particulier, les entreprises qualifiées d'« opérateurs d'infrastructures critiques d'information » (CII) devront se soumettre à cette procédure d'approbation avant de procéder à tout transfert transfrontalier de données. De la même manière, les données personnelles doivent être stockées sur le territoire chinois, et leur exportation est conditionnée à une autorisation et un audit de sécurité.

Dans ce contexte, les données générées par les réseaux IdO feront, elles aussi, l'objet d'une attention accrue. D'une part, les données considérées comme non sensibles, et dont le transfert doit être promu afin de favoriser le développement économique en optimisant des lignes de production industrielles par exemple, verront leurs échanges préconisés. Il s'agira alors d'identifier, de classifier, et de rendre ces données interopérables. D'autre part, les données considérées comme importantes ou essentielles verront leurs collectes, stockages et flux régulés. Ainsi la gestion des données générées par un réseau IdO donné dépendra du type de données générées. Des réglementations sectorielles se dessinent, notamment dans le domaine automobile : deux réglementations (avril et mai 2021) prévoient ainsi de restreindre très fortement la nature et le volume de données, notamment personnelles, pouvant être collectées et de limiter celles pouvant être stockées dans le *cloud*. Le texte mentionne en outre explicitement que les données issues des véhicules connectés doivent être stockées en Chine. Les textes réglementaires

[1] Par exemple, la société de gestion des actifs d'État (ou SASAC, qui assure la gestion des actifs d'État et en particulier les SOE) a publié une liste de 28 entreprises chargées de fédérer les entreprises de leurs industries respectives en mettant en place des plateformes sectorielles visant de tels échanges de données.

[2] Le 29 octobre 2021, la CAC a publié une première version, ouverte aux commentaires, des « mesures pour l'évaluation de sécurité des transferts de données vers l'étranger ». Les données soumises aux procédures de contrôle sont les suivantes : (1) données générées par des « opérateurs d'infrastructures critiques » (CILO) ; (2) données « importantes », dont le principe a été introduit par la loi sur la sécurité des données ; (3) données générées par des opérateurs disposant de données personnelles de plus de 1 million de personnes ; (4) données générées par des opérateurs exportant vers l'étranger des données de plus de 100 000 personnes, ou plus de 10 000 personnes s'il s'agit de données personnelles sensibles ; (5) toute autre situation requise par une règlementation spécifique de la CAC.

sectoriels prévoient notamment que les entreprises obtiennent une autorisation des autorités avant de procéder à un tel transfert. Plusieurs entreprises automobiles ont commencé à prendre leurs dispositions : Tesla a par exemple annoncé la création d'un centre de données en Chine pour stocker et traiter les données générées par ses véhicules sur le territoire chinois. Ainsi, s'il n'existe pas de réglementation spécifique sur les données générées par les réseaux IdO à ce jour, des réglementations sectorielles en cours d'élaboration et à venir préciseront progressivement ce cadre.

b. Si plusieurs bénéfices sociétaux peuvent être considérés pour les biens de consommations pour les « maisons intelligentes » ou capteurs mesurant en temps réel la pollution de l'air, ceux-ci ne semblent pas faire l'objet d'une mise en avant spécifique contexte national. Ils sont davantage **mis en avant pour des applications dans les « villes intelligentes »** (inclusion d'IdO dans les systèmes de transports sous la forme de caméras évaluant le trafic en temps réel, chargeurs pour véhicules électriques). Alors que le taux d'urbanisation de la Chine devrait atteindre 75 % en 2030, 74 milliards de dollars ont été investis dans les « villes intelligentes » au cours de la période 2016-2020[1]. La « ville intelligente » chinoise vise à améliorer la qualité de vie des citoyens tout en permettant une gestion de la ville économe en ressources (eau, transports, énergie)[2]. Ainsi, un ensemble de capteurs collecte et intègre des données, dont l'analyse vise à anticiper les besoins des citoyens. À ce titre, plusieurs géants du numérique proposent déjà des solutions intégrés (City Brain d'Alibaba). Si les « villes intelligentes » visent à optimiser la gestion urbaine, il convient de garder à l'esprit que leur déclinaison chinoise se distingue aussi par son orientation sécuritaire (déploiement de caméras de surveillance à reconnaissance faciale, applications suivant le déplacement de citoyens).

c. Avec le développement rapide de l'IdO, de la 5G et de la *blockchain* en Chine, **les infrastructures numériques représentent un poste de consommation énergétique de plus en plus important**. D'après un rapport de 2020 sur les « nouvelles infrastructures[3] » publié par *China Center for Information Industry Development* (CCID), centre de recherche affilié au MIIT, la consommation d'électricité des centres de données en Chine a ainsi augmenté de plus de 12 % annuellement pendant huit années consécutives, et ce malgré l'amélioration de leur efficacité énergétique (passant d'un PUE[4] de plus de 1,7 vers 2013

[1] *Financial Times* (2019), « How China's smart-city tech focuses on its own citizens », 4 juin.

[2] Institut Montaigne (2021), « China Trends 10 – How AI will transform China » document de travail, novembre, p. 11.

[3] Concept présenté pour la première fois lors de la Conférence de travail annuelle sur l'économie du Comité central en fin 2018, les « nouvelles infrastructures » font références aux infrastructures pour la 5G, l'intelligence artificielle, l'IDO, le big data, etc. et constituent une priorité stratégique pour le gouvernement chinois.

[4] Le PUE (power usage effectiveness ou indicateur d'efficacité énergétique) est un indicateur général de l'efficacité énergétique des centres de données. Plus il est proche de 1, plus l'efficacité est élevée.

à environ 1,47 en 2020, selon la NDRC). Dans son rapport de mai 2021[1], l'ONG Greenpeace East Asia évalue qu'en 2020, la consommation d'électricité associée au secteur de la 5G et aux centres de données en Chine aurait atteint 201 TWh, équivalente aux consommations annuelles des villes de Pékin et de Shenzhen combinées, ou encore à 2,7 % de la consommation nationale. Plus de 60 % de l'électricité utilisée par ces infrastructures numériques provient du charbon, portant les émissions du secteur à près de 123 millions de tonnes en 2020.

Selon les projections réalisées pour 2035, leur consommation électrique devrait exploser pour atteindre 782 TWh (+289 % par rapport à 2020), soit 5 % à 7 % du total national, dont 297 TWh rien que pour le secteur de la 5G (+488 %). Au total, les émissions liées aux infrastructures numériques devraient continuer à augmenter d'ici 2035, et atteindre 310 Mt.

Le rapport relève que seulement deux grandes entreprises chinoises exploitant des centres de données se sont actuellement engagées à atteindre 100 % d'énergies renouvelables d'ici 2030 (Chindata et Athub). Greenpeace a également publié cette année son deuxième rapport annuel *Clean Cloud*[2] pour la Chine, qui évalue les performances climatique et énergétique des 22 plus grands fournisseurs de services *cloud* et d'opérateurs de centres de données chinois.

Sur la partie amont de la chaîne de valeur, un autre récent rapport de Greenpeace réalisé conjointement avec l'Institut de l'environnement de l'université Renmin estime que les émissions liées à la production des « nouvelles infrastructures » en 2020 sont inférieures de 7,24 % à celles des infrastructures traditionnelles[3], soit environ 172,7 Mt contre 186,1 Mt de CO_2. Cependant, le potentiel des « nouvelles infrastructures » en matière de réduction d'émissions reste assez limité tant que l'ensemble de la chaîne d'approvisionnement reposera sur le bouquet énergétique chinois très dépendant du charbon. En effet, la production en amont des « nouvelles infrastructures » provoque une forte demande en produits issus des secteurs énergivores et très émissifs, notamment la métallurgie, la chimie et les produits minéraux non métalliques[4]. Ainsi, en l'absence de normes environnementales pour l'ensemble de la chaîne d'approvisionnement, les gains en matière d'efficacité énergétique et de réduction d'émissions liées à l'exploitation de ces nouvelles infrastructures du numérique pourraient être facilement contrebalancés par les industries en amont.

Enfin, le déploiement rapide des objets connectés présente également le risque d'une accumulation sans précédent des déchets électroniques, notamment ceux devenus

[1] Greenpeace (2021), *China 5G and Data Center Carbon Emissions Outlook 2035*, rapport, mai.

[2] Greenpeace (2021), *Clean Cloud 2021. Tracking Renewable Energy Use in China's Tech Industry*, rapport, avril.

[3] Greenpeace (2021), « In 2020, China's "new infrastructure" emitted 7.24% less carbon than traditional infrastructure: Greenpeace », communiqué de presse, 29 septembre.

obsolètes car « non connectés » ou incompatibles avec la 5G. En Chine, d'après les données officielles[1], la capacité de traitement annuelle des déchets D3E (équipements électriques et électroniques) est de 160 millions d'unités (téléviseur, réfrigérateur, machine à laver, climatiseur, ordinateur), avec 2,18 Mt de déchets effectivement traités en 2019. Ce chiffre est bien en deçà de la quantité théorique de déchets D3E (14 catégories) estimée par l'Institut de recherche sur les appareils électroménagers en Chine (CHEARI) à 6,34 Mt pour 2019, équivalent de 624 millions d'unités[2].

d. Conscient de la consommation importante d'énergie et de ressources des infrastructures du numérique, le gouvernement chinois a introduit ces dernières années de multiples politiques incitatives pour encourager le développement « vert » du secteur dans l'ensemble du pays. En septembre 2019, dans l'Avis sur le renforcement du développement vert des centres de données, le MIIT appelle à améliorer l'efficacité de l'utilisation des ressources en eau et le recyclage des déchets D3E ainsi qu'à augmenter la part des énergies renouvelables. Son récent 14e plan quinquennal pour l'industrie de l'information et des communications (ICT), publié le 16 novembre, prévoit une réduction de 15 % de la consommation d'énergie dans le secteur des télécommunications et une diminution de PUE de 1,4 à moins de 1,3 pour les nouveaux grands et très grands centres de données. Dans un document d'octobre 2021[3] relatif à l'efficacité énergétique et à la réduction des émissions de carbone dans l'industrie, la plus haute autorité de régulation économique chinoise (NDRC) prévoit également d'optimiser la planification géographique des centres de données et interdit aux gouvernements locaux d'accorder des politiques préférentielles en termes de terrains, de financement et de fiscalité à des nouveaux centres construits en dehors des huit agglomérats numériques nationaux[4].

4. Quelle est la prise en compte des dimensions cybersécurité et enjeux géostratégiques ?

a. Le risque de cyberattaques et la vulnérabilité augmentent naturellement avec le nombre d'objets connectés, chaque élément composant un réseau IdO devenant la cible d'une attaque potentielle, **mais une attaque à l'encontre d'un objet connecté exposant aussi potentiellement l'ensemble du réseau IdO auquel cet objet est connecté** (vers IdO polymorphiques).

[1] Voir le rapport annuel 2020 du ministère de l'Écologie et de l'Environnement sur la prévention et le contrôle de la pollution par les déchets solides dans les grandes et moyennes villes.

[2] Source : https://www.qianzhan.com/analyst/detail/220/210414-2e3f6e82.html (en chinois).

[3] Source : https://www.ndrc.gov.cn/xxgk/zcfb/tz/202110/t20211021_1300583.html?code=&state=123 (en chinois).

[4] Mégalopole Pékin-Tianjin-Hebei, région du delta du fleuve Yangtze, région de la Grande Baie de Guangdong-Hong Kong-Macao, cluster Cheng-Yu, Guizhou, Mongolie intérieure, Gansu et Ningxia.

Parmi les vulnérabilités identifiées, figure notamment un niveau insuffisant de sécurisation des terminaux connectés. Fin 2016, le producteur d'appareils IdO Hangzhou Xiongmai Technology Co. Ltd (杭州雄迈信息技术有限公司) a été forcé de rappeler plus de 10 000 webcams après qu'elles aient été victimes d'une attaque par le malware Mirai botnet. Les appareils Xiongmai auraient en fait été mis sur le marché sans même être équipés de dispositif de sécurité de base, en faisant des cibles privilégiées. En 2017, il a été démontré que plus de 175 000 caméras connectées (reliées à un réseau IdO) produites par Shenzhen Neo Electronics et installées dans plusieurs pays étaient en réalité accessibles à distance en raison, là aussi, d'une insuffisante sécurité dans les protocoles d'accès des appareils.

Pour autant, la question de la sécurité des appareils connectés à un réseau IdO n'est pas nouvelle pour les autorités. Dès 2011, l'Académie de la recherche en télécommunications du MIIT avait identifié la sécurité comme l'un des principaux défis du développement de l'IdO, appelant à une évaluation méticuleuse des menaces sécuritaires et des vulnérabilités liées aux fuites de données[1]. Par la suite, le plan d'action spécial pour le développement de l'IdO (2013) et l'annexe dédiée à l'IdO du plan de développement de l'industrie de l'information et de la communication (2016) identifient la sécurité de l'IdO comme l'une des tâches les plus importantes.

Ainsi, les recherches sur la sécurité des réseaux IdO se multiplient. Selon les données de CNKI, environ 1 229 articles relatifs à la sécurité IdO ont été publiés en 2017[2], contre 9 en 2009 – des chiffres à lire également au regard du nombre croissant d'appareils connectés. La recherche s'est principalement concentrée sur les vers IdO polymorphiques[3], tentant de modeler la manière dont un tel vers pourrait se propager[4]. De même, **sont régulièrement publiées des évaluations des vulnérabilités** de différents logiciels sur une banque de données nationale des vulnérabilités (国家信息安全漏洞库) afin de faciliter l'identification pour les entreprises des points de vulnérabilités dans leurs architectures de sécurité. Plusieurs instituts de recherche se penchent sur la question de la sécurité des réseaux : le Beijing Key Laboratory of IdO Information Security Technology se concentre par exemple sur les systèmes de contrôle industriel.

Enfin, les comités en charge d'élaboration des normes se concentrent principalement sur la sécurité des composants constituant un réseau IdO. Le comité technique TC260, principal organisme en charge de définir les normes du secteur ICT en

[1] Source : http://tech.sina.com.cn/t/2011-05-20/14515550667.shtml (en chinois).

[2] SOSi (2018), *China's Internet of Things*, *op. cit.*

[3] Permettant d'infecter plusieurs appareils connectés à un réseau, une fois le premier appareil infecté.

[4] À noter par ailleurs que la modélisation de la propagation d'un malware IdO polymorphique a des applications défensives, mais aussi offensives.

Chine, est notamment en charge d'élaborer le cadre pour la sécurité des réseaux d'infrastructures d'information critiques (CII) ainsi que de la sécurité du système de contrôle industriel. La *China Communications Standards Association* (CCSA), organisation responsable de la communication et de la sécurité des réseaux, contient trois groupes de travail techniques[1]. Le TC10 pour les réseaux ubiquitaires est en charge des conditions de sécurité, des analyses de conditions de sécurité pour les villes intelligentes ; le TC8 Network and Information Security élabore les conditions pour la protection et la sécurité des systèmes d'information M2M ; enfin, le TC11 est en charge de la recherche sur les problèmes de sécurité de l'information.

b. L'élaboration de normes en matière d'IdO répond d'abord à un besoin intérieur. Il s'agit d'assurer l'interopérabilité de ce qui constitue les réseaux IdO (objets, passerelles applicatives, plateformes), et de limiter les risques de sécurité. En octobre 2021, le plan d'orientation pour établir un système de normes de sécurité de base pour l'IdO préconise d'élaborer au moins dix normes industrielles IdO d'ici 2022 et 30 d'ici 2025, qui devront améliorer le niveau de sécurité dans différentes applications industrielles. Il préconise l'élaboration de normes permettant d'assurer la sécurité des terminaux IdO (objets), des passerelles applicatives[2], des plateformes, mais aussi d'améliorer les conditions générales de sécurité. Le plan s'avère assez détaillé dans ses recommandations (nécessité de se baser sur des scénarios de risques, encouragement à établir dès à présent des modèles d'architecture de sécurité, assurer la sécurité des données mais aussi de l'appareil en lui-même), ce qui témoigne de l'importance d'établir ces normes.

La standardisation pour l'IdO procède essentiellement des compétences du MIIT et de l'Administration de la standardisation (SAC). En 2019, cette dernière a créé un organe coordinateur national (SAC/TC28/SC41), **dont le mandat est la standardisation complète de l'IdO**. Créé par le MIIT en 2002, l'Association des standards de communication (CCSA) participe à l'élaboration de normes à l'échelle internationale, étant notamment active au sein du 3GPP (*Third-generation partnership project*) et de l'Union internationale des télécommunications (UIT).

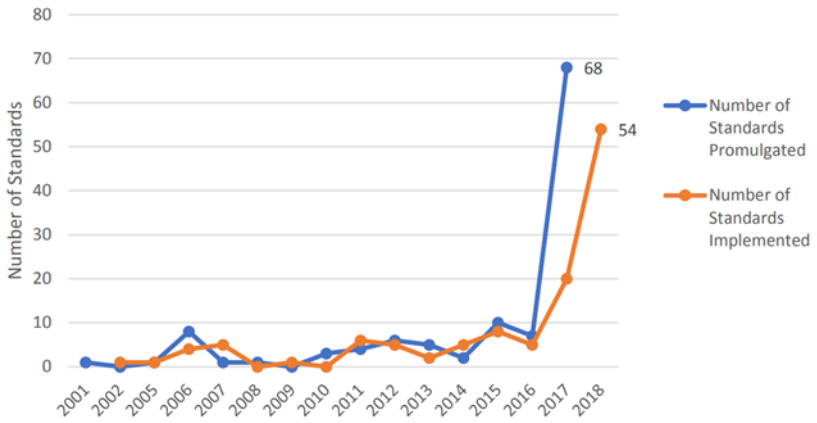
Conséquence directe de ces injonctions, le nombre de normes IdO élaborées et mises en œuvre a sensiblement augmenté depuis 2016. En janvier 2021, le pays compterait ainsi 76 normes nationales adoptées, dont 30 dans l'IdO industriels – et 62 normes adoptées au niveau local. Plus de trente comités techniques, affiliés à la SAC et/ou au MIIT, auraient participé à leur élaboration[3].

[1] Huawei (2016), « IoT Security Policy and Regulation initiatives in China », ETSI IoT Security Workshop, juin.

[2] Ou *gateway* en anglais, qui assure la transmission des objets connectés à la plateforme, *cloud* par exemple, qui les analyse.

[3] SOSi (2018), *China's Internet of Things*, *op. cit.*

Nombre de normes IdO adoptées et mises en application en Chine, 2001-2018



Source : SOSi (2018), China's Internet of Things, rapport pour la U.S.-China Economic and Security Review Commission, octobre, p. 64

Loin de faire figure d'exception, le secteur de l'IdO figure au contraire à l'avant-poste des efforts de la Chine en matière de standardisation à l'échelle internationale, réaffirmés dans le plan *China Standards 2035*. Les standards sont généralement perçus comme un enjeu stratégique de compétitivité[1], et les standards industriels notamment comme un moyen d'augmenter la compétitivité des biens et services chinois à l'international, notamment dans les secteurs comme les télécommunications, la *blockchain* et l'IdO. Ainsi, le plan d'orientation du MIIT (janvier 2021) appelle à une coopération avec d'autres pays en matière de standards de sécurité de base pour l'IdO, tandis que le plan *China Standards* 2035 appelle à la standardisation de l'IdO. En particulier, le rôle des entreprises dans l'influence de normes est appelé à se renforcer. *China Standards 2035* et *Made in China* 2025 encouragent les entreprises chinoises (et notamment les « champions nationaux ») en ce sens. Plus récemment, le plan pour le développement de la standardisation (octobre 2021) appelle, conformément aux axes définis[2] par la nouvelle version (2018) de la loi sur la standardisation datant de 1988, à renforcer le rôle du marché dans la standardisation, tandis que le 14e plan quinquennal pour les TIC (2021-2025) du MIIT abonde dans ce sens : il incite les entreprises chinoises à s'internationaliser et à participer à la définition de normes internationales dans plusieurs domaines, dont l'IdO.

Une double démarche est à l'œuvre pour influer sur les normes au niveau international : participer à leur élaboration *via* des représentations et une activité accrue au sein d'enceintes internationales de standardisation d'une part, tout en assurant une large adoption de produits ICT chinois par d'autres pays d'autre part. Le plan d'action pour

[1] de la Bruyère E. (2021), « China's quest to shape the world through standards setting », *HinrichFoundation.com*, 13 juillet.

[2] Garofano V. A. (2018), « New China's standardization law: an overdue reform », *Lexology.com*, 30 janvier.

la formulation de normes (标准制定专项行动计划), l'un des dix segments du plan d'action pour le développement de l'IdO (物联网发展专项行动计划), appelle à s'imposer au sein d'organes tels que l'ISO/IEC et l'IUT. De même, un nombre croissant de projets dans le secteur des TIC en pays tiers, dans le cadre des routes de la soie numériques par exemple, permettent aux entreprises chinoises d'y installer leurs propres infrastructures en diffusant ainsi leurs propres normes dans ces pays, ouvrant la voie à une adoption *de facto* de ces normes et garantissant une nécessité future d'interopérabilité. Fin 2020, sur 18 normes IdO adoptées par l'ISO/IEC, 10 étaient proposés par des acteurs chinois. Parmi les exemples mentionnés dans les médias chinois, figurent :

- l'adoption en 2018 de la norme ISO/IEC30141 (architecture de référence), dont l'élaboration est présentée comme ayant été dirigée par l'institut IdO de Wuxi, est souvent montrée comme un exemple à suivre ;
- la WAPI Industry Alliance (organisation chinoise promouvant le standard WAPI comme alternative au WIFI), composée d'industriels chinois, a obtenu en 2017 la reconnaissance par l'ISO de son standard TRAIS-X7[1], notamment utilisé pour sécuriser les protocoles IoT ;
- la Chine est à l'initiative d'un groupe de travail (ISO/I EC JTC1) dédié à la standardisation d'une technologie combinant la *blockchain* et de l'Internet des objets (IoT).

S'agissant des deux premières normes néanmoins, leurs impacts semblent faibles. La première, ISO/IEC30141, est une architecture de référence, s'apparentant à une sorte d'annuaire permettant d'identifier les différents éléments composant un réseau IdO, et ayant ainsi peu d'implications techniques et technologiques. La seconde concerne principalement les interfaces RFID (interface d'identification par fréquence) permettant d'identifier des objets sur des distances très courtes (de l'ordre de 10 cm), et apparaît peu utilisée.

[1] Source : http://www.xinhuanet.com/webSkipping.htm (en chinois).

Annexe – Perspectives de développement de l'Internet des objets : enjeux environnementaux et sociaux en Chine

Liste des objectifs préconisés dans le plan triennal pour l'IdO :

- **Amélioration du système de standardisation** : création d'un système de sécurité des réseaux, des données et permettant la protection des données personnelles. Il est préconisé d'établir une cartographie des normes IdO pour l'ensemble de la chaîne industrielle et de poursuivre la participation dans les enceintes internationales de standardisation.
- **Interaction avec les technologies complémentaires** : développer davantage les capteurs, les puces spécifiques pour l'IdO ; y favoriser l'intégration de la 5G, du Big Data, de l'IA et de la *blockchain*.
- **Optimisation de la capacité d'innovation** notamment en soutenant la recherche dans les « *hard tech* » (capteurs, technologies de communication courte distance, positionnement de BeiDou, capteurs MEMS et puces IdO, développement du *edge computing*, IPv6, optimiser la 5G pour réduire les latences, continuer la recherche sur l'IA, *machine learning*, etc.).
- **Objectifs chiffrés de développement de l'IdO** : le nombre de connexions IdO doit dépasser le seuil de 2 milliards d'ici 2023 ; et 10 entreprises IdO dont la valeur de la production doit excéder 10 milliards de yuans d'ici 2023 doivent être créées.
- **Améliorer l'IdO pour les chaînes industrielles** (transformation numérique) notamment dans les zones de développement comme le Yangzi River Delta, la Greater Bay Area et Chengdu-Chongqing Twin Cities Economic circle. La plupart de ces zones développaient déjà un *cluster* pour l'IdO industrielle : Yangtze River Delta (capteurs, développement des logiciels et intégration des systèmes) ; le Pan-Pearl River Delta (production d'équipements intelligents ; intégration des logiciels, services d'opération des réseaux).
- **Applications dans les villes intelligentes** : villes intelligentes (infrastructures urbaines digitalisées, avec des capteurs dans les tunnels, des plateformes hébergeant des données urbaines au niveau des villes) ; villages numériques en renforçant le rôle des technologies de capteurs et équipements IdO pour des gestions de crise par exemple (prévention des désastres naturels, prévention épidémique, etc., pour soutenir la capacité de gouvernance rurale). Transports intelligents (bus, informations relatives au trafic routier) : établir notamment une plateforme de surveillance complète pour coordonner les réseaux de véhicules intelligents (et établir des scénarios applicatifs pour la gestion du parking, du trafic urbain).
- **Applications industrielles** : (1) dans l'agriculture « intelligente » ; (2) *smart manufacturing* : surveillance en temps réel des statuts de production, encourager les

entreprises à adopter des réseaux où les temps de latence sont faibles comme la 5G ; (3) construction « intelligente » (pour les sites de construction par exemple) ; (4) protection environnementale « intelligente » avec des terminaux de capteurs pour les environnements aquatiques, les sols, les déchets solides, mais aussi créer des applications de gestion des sources de pollution, etc. ; (5) tourisme culturel et intelligent (entrée des touristes sur les sites).

- **Promouvoir l'application à grande échelle d'IPv6** : en améliorer les normes techniques ; encourager les entreprises à adopter des solutions d'application basées sur l'IPv6 pour des applications industrielles en faisant des applications pilotes s'appuyant sur l'IPv6.
- **Améliorer la sécurité des réseaux** (comme la vulnérabilité augmente avec le nombre de connexions et d'appareils connectés).
- **Cultiver les talents ; renforcer le soutien financier et fiscal** (fonds gouvernementaux au niveau national et local, les institutions financières sont aussi encouragées à participer à la construction d'infrastructures).

Étude de cas : l'Estonie, la Lettonie et la Lituanie

Ambassade de France en Estonie

Antenne à Tallinn du Service économique des États baltes

Questionnaire : Internet des objets (IdO) – Estonie

Personnes interrogées dans le cadre de ce questionnaire :

- **Indrek Ruiso**, CEO de l'entreprise de solutions IoT Eliko. L'entreprise a déjà une expérience en France, via un partenariat avec Le Puy du Fou et est l'une des plus anciennes sur le marché (2004).
- **Pelle Jakovitz**, co-directeur du laboratoire de recherche IoT Lab de l'université de Tartu. Il est également co-directeur du parcours centré sur l'IoT proposé au sein de l'université.

1. Quelle est l'ampleur du développement de l'Internet des objets ?

En 2017, l'Estonie a été classée parmi les meilleures réussites dans le domaine de l'Internet des Objets par un rapport de la Banque mondiale[1]. La stratégie *Digital Agenda 2020* du ministère des Affaires économiques et des Communications place l'IdO dans sa liste de solutions d'avenir pour développer le bien-être des consommateurs, notamment en assurant l'efficience des solutions proposées et mises en place par les entreprises et le gouvernement. Ces solutions visent à être utilisées par les citoyens au quotidien, dans leurs interactions avec les pouvoirs publics mais aussi avec les agents privés.

Dans les faits, de nombreuses solutions IdO sont d'ores et déjà mises en œuvre par les entreprises estoniennes. On peut en retrouver sur des projets d'ampleur et d'utilité variable :

- en 2017-2018, Proekspert a développé un système permettant de contrôler et d'ajuster automatiquement la **consommation d'énergie sur les bateaux**, en se concentrant sur l'air conditionné[2] ;
- en 2020, Eliko a développé un **système de localisation en temps réel**, qui permet de contrôler et organiser les flux (de transports ou de personnes) en temps réel[3] ;
- en 2019, SBA Service a développé une **usine de granulés de bois entièrement automatisée**, ajustant sa production à des données en temps réel (consommation, température, souci quelconque sur la chaîne d'approvisionnement, etc.)[4]. Ils ont aussi contribué à l'automatisation de l'usine de Le Moulin Lautier en France (2019)[5] ;

[1] Banque mondiale (2017), *Internet of Things. The New Government to Business Platform*, rapport.

[2] Proekspert (s.d.), « Reduce HVAC power consumption 10% ».

[3] Eliko (s.d.), « How real-time tracking of vehicles is optimising logistics », étude de cas.

[4] SBA (s.d.), « Vägari. Project in Estonia, 2019 ».

[5] SBA (s.d.), « Le Moulin Lautier. Project in France, 2019 ».

- depuis 2014, Starship a développé un **système de robots livreurs**, s'adaptant aux obstacles en temps réel ;
- AuveTech développe actuellement un **système de navette autonome**, prenant en compte la circulation en temps réel ;
- depuis 2017, Telia a développé un système destiné au suivi et à l'orientation des performances sportives dans le cadre du centre sportif de Kääriku[1] ;
- depuis 2016, Eliko a développé le système **Smart Street** à Kalaranna, contrôlant l'éclairage (selon la circulation/l'heure/le nombre de passants), l'intensité du trafic routier, l'état des poubelles ou encore le niveau de pollution.

La tendance est à l'accroissement de ce type de technologie, notamment dans le secteur de l'énergie et dans le secteur du transport. Si la situation du réseau mobile est déjà satisfaisante, notamment depuis la mise en œuvre de la 5G dès 2020, son amélioration permettra de développer de nouvelles solutions, plus précises et potentiellement adaptées à chaque situation.

La recherche entourant l'IdO va en s'accroissant. Par exemple, en 2016 un laboratoire dédié a été ouvert à l'université de Tartu – en collaboration avec Telia. Il s'agit d'un laboratoire de recherche, permettant de tester l'application de nouvelles technologies d'IdO – en particulier pour les questions d'économie d'énergie. Le laboratoire reste ouvert à toute recherche dans d'autres secteurs (santé, agriculture, enseignement) tant qu'elle implique l'IdO. Le laboratoire se satisfait de voir que les autres secteurs de la recherche universitaire se tournent de plus en plus vers eux. Néanmoins, Pelle Jakovitz regrette le manque de coopération internationale sur le sujet.

Enfin, il faut noter l'engagement de plusieurs entreprises estoniennes (Eliko, Proekspert, Telia) dans l'Industrie 4.0 – qui vise à mettre en œuvre les solutions IdO dans l'industrie. Ce dernier souligne l'intérêt croissant des autres secteurs de la recherche pour le sujet, dans une grande diversité. Indrek Ruiso, CEO d'Eliko, souhaite tempérer : les entreprises d'IdO estoniennes implantent surtout leurs solutions à l'étranger. La raison est très simple : l'industrie estonienne est très faible et très en retard sur le plan technologique.

De manière plus concrète, l'agence de statistiques gouvernementales (Statistics Estonia) étudie l'utilisation de l'IdO par les entreprises depuis 2020 et surtout le type d'utilisation. Les résultats figurent dans le tableau page suivante[2].

[1] Digitark (2017), « Telia ja Kääriku Spordibaas hakkavad koos arendama terviseandmete analüüsi tulevikutehnoloogiaid », 10 mars.

[2] Disponibles ici : Statistics Estonia (s.d.), IT148: Enterprises using Internet of Things by Economic activity and Number of persons employed, base de données statistiques.

Entreprises utilisant l'Internet des objets par indicateur, activité économique, nombre d'employés et période de référence

	Total		De 10 à 19 employés		De 20 à 49 employés		De 50 à 99 employés		De 100 à 249 employés		250 employés et plus	
	2020	2021	2020	2021	2020	2021	2020	2021	2020	2021	2020	2021
Entreprises utilisant des dispositifs ou des systèmes interconnectés qui peuvent être surveillés ou contrôlés à distance par Internet (Internet des objets), en %.	16,1	17,4	14,3	16,2	16,0	16,2	17,9	19,5	25,6	23,8	29,8	36,3
Entreprises utilisant des compteurs, lampes ou thermostats intelligents pour optimiser la consommation d'énergie dans leurs locaux	33,6	35,4	27,7	28,2	32,2	35,7	37,7	40,8	54,4	52,4	60,8	67,9
Entreprises utilisant des capteurs, des étiquettes RFID ou IP, ou des caméras pilotées par Internet pour améliorer le service client, suivre les activités des clients ou leur offrir une expérience d'achat personnalisée, en %	38,2	15,9	33,0	17,5	45,1	13,7	35,8	15,7	42,9	14,3	45,1	15,1
Entreprises utilisant des capteurs de mouvements ou de maintenance pour suivre le déplacement de véhicules ou de produits ou proposer un service d'entretien des véhicules en fonction de leur état, en %	53,2	26,5	55,8	18,0	55,6	29,7	46,8	36,5	42,7	45,2	43,1	43,4
Entreprises utilisant des étiquettes RFID pour surveiller ou automatiser les processus de production, gérer la logistique, suivre le mouvement des produits, en %	21,0	42,3	14,1	39,1	20,0	43,7	34,6	50,6	34,7	41,7	45,1	49,1
Entreprises utilisant des dispositifs IdO pour assurer la sécurité de leurs locaux, en %		69,6		65,9		72,2		66,1		80,5		83,0
Entreprises utilisant des dispositifs ou systèmes IdO, en %	35,6	23,5	34,7	20,6	28,9	19,7	49,6	33,7	42,3	28,8	45,1	43,4

Il est intéressant de constater que les entreprises utilisent aujourd'hui les solutions IdO essentiellement à des fins de sécurité et cybersécurité. Cette tendance a été confirmée par Pelle Jakovitz de l'IoT Lab. En dépit de quelques exceptions (caméras et alarmes

antivols), ce sont les plus grandes entreprises qui mobilisent le plus de solutions IdO – et souvent de diverses natures.

2. Existe-t-il une politique publique dédiée portant sur l'IdO ?

a. L'IdO n'est pas l'objet d'une politique dédiée mais est intégré comme outil de certaines politiques, dans le cadre de la stratégie *Digital Agenda 2020*. De la même manière, il doit permettre d'atteindre les objectifs fixés par la stratégie *Estonia 2035*, votée par le Parlement en mai 2021. Cet outil, parmi d'autres, doit notamment permettre :

- une utilisation croissante des NTIC dans les entreprises, notamment industrielles ;
- une meilleure gestion des ressources naturelles, pour limiter la pollution ;
- un meilleur accès aux informations pour le quotidien (embouteillages, travaux, éclairage en panne, consommation électrique au quotidien, qualité de l'air dégradée dans certaines rues, etc.).

Il faut toutefois noter le rôle majeur des gouvernements au tournant des années 2000, qui ont forcé l'intérêt pour ces questions. Eliko, entreprise d'IdO créée en 2004, est né parce que le gouvernement a promu tous les bénéfices qu'il était possible de retirer de l'IdO. Mais la population n'était pas forcément réceptive à ce moment, le concept restait flou. Il a donc fallu un fort soutien et une communication intense du gouvernement, alors qu'aujourd'hui celui-ci se tient davantage en retrait et compte sur l'écosystème créé pour auto-entretenir son développement.

La situation de l'IdO dans la recherche universitaire traduit bien cette perception. Le ministère de l'Éducation ne finance aucun projet d'IdO parce que c'est un projet d'IdO : il finance des projets d'IdO parce qu'ils concourent au développement industriel. L'IoT Lab de Tartu ne reçoit aucun financement direct du gouvernement, ni des autorités locales. Son budget est d'environ 15 000 euros par an, en comptant le financement indirect de l'État (bourses d'études, soutien à une étude, etc.). Toutefois, les autorités locales de Tartu sont très ouvertes à la collaboration et mettent à disposition le territoire pour des essais (voiture autonome ou *smart cities* récemment).

En Estonie, l'IdO est indissociable de la question de l'Intelligence artificielle (IA). En 2019, un groupe de travail mandaté par le ministère des Affaires économiques et des Communications a rendu un rapport sur l'état des lieux de l'IA en Estonie[1]. Il y est question des « kratts », terme introduit en Estonie pour désigner les applications concrètes de l'IA. Ce rapport pose un double objectif pour l'Estonie : généraliser l'utilisation des kratts à court terme, dans le secteur public et dans le secteur public, mais aussi développer une stratégie de long terme pour le développement de l'IA, basée sur la R & D. Dans ce cadre, le groupe préconise d'attribuer 500 000 euros annuels à un groupe de travail scientifique sur

[1] Ministère des Affaires économiques et des Communications (2019), *Report of Estonia's AI Taskforce*, mai.

l'application de l'IdO dans les processus industriels. Ce dernier point n'a pas été retenu par le gouvernement dans sa stratégie digitale 2019-2021[1].

b. S'il n'y a pas de montant précis attribué au développement de l'IdO, une partie des ressources consacrées à la transformation numérique et à la transition écologique participeront à son développement. À titre d'exemple, son plan « Facilité pour la relance et la résilience » prévoit 100 millions d'euros pour le développement de la « *greentech* ».

Les pouvoirs publics attribuent un soutien aux start-up du digital en général. Le programme « Startup Estonia », mené conjointement par KredEX et le gouvernement, aide les entrepreneurs au quotidien : pour récolter des fonds, pour établir les contacts nécessaires, pour établir un réseau, pour faciliter le recrutement de talents étrangers (*Estonian Startup Visa*[2]) et pour créer un écosystème propice aux développements des start-up. Ce qui inclut les start-up se basant sur des solutions IdO.

Dans le cadre de l'*Electricity Market Act* de 2013, le gouvernement estonien a exigé que tous les compteurs électriques soient remplacés par des compteurs intelligents. Ceci permet à chaque utilisateur de surveiller précisément sa consommation ainsi que le mix énergétique de l'électricité qu'il consomme, permettant de l'adapter au besoin. Depuis l'*Electricity Market Act* de 2013, chaque citoyen peut librement choisir son fournisseur d'énergie – notamment en se fondant sur les informations récupérées avec ces compteurs connectés.

Les pouvoirs publics mettent en place un cadre favorable à la recherche digitale, et l'IdO en profite. Mais il n'y a pas de financement direct. Il en va de même pour les entreprises : Eliko reçoit des fonds du gouvernement selon l'intérêt du projet, indépendamment de la part d'IdO dans celui-ci. C'est un problème souligné par Pelle Jakovitz de l'IoT Lab : il n'y a aucun fléchage en faveur de l'IdO. Nécessairement, cela met les projets de recherche dans l'IdO en concurrence avec les autres projets de recherche technologique (connectivité, cyber, traitement de données, etc.) au lieu de favoriser la coopération.

c. De manière plus générale, l'Estonie a mis en place un écosystème propice au développement de l'IdO : bonne couverture mobile (notamment depuis l'implantation de la 5G), éducation et sensibilisation numérique de sa population, structures de R & D dédiées aux NTIC, cadre législatif souple pour permettre les innovations. Mais il n'existe pas de cadre spécifiquement dédié à l'IdO. De même, la recherche en IdO reste aujourd'hui très segmentée : les collaborations entre universitaires et entreprises sont uniquement ponctuelles.

[1] « Estonia's national artificial intelligence strategy 2019-2021 », juillet 2019.

[2] Voir le site https://startupestonia.ee/visa.

En outre, l'IoT Lab regrette le fait que l'Estonie n'adopte plus de législation spécialement dédiée au développement des nouvelles technologies : les entreprises composent avec les règles européennes.

3. Le développement de l'IdO dans le pays a-t-il fait ou va-t-il faire l'objet de débats public ?

a. Le débat autour des données de l'IdO est le même que pour les données en général, à savoir quelle protection et quelle utilisation. Il est notamment question de laisser la possibilité aux citoyens de choisir quelles données peuvent être utilisées par l'État et par les entreprises, que ces données soient personnelles ou non. Autre débat plus général, celui du droit à l'oubli – notamment auprès des entreprises. Aucune disposition nationale ne s'ajoute à celles prévues par le RGPD.

Il n'existe presque pas de débat sur l'usage et le développement de l'IdOT. Trois explications sont ressorties de nos entretiens :

- la confiance dans les institutions et le cadre légal, qui part de l'idée que si une technologie est en place c'est qu'elle respecte les droits de chacun, notamment en matière de confidentialité ;
- l'omniprésence de l'IdO, qui est considérée comme une part courante de la vie. Pour reprendre la métaphore d'Indrek Ruiso, d'Eliko : les Estoniens ne « contestent pas le fait de porter des vêtements, pourquoi contesteraient-ils la présence d'objets connectés ? »
- Aux yeux de Pelle Jakovitz, il y a une part d'ignorance à ne pas négliger. Beaucoup de produits sont utilisés sans que la plupart des Estoniens ne cherchent à savoir ce qu'il y a derrière (exemple des montres connectées). Lorsqu'on prend la peine d'expliquer, il peut y avoir des contestations : l'exemple des *smart cities* est parlant, l'IoT Lab ayant rencontré le rejet de certains habitants qui estiment certaines technologies trop intrusives.

b. L'Internet des objets est présenté comme un facilitateur au quotidien, pour tous les citoyens et pour toutes les entreprises. Source d'économie énergétique et financière, l'IdO permettrait également d'automatiser certaines tâches à faible valeur ajoutée et/ou tâches routinières.

La mise en œuvre de l'IoT dans les chaînes de production est synonyme d'automatisation croissante, et donc potentiellement d'un besoin de main-d'œuvre plus limité. Il va également permettre d'améliorer l'efficacité des employés, mais peut laisser craindre un contrôle permanent du comportement de ces derniers.

Il y a peu de débats sur le développement des solutions IdO. Certains existent toutefois, et sont généralement portés lors de grandes consultations publiques, comme lors de l'implantation de la 5G sur le territoire. Il est également possible de faire remonter des

questions et protestations au Parlement par des pétitions et moratoires. En 2019, une pétition signée par 1 122 personnes (sur 1,3 millions d'habitants) avait conduit à une audition parlementaire sur la question du déploiement de la 5G.

c. L'impact environnemental de l'IdO est essentiellement abordé par le prisme énergétique. Les innovations de l'IdO offrent une manière de mieux contrôler la production et la consommation d'énergie, pour limiter les pertes et être efficient énergétiquement. Ceci doit permettre de réduire l'empreinte environnementale de chacun, des individus aux entreprises, dans le domaine énergétique en particulier.

d. De manière plus pragmatique, tous les interlocuteurs du service économique ont confié que l'enjeu environnemental était secondaire, l'important étant l'efficacité économique. De ce fait, les régulations plus strictes envers les solutions polluantes conduisent l'IdO à se vouloir plus vertueux, mais ce n'est pas une conscience environnementale qui guide ce changement. Par exemple, la question de la consommation des *data centers* est uniquement abordée à travers le prix de l'électricité consommée, y compris dans le monde universitaire.

4. Quelle est la prise en compte des dimensions cybersécurité et enjeux géostratégiques ?

a. L'IoT Lab souligne l'importance de la confiance dans le développement de l'IdO, et notamment en matière de confidentialité. Cela devrait être le premier prérequis au développement de toute solution, et même réflexion, IdO. Ce n'est pas le cas aujourd'hui : de nombreux produits connectés, notamment chinois, circulent sur le marché malgré un flou total sur l'utilisation des données. L'IoT Lab travaille actuellement sur les montres connectées Xiaomi et pointe le risque d'une fuite des données vers des opérateurs internationaux.

Pelle Jakovitz souligne qu'il y a depuis 2020 un intérêt croissant du cyber pour les activités de l'IoT Lab, et notamment pour les étudiants de celui-ci (cinq à six par an, suivant un parcours centré sur l'IdO). Il y a eu une prise de conscience des entreprises de cybersécurité et des agences dédiées que la cybersécurité commence par la cybersécurité des produits de tous les jours. Pour l'instant, aucune mesure concrète n'a été prise mais Pelle Jakovitz estime que cela pourrait venir rapidement si la réflexion se diffuse à travers l'UE.

Cette réflexion est bien présente au niveau gouvernemental. En effet, la *Stratégie de cybersécurité 2019-2022*, document cadre pour la planification de la cybersécurité nationale, fait figurer l'IdO comme l'un des facteurs technologique de risque pour la sécurité.

La sécurité dans le domaine de la technologie consiste en premier lieu à maintenir les logiciels à jour, mais aussi à former les agents susceptibles d'interagir avec ces nouveaux outils. Sous l'impulsion du ministère estonien de la Défense, et conjointement avec l'entreprise estonienne CybExer Technologies, depuis 2017, le gouvernement estonien a mis en place plusieurs formations et des tests à destination des agents du secteur public et du gouvernement, pour prendre la mesure des enjeux du cyberhygiène. Concernant le

secteur privé et les dirigeants d'entreprise, la cybersécurité fait l'objet d'une formation spécifique, proposée notamment par l'Estonian Business School (EBS), en collaboration avec les entreprises estoniennes BHC Laboratory et CybExer Technologies.

L'étude *Estonian Cybersecurity R&D Concept* commandée par le ministère estonien des Affaires économiques et des Communications, et produite par TalTech en 2019, met en lumière les principales caractéristiques du secteur de la cybersécurité en Estonie et les principaux enjeux identifiés, incluant la dimension liée à l'Internet des objets.

Parmi les défis identifiés dans l'étude, il est fait état :

- du besoin de sensibiliser les acteurs publics aux enjeux de cybersécurité et de confidentialité ;
- de l'éducation et de la formation au grand public ;
- de la complexité et des menaces portant sur les chaînes logistiques.

Les technologiques quantiques et la cryptographie sont deux domaines prioritaires dont l'université de Tartu s'est saisie, à travers des travaux de recherche sur l'application des outils de cryptographie quantique au contexte de cybersécurité national. Une étude de Cybernetica, entreprise estonienne pionnière dans ces recherches, mentionne l'Internet des objets (cryptographie au sein d'environnements finis) au rang des technologies les plus prometteuses pour l'Estonie.

Enfin, les sujets associés à la « criminalistique numérique » constituent une priorité politique pour l'Estonie, y compris dans les secteurs de l'IdO et du *data mining*, matérialisés par les efforts déployés dans la détection, le contrôle et l'attribution des cyber-attaques.

Enfin, il faut noter que la question est bien considérée du côté universitaire. Plusieurs groupes de réflexions sur les problématiques IdO/cybersécurité sont apparus dans les universités estoniennes ces dernières années, notamment l'université de technologie de Tallinn :

- Data Science Group ;
- High-assurance Software Laboratory ;
- Thomas Johann Seebeck Department of Electronics (TJSeebeck).

b. Le principal enjeu se situe au niveau des normes. L'Estonie se fonde sur les normes européennes (et n'en impulse plus réellement) et se confronte donc aux normes américaines et chinoises. Encore une fois, l'opposition se centre essentiellement sur les questions d'utilisation des données et de confidentialité. En revanche, il n'existe pas d'enjeu réel au sein même de l'UE : les entreprises estoniennes développent leurs solutions IdO dans n'importe quel pays européen. En évoquant la France, où ils ont travaillé avec Le Puy du Fou, Eliko pointe uniquement le surplus de formalités administratives et souhaite une harmonisation au niveau européen. Mais ce surplus ne fait que ralentir son activité, sans limiter sa diffusion.

Questionnaire : Internet des objets (IdO) – Étude de cas Lettonie

Selon les données fournies par le département des Communications électroniques du ministère des Transports, on compte actuellement 440 970 connexions M2M actives, y compris les connexions de l'Internet des objets (IdO). La répartition des connexions entre B2B et B2C n'est pas connue.

Selon le Plan national de numérotation, une numérotation spéciale à 10 et à 12 chiffres a été réservée pour les communications M2M et IdO. Afin de favoriser l'utilisation du protocole IPv6 qui permet d'augmenter le nombre d'adresses IP individuelles et d'assurer la sécurité des services, le ministère des Transports a initié le passage du protocole IPv4 au protocole IPv6 dans tous les établissements publics et municipaux.

Déploiements de l'Internet des objets par les entreprises (en % du total, source : Bureau central des statistiques[1]) :

- compteurs, lampes, thermostats intelligents pour l'optimisation de la consommation énergétique – 30,6 %.
- surveillance et contrôle de l'activité des clients (caméras, capteurs, technologies RFID) – 28 %.
- gestion des parcs de véhicules (pour suivre le trajet des véhicules, le comportement des conducteurs, l'état technique de véhicules) – 39,9 %.
- capteurs ou technologies RFID pour la surveillance des processus de production automatisés, la logistique, la gestion des stocks, etc. – 12,6 %.

En Lettonie, le développement de l'IdO est assuré par les opérateurs de téléphonie mobile, comme Tele2 et LMT, ainsi que par l'entreprise TET, opérateur de téléphonie fixe, d'Internet et de télévision.

À ce stade, aucune étude sur les tendances et les perspectives de développement de l'IdO dans le pays, ainsi que les impacts en termes de gains attendus, n'a été réalisée. Le développement de l'IdO ne fait pas pour le moment l'objet de débats publics.

[1] www.csb.gov.lv

Questionnaire : Internet des objets (IdO) – Étude de cas Lituanie

1. Quelques éléments de cadrage

Concernant la téléphonie mobile, 3 672 000 individus furent abonnés actifs à des forfaits de téléphonie mobile en Lituanie en 2020. On dénombre cette année-là 131,4 téléphones mobiles pour 100 habitants.

Concernant le haut débit d'Internet (plus de 30 Mbps), en 2020, 53,6 % de la population lituanienne y avait accès dont près du tiers disposait d'un débit supérieur à 100 Mbps.

2. Les compteurs intelligents dans le domaine de l'énergie

Après des premières démarches entreprises en 2017 et une réponse à l'appel d'offres à la fin de 2019, le groupe français Sagemcom a signé, en mai 2021, un contrat de 75 millions d'euros pour déployer 1,2 millions de compteurs électriques intelligents pour la Lituanie. Dans cette optique, Sagemcom travaillera avec l'opérateur mobile Bite Lietuva, qui intégrera les données au système d'information en utilisant les technologies de l'Internet des objets, à savoir NB-IoT et LTE-M. La NB-IoT (*narrowband Internet of things*), développée par la 3GPP, était arrivée en Lituanie par l'intermédiaire de Telia en janvier 2020. L'installation des compteurs devrait démarrer au premier trimestre 2022 pour une première phase de déploiement au niveau national achevé en 2024. Sagemcom souhaite investir aussi sur d'autres marchés en Lituanie, notamment les compteurs intelligents d'eau et de gaz.

Par ailleurs, Sigfox, une autre entreprise française, tente déjà d'investir le marché de compteurs d'eau intelligents en Lituanie et propose d'ores et déjà certaines de ses solutions à certaines municipalités. Contrairement au marché public relatif aux compteurs électriques qui a été passé au niveau national, les municipalités sont en charge des appels d'offres pour les compteurs d'eau. Sigfox Lithuania est la branche baltique (anciennement nommée 0G Baltic) de Sigfox, leader dans l'IdO grâce à son utilisation économe d'une onde très fine dite UNB (*ultranarrow band*[1]) qui offre un bas débit sur terre (0G).

3. Teltonika Group

Teltonika Group est un acteur majeur de l'IdO en Lituanie, fournissant des objets électroniques et des solutions connectées en surveillance et en transport « made in Lithuania ». Le groupe emploie actuellement 2 000 salariés et prévoit d'obtenir en 2021 un

[1] Réseau de télécommunication à bande ultra étroite.

CA de 215 millions d'euros (soit plus du double du CA de 2020) pour un bénéfice net d'environ 50 millions d'euros.

Teltonika envisage d'investir 3,7 milliards d'euros dans la fabrication domestique de puces électroniques, de semi-conducteurs et de microplaquettes d'ici à 2030. À cette fin, des usines et laboratoires employant jusqu'à 8 000 ouvriers et chercheurs devraient voir le jour, ce qui permettrait de sécuriser leur chaîne d'approvisionnement aujourd'hui largement dépendante de la Chine et de Taiwan.

4. La 5G

Outre l'objectif annoncé de la mise en service de la 5G dans les cinq grandes villes du pays pour 2023, la Lituanie a des ambitions supplémentaires à l'horizon 2025 sur le déploiement de la 5G. L'ensemble des ménages lituaniens devront avoir accès à un débit au moins égal à 100 Mbps quand aujourd'hui plus de 30 % de la population n'a toujours pas accès à 30 Mbps de débit. Les institutions et entreprises travaillant dans le secteur IT devront avoir un débit d'au moins 1 Gbps. Enfin, 95 % du territoire lituanien devrait être couvert par la 5G en 2030.

L'appel d'offres public pour l'utilisation des bandes 713-733 MHz et 768-788 MHz est lancé depuis janvier 2021. Le réseau mobile devra donc commencer à être déployé en 2022. La vice-ministre, Mme Vaiciukeviciute, a signalé que les bandes à 3,5 GHz seront tout de même mises aux enchères prochainement malgré l'absence de solution trouvée avec la Russie, qui utilise cette fréquence pour ses équipements militaires et dont l'étendu couvre une partie importante du territoire lituanien.

Étude de cas : la Finlande

Ambassade de France en Finlande Helsinki, le 16 novembre 2021

Service économique de Helsinki

Questionnaire : Internet des objets (IdO) – Finlande

1. Quelle est l'ampleur du développement de l'Internet des objets ?

La tendance générale est à la forte prévalence de l'IdO. Il y a de nombreuses applications IdO et d'interfaces de télécommunications différentes dans le secteur de la consommation (alarmes antivol et incendie dans les chalets et les habitations, caméras, contrôles de température) mais également dans l'industrie et plus de 99 % des clients des sociétés d'électricité en Finlande ont un compteur électrique dit intelligent. La dernière nouveauté de l'IdO est le développement des trottinettes électriques.

La Finlande compte de nombreuses sociétés d'IdO industrielles qui fournissent des solutions aux entreprises (solutions de fabrication, des technologies intelligentes pour la production et gestion d'énergie efficace, et pour surveiller, automatiser et optimiser les flux d'énergie dans la production, les bâtiments intelligents, la santé et le bien-être)[1].

Les applications de l'Industrie 4.0 et 5G sont supportées par des écosystèmes d'entreprises et des partenariats public-privé.

Utilisation par les consommateurs

L'Agence finlandaise des transports et des communications (Traficom) réalise des études consommateurs sur le sujet. Selon les statistiques de mai 2021, 64 % (contre moins de 50 % en 2018) des foyers ont au moins un appareil connecté à Internet (le plus souvent une Smart TV). 23 % ont des jeux et équipements sportifs, 21 % des équipements liés à la santé mais seulement 5 % des Finlandais ont des appareils électroménagers connectés à l'Internet (Annexe 1).

Le nombre des cartes SIM M2M (*machine to machine*) est l'indicateur IdO des opérateurs télécoms. Il y en avait 1,8 million au printemps 2021 en Finlande et la croissance paraît lente (1,7 million au printemps 2020). Ces chiffres incluent l'équipement des postes de guichet.

[1] https://www.businessfinland.fi/en/do-business-with-finland/explore-key-industries/ict-digitalization/intelligent-connectivity

Utilisation par les entreprises

40 % des entreprises finlandaises comptant au moins 10 employés utilisent des appareils ou des systèmes qui peuvent être contrôlés ou gérés via Internet[1]. Cependant, l'utilisation de ces systèmes est encore inégale, variant selon la taille de l'entreprise.

L'utilisation de l'IoD (*Internet of Data*) est beaucoup plus élevée parmi les grandes entreprises (avec au moins 100 employés), où elle est passée à 52 %. Parmi les plus petites entreprises (de 10 à 19 salariés), 34 % ont intégré l'IoD dans leurs processus quotidiens.

Les entreprises finlandaises utilisent le plus souvent les outils et systèmes basés sur Internet pour surveiller la sécurité des locaux commerciaux (dans 31 % des cas) et dans la logistique (14 %). L'IoD a également été relativement souvent utilisé dans la maintenance conditionnelle (12 %), la gestion de la consommation d'énergie (12 %) et le processus de production (10 %). En lien avec le service client, l'Internet des objets est utilisé par 6 % des entreprises.

Utilisation par l'industrie

L'Internet des objets est utilisé de manière assez uniforme, dans la plupart des secteurs, entre 40 et 48 % des entreprises. Mais il est moins utilisé que dans d'autres dans la construction (27 %) et les activités professionnelles, scientifiques et techniques (32 %).

L'utilisation de l'IoD pour surveiller la sécurité des locaux commerciaux est plus courante dans les industries du commerce de gros (40 %) et du commerce de détail (39 %). En logistique (33 %) et en maintenance conditionnelle (20 %), l'IoD est le plus couramment utilisé dans l'industrie du transport et du stockage. Dans la gestion de la consommation d'énergie, l'utilisation de ces systèmes est la plus répandue dans la fabrication (17 %) et le commerce de détail (17 %) et dans le processus de production dans le secteur manufacturier (20 %).

En lien avec le service client, l'Internet des objets est le plus utilisé dans les activités de services administratifs et de support (9 %) et dans le commerce de détail (8 %).

Un réseau IoD

Connected Finland[2] offre un réseau mobile national conçu uniquement à des fins de l'Internet des objets. Le réseau fait partie de l'écosystème mondial Sigfox[3] (français) et Connected Finland agit en tant qu'opérateur local exclusive en Finlande. Sigfox atteint

[1] Données recueillies par Statistics Finland lors d'une enquête au printemps 2020 (« Forty per cent of enterprises have the Internet of Things in use », décembre 2020).

[2] Voir sur le site de Connected Finland.

[3] Sigfox est le plus grand écosystème IdO au monde et est déjà disponible dans 75 pays.

90 % des Finlandais et la zone de couverture du réseau sera encore étendue. Les applications particulièrement populaires sont les différents types de mesures liées aux propriétés, telles que la température de l'air et l'humidité relative, la teneur en CO_2 et d'autres mesures de qualité de l'air, ainsi que la gestion des locaux. Fin 2020, le nombre d'appareils sur le réseau finlandais Sigfox avait dépassé les 200 000 appareils.

Ces appareils, qui fonctionnent avec des piles, ne sont pas directement connectés à l'Internet mais transmettent ponctuellement les données (la quantité des données transmis est très faible) à des stations de base, après quoi les données continuent à circuler via Internet. Ainsi ils utilisent beaucoup moins d'énergie et ne sont pas assujettis aux mêmes questions de cybersécurité que l'IoD, dans lequel les appareils sont directement connectés à l'Internet. Ils opèrent sur de basses fréquences sans licence, mais dont l'utilisation est régulée par l'organisme de normalisation ETSI (Traficom en Finlande).

5G non cellulaire pour l'IoD d'entreprise

L'entreprise Wirepas dit avoir la première technologie de connectivité 5G non cellulaire[1] au monde pour l'IoD d'entreprise qui fonctionne sur des fréquences gratuites. Cette 5G non cellulaire et non opérée entend répondre aux besoins des réseaux IdO à très forte densité avec un coût modique et une empreinte environnementale réduite[2].

2. Existe-t-il une politique publique dédiée portant sur l'IdO ?

Il n'existe pas de stratégie spécifique dédiée à l'IdO. La Finlande attend semble-t-il le développement d'un cadre commun européen sur ce sujet.

Soutien au développement du réseau large bande et de la 5G

Même s'il n'y a pas de politique publique dédiée à l'IoD, son développement est **indirectement soutenu** par des subventions au développement du réseau large bande (câbles de fibre optique) dans les zones rurales ainsi que par des subventions liées au développement du réseau 5G (permis et financement de la R & D).

Un programme de soutien gouvernemental a été mis en place en 2010 pour accélérer la construction d'un réseau à haut débit (câbles de fibre optique) dans les zones et municipalités rurales où il n'y a pas d'accès à Internet à haut débit commerciale (et ou la construction n'est pas possible aux conditions du marché). La *Stratégie d'infrastructure numérique 2025* prévoit 135 millions d'euros pour des subventions publiques pour le haut

[1] Norme ETSI TS 103 636 series, plus connue sous l'appellation « DECT-2020 NR ».

[2] Coutance P. (2021), « La 5G non cellulaire et non opérée de Wirepas obtient la certification de l'UIT », *VIPress.net*, 21 octobre.

débit (69,50 millions d'euros de l'État, le reste venant des municipalités et des Centres ELY[1]).

Les connexions à large bande sont également financées par le Fonds de développement rural de l'UE (Feader) depuis des années, mais le soutien est principalement axé sur les projets de réseaux villageois. Le Feader ne finance donc pas le programme national de soutien à haut débit. Seize millions d'euros provenant du Feader seront dédiés à la construction d'un réseau à haut débit dans les prochaines années.

Soutien au R & D

Business Finland[2] et l'Académie de la Finlande soutiennent le développement de produits et la recherche. *The Connected Intelligent Industries Finland program (2015-2019)* de Business Finland visait à soutenir la collaboration entre les PME, les grandes entreprises et les organismes et institutions de recherche. Actuellement, en plus des activités propres des entreprises, de nombreuses initiatives nationales cherchent à faire avancer la numérisation de l'industrie (Annexe 1).

Les procédures d'autorisation d'utilisation de fréquences par les opérateurs de télécommunications sont facilitées. Des bandes de fréquence pour les tests de 5G ont été accordé très tôt en Finlande et les universités de Turku, Helsinki, Tampere et d'Oulu ont ce genre d'environnements d'essai et de test dans leurs propres locaux[3]. Désormais, une partie des subventions au titre du Fonds de relance est spécifiquement destinée à la recherche 5G/6G, aux environnements de test et au développement du réseau large bande dans les zones rurales.

La 5G est considérée comme importante et est promue aussi bien par des acteurs privés (opérateurs de télécommunications et Nokia) que par l'État[4].

Internet industriel des objets

Il y a également plusieurs écosystèmes d'entreprises et des PPP qui cherchent à faire avancer l'IIdO (Internet industriel des objets), l'Industrie 4.0 et la fabrication avancée, notamment :

- Reboot IoT Factory ;

[1] Centres régionaux pour le développement économique, les transports et l'environnement : https://www.ely-keskus.fi/en/web/ely-en

[2] Business Finland est l'agence gouvernementale de financement de la recherche dépendant du ministère des Affaires économiques et de l'Emploi de Finlande.

[3] Cf. le réseau de tests 5GTNF (5G test Network Finland).

[4] Selon une enquête de Prior Consulting Oy (automne 2020) les investissements dans la technologie 5G augmenteraient régulièrement chaque année dans les entreprises et organisations finlandaises : une croissance annuelle d'environ 50 % par rapport à l'année précédente serait la tendance depuis 2018. Nokia investi actuellement massivement dans la 5G.

- SuperIoT ;
- Finnish Industrial Internet Forum Finnish Industrial Internet Forum ;
- Digital, Internet, Materials & Engineering (DIMECC)[1] ;
- Finnish Advanced Manufacturing Network (FAMN).

La stratégie pour le renouveau de l'industrie (juin 2021)

La stratégie finlandaise pour le renouveau de l'industrie contient un chapitre sur la digitalisation. Elle note que « les investissements et les activités de RDI liés à la numérisation avancée se concentrent sur un petit nombre de grandes entreprises et de startups en Finlande » et que l'investissement numérique de la grande partie du secteur industriel n'est pas au niveau des pays de référence. Pourtant la quatrième révolution industrielle nécessite l'utilisation des technologies numériques à différents stades de création de valeur. Ainsi, la **stratégie propose la création d'un programme d'investissement soutenant *Advanced Manufacturing* pour permettre la percée de nouvelles technologies de pointe, tel l'IdO, et l'utilisation des données dans les entreprises, en particulier les PME**.

La réglementation

Il n'y a pas de législation spécifique dédiée à l'IdO. Selon Traficom, il n'est pas nécessaire de réglementer les technologies individuelles, mais leurs effets et leurs utilisations doivent être réglementés.

Indirectement, le décret sur les compteurs électriques intelligents, par exemple, concerne l'IdO.

3. Le développement de l'IdO dans le pays a-t-il fait ou va-t-il faire l'objet de débats publics ?

En Finlande, les données de l'IdO n'ont pas vraiment fait l'objet de débat. Le public et les politiques s'intéressent davantage, par exemple, à des données de type Facebook, les données collectées par les magasins, et les données de santé. Cependant les risques liés à la protection de la vie privée sont reconnus (qui conserve les données ? et que fait-on avec ?), tout comme le sujet du piratage des objets ménagers connectés.

Transformation sociale

La révolution des soins de santé et la télémédecine ainsi que la révolution des soins aux personnes âgées sont considérées comme des changements importants à venir – notamment les technologies de soins aux personnes âgées à domicile pour éviter les

[1] DIMECC (s.d.), « IIOT meets 5G – Introduction to the topic. Antti Karjaluoto, DIMECC Ltd. ».

placements dans des établissements de santé. Dans le domaine industriel, les connexions vidéo vont réduire les déplacements et la télémaintenance devient plus fréquente.

La digitalisation de l'industrie va changer les processus de production et implique à la fois une reconversion professionnelle des travailleurs et l'emploi de beaucoup de nouveaux experts, or il existe déjà une pénurie d'experts en matière de données et d'IoD en Finlande.

L'IdO permettrait également le développement d'une économie de plateforme fondée sur Internet et la location de divers équipements payés selon leur utilisation.

La Finlande est consciente que les effets positifs de l'IdO (réduction de consommation ou l'usage plus efficace de l'eau et de l'électricité avec des capteurs, par exemple) nécessitent de la connectivité et des appareils auxquels tout le monde n'aura pas d'accès. L'IdO pourrait augmenter l'inégalité sociale.

L'impact environnemental

Les questions environnementales de l'IdO ne font pas l'objet de discussions en Finlande mais, en général, on parle de l'empreinte CO_2 du secteur technologique. 85 % de l'électricité produite en Finlande est déjà décarbonée[1]. Cela influencerait les attitudes, tout comme le fait que peu de gens pourraient imaginer la vie sans ordinateurs et d'autres technologies.

La Finlande est d'avis que les TIC ont beaucoup de potentiel pour réduire les émissions dans le secteur de l'énergie[2]. Le gouvernement vise notamment l'électrification de l'industrie et des transports pour réduire les émissions de la Finlande et souligne que cette électrification nécessite des systèmes de mesure et de contrôle efficaces qui reposent fortement sur les TIC.

Selon l'Institut de recherche sur l'économie finlandaise (Etla), le secteur des TIC représente environ 1 % à 2 % de la consommation totale de l'électricité de la Finlande, mais la majorité des émissions TIC du pays sont générées en dehors de ses frontières[3]. Ainsi, une part importante des services numériques utilisés quotidiennement par les organisations et les consommateurs finlandais sont produits dans des centres de données situés à l'étranger.

[1] Selon l'Association finlandaise de l'industrie de l'énergie, les énergies renouvelables représentaient 51 % de la production d'électricité de la Finlande, l'énergie nucléaire 34 % et les fossiles et la tourbe 14 % (2020).

[2] Ministère des Transports et des Communications de Finlande (2020), *ICT:n rooli kasvihuonekaasupäästöjen vähentämisessä energia-alalla (Le rôle des TIC dans la réduction des émissions de gaz à effet de serre dans le secteur de l'énergie)*.

[3] Etla (2021), *Energy and Electricity Consumption of the Information Economy Sector in Finland*, rapport, janvier.

La gestion des eaux

La gestion des eaux en Finlande est sur le point d'être numérisée et de nombreuses installations d'alimentation d'eau ont commencé à remplacer leurs anciens compteurs par **compteurs d'eau électrique intelligents**. *Allied ICT Finland (AIF) Water Ecosystem* est un projet FEDER (370 000 euros) créant de nouveaux outils et modèles d'analyse pour le traitement des données à utiliser dans les usines de traitement des eaux afin de **développer la gestion du réseau d'eaux usées** et de détecter les blocages et les fuites dans le réseau. Le projet vise à réduire les dommages environnementaux, la consommation d'énergie et les émissions du processus des stations d'épuration. Nokia dirige un projet *Smart Water Management* (SWIM[1]).

Intelligence artificielle

En Finlande, l'IdO est une question d'intelligence artificielle[2] et le gouvernement actuel cherche des moyens pour profiter de l'intelligence artificielle en pratique (comment en tirer des avantages environnementaux positifs). Cela notamment dans les domaines d'efficacité énergétique des bâtiments (optimisation de la capacité de chauffage) et la logistique (transport de conteneurs) et plus généralement à des fins d'anticipation dans le domaine de maintenance (intervention avant rupture ou dommage de l'équipement). Les entreprises parlent également des impacts positifs de l'IdO sur l'environnement.

Stratégie climat et environnement pour le secteur des TIC (mars 2021)

La récente *Stratégie climat et environnement pour le secteur des TIC* en Finlande recommande des mesures pour une infrastructure des TIC et une économie des données respectueuses du climat et de l'environnement.

La stratégie comprend six objectifs (et énumère des mesures à prendre pour les atteindre) :

1. Efficacité énergétique des infrastructures TIC et sources d'électricité sans carbone
2. L'économie des données respectueuse du climat
3. Durée de vie plus longue des équipements et circulation des métaux précieux
4. Vue d'ensemble des impacts environnementaux de la numérisation
5. Les consommateurs conscients de l'impact environnemental

[1] Business Finland (2021), « Data, digitalization and IoT transform water management in Nokia's leading company project », juin.

[2] Le programme IA 4.0 de la Finlande combine les technologies IA avec d'autres technologies numériques, tel IdO. Voir ministère des Affaires économiques et de l'Emploi de Finlande (2020), « Artificial Intelligence 4.0 programme to speed up digitalisation of business », communiqué de presse, novembre.

6. Utilisation des technologies émergentes dans le travail climatique et la protection de l'environnement

4. Quelle est la prise en compte des dimensions cybersécurité et enjeux géostratégiques ?

Selon Traficom, le besoin de cybersécurité augmente à mesure que le nombre d'appareils connectés à Internet augmente. Les risques les plus importants seraient les cyberattaques, la performance du réseau et le grand nombre d'appareils non sécurisés sur le réseau connectés au cloud et la conservation des données.

Les sources interrogées à propos de cybersécurité ont dit que les risques identifiés font l'objet de discussions, notamment dans les milieux professionnels. Les systèmes IdO existants auraient des installations sur site et n'utiliseraient aucun service cloud. Il existe de nombreux acteurs de sécurité informatique en Finlande qui sont des leaders mondiaux dans leur domaine (comme F-Secure).

Violation des données

Selon Etla[1], le nombre de violations de données (piratage informatique, interférence avec les systèmes d'information et violations de la vie privée) a doublé en quelques années. On estime que le coût financier des cyberattaques augmente encore plus rapidement. Cependant, il n'y aurait pas de compréhension précise des effets économiques des cybermenaces sur l'économie finlandaise. On sait peu de choses sur la cybersécurité dans les micro-entreprises.

Alors que le niveau de cybersécurité dans les entreprises finlandaises est supérieur à la moyenne européenne, la Finlande est, selon Etla, à la traîne des principaux pays selon de nombreux indicateurs différents. Les fuites de données en particulier semblent être particulièrement difficiles pour les entreprises finlandaises. Il y aurait également une pénurie de main-d'œuvre qualifiée en cybersécurité.

Secteurs critiques

Un rapport du ministère de la communication[2] (février 2021) propose des modifications législatives et d'autres mesures pour améliorer la sécurité de l'information et la protection des données dans les secteurs critiques de la société, notamment dans les secteurs de l'énergie, transport et eau, dans lesquels il y a peu ou pas d'exigences légales, mais aussi dans le secteur de la santé. La meilleure situation en termes de sécurité de l'information serait dans les secteurs de la finance et des télécommunications.

---

[1] Etla (2020), « The New Cybersecurity Landscape – How Are Finnish Companies Faring? », décembre.

[2] Le rapport final d'un groupe de travail sur l'amélioration de la sécurité de l'information et la protection des données dans les secteurs critiques de la société (*Final Report of the Working Group: A Well-Functioning Digital Society Will Require Investments in Information Security*, février 2021).

Le label finlandais de cybersécurité

Le Centre de cybersécurité de Traficom, qui surveille le respect des obligations en matière de protection et de sécurité des données de la loi sur les services de communications électroniques (2014), a très tôt identifié des lacunes dans la sécurité des appareils intelligents connectés au réseau des consommateurs.

Le rapport sur l'état de cybersécurité du Centre (2018) a montré qu'il y avait de plus en plus d'appareils non sécurisés sur le réseau et que plus de la moitié de ces appareils non sécurisés était des appareils IdO, notamment des appareils d'automatisation des bâtiments[1] et de l'électronique grand public (Annexe 2). Le Centre a alors voulu agir et a développé un label de cybersécurité.

En novembre 2019, le centre est devenu la première autorité au monde à créer un label de cybersécurité (*Finnish Cybersecurity Label*[2]) pour les appareils IdO grand public.

Le label est accordé aux appareils ou services intelligents connectés ainsi qu'aux applications qui répondent aux exigences de sécurité de l'information définies par le centre de cybersécurité national. Le label est principalement destiné aux appareils intelligents grand public (les téléviseurs intelligents, les bracelets intelligents et les routeurs domestiques). La Commission européenne préparerait une initiative européenne dans ce sens[3].

L'application *112* et le *Cyber Weather* pour informer les citoyens

Les citoyens sont, depuis octobre 2021, informés des principaux incidents et événements liés à la sécurité de l'information via l'application *112 Finlande*[4].

Le Centre de cybersécurité publie également des informations météorologiques mensuelles (*Cyber Weather*) donnant une mise à jour sur les principaux incidents et phénomènes de sécurité de l'information du mois.

[1] Généralement, ces systèmes contrôlent la ventilation, le chauffage, l'éclairage ou le contrôle d'accès automatique d'un bâtiment.

[2] Le label utilise la norme ETSI EN 303 645.

[3] La directive équipements radioélectriques 2014/53/UE permettrait de définir des exigences de sécurité pour les équipements radioélectriques.

[4] Traficom (2021), « Citizens informed about major information security incidents and events via the app 112 Suomi », novembre.

Annexes – Perspectives de développement de l'Internet des objets : enjeux environnementaux et sociaux en Finlande

Annexe 1 – Initiatives nationales cherchant à faire avancer la numérisation de l'industrie

Business Finland soutient, de plusieurs manières, les entreprises dans la numérisation. Le programme *Sustainable Manufacturing Finland* est particulièrement pertinent pour l'industrie. Au cœur du programme sont la croissance par le renouvellement des entreprises et le développement de la valeur des exportations. Le programme vise à améliorer la compétitivité de la production des entreprises en développant des chaînes de valeur commerciales et des processus de fabrication, par exemple avec la numérisation et les nouveaux modèles économiques.

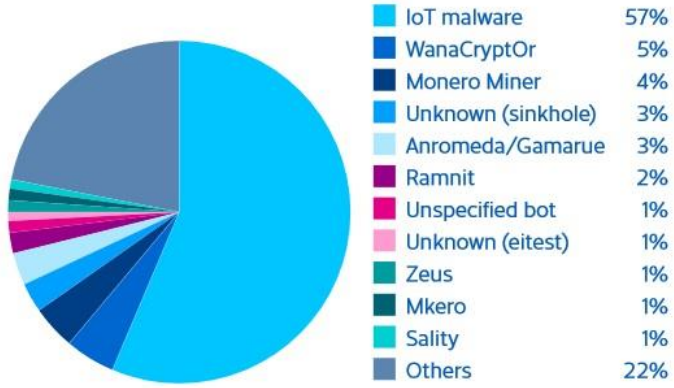
Business Finland gère également un important programme *AI Business,* dont l'objectif est de faire de la Finlande le meilleur endroit au monde pour développer et utiliser l'intelligence artificielle et l'économie de plateforme dans les affaires. Le financement se concentre sur les technologies qui comblent les lacunes des technologies d'intelligence artificielle existantes, le traitement du langage naturel, l'interaction optimisée entre l'homme et l'intelligence artificielle, les nouveaux modèles commerciaux dans l'économie des plateformes et l'application de l'intelligence artificielle à de nouveaux domaines.

Le programme phare de l'Académie de Finlande soutient la recherche de haute qualité. Parmi les principaux fleurons du programme Intelligence artificielle 4.0 et de l'industrie manufacturière figurent le Centre finlandais d'intelligence artificielle (FCAI), l'Accélérateur d'intelligence artificielle (FAIA) et l'Initiative phare des technologies de réseau sans fil (6G Flagship).

Le projet IHAN[1] de *Finnish Innovation Fund* (Sitra) construit un modèle européen d'économie de données équitable qui combine l'humain, la confiance et les principes d'une croissance durable.

Les réseaux et clusters de collaboration en cours, tels que Sustainable Industry X (SIX), fournissent des outils pratiques pour accélérer la numérisation des entreprises et la mise en œuvre des plans stratégiques au niveau national.

Annexe 2 – Les logiciels malveillants détectés en 2018



Note : les logiciels malveillants IdO représentaient près de 60 % de tous les malwares détectés en 2018.

Source : Centre de cybersécurité de Traficom (2019), Information Security in 2018*, janvier, p. 12*

[1] Ihan.fi est une plateforme expérimentale et une boîte à outils pour construire des services conformes à une économie de données équitable.

Étude de cas : l'Inde

Service économique de New Delhi Delhi, le 15 novembre 2021

Questionnaire : Internet des objets (IdO) – Inde

1. Quelle est l'ampleur du développement de l'Internet des objets ?

Le projet de politique sur l'Internet des objets publié en 2015 par le ministère indien de l'Électronique et des Technologies de l'information (MeitY) définit l'IdO comme « un système de réseau connecté d'objets / dispositifs intégrés, avec des identifiants, pour lesquels la communication sans aucune intervention humaine est possible en utilisant des protocoles de communication standards et interopérables[1] ».

D'après une étude de juin 2020 intitulée *India – Emerging Hotbed of IoT Opportunies* du cabinet de conseil Zinnov, l'Inde avait 200 à 250 millions d'objets connectés fin 2019 et le nombre d'objet connectés serait multiplié par dix en deux ans pour atteindre deux milliards d'équipements en 2021. De même, les investissements indiens dans l'IdO passeraient de 5 milliards de dollars en 2019 à environ 15 milliards en 2021, portés par trois secteurs : (i) l'industrie manufacturière, (ii) l'automobile et les transports, et (iii) l'énergie. Environ 60 % à 70 % de ces investissements concernent les objets connectés eux-mêmes (logiciels et électronique), et le solde les services associés à l'IdO. En termes d'usages, 20 % à 25 % des investissements ciblent l'industrie du futur (« Industrie 4.0 »), tandis que les produits connectés et la logistique représentent chacun 15 % à 20 % du total, et les travailleurs connectés 5 % à 6 %. L'industrie indienne de l'IdO devrait connaître un taux de croissance annuel moyen de 13,2 % jusqu'en 2035[2].

Dans son rapport *State of IoT – The Post Pandemic Resurgence* publié en août 2021, NASSCOM, la principale association professionnelle indienne du numérique, estime qu'outre l'industrie manufacturière et la logistique, l'agriculture, les sciences de la vie et l'industrie pharmaceutique adopteront rapidement l'IdO. Concernant l'innovation, 5 000 brevets sur l'IdO ont été déposés en Inde entre 2014 et 2019, plus de 480 start-up indiennes travailleraient sur le sujet, et les entreprises indiennes fabriquant des objets intelligents devraient déployer en 2021 des solutions de surveillance et de diagnostic à distance (*remote monitoring and diagnostic* – RM & D) afin valoriser les données collectées.

---

[1] « *IoT is a seamless connected network of embedded objects/devices, with identifiers, in which M2M communication without any human intervention is possible using standard and interoperable communication protocols*. » La définition complète est disponible ici.

[2] Voir l'article « Growth Opportunities in the Indian Internet of Things (IoT) Market 2021: IoT Optimizes the Omnichannel Experience and Supply Chain in Retail », *Yahoo!Finance.com*, 30 septembre 2021.

À moyen terme, les principales tendances identifiées par NASSCOM sont :

- **l'IdO interconnecté pour l'industrie**, notamment la numérisation des chaînes logistiques et la maintenance prédictive afin d'améliorer l'efficacité opérationnelle et la compétitivité de l'industrie indienne à l'export ;
- **les villes intelligentes** pour l'optimisation des transports et de la consommation d'énergie en temps réel, et le management intelligent des déchets ;
- **le traitement des données en périphérie du réseau** (*edge computing*) ;
- **l'optimisation du management des flottes de véhicules** ;
- **l'optimisation des infrastructures et le management de l'énergie.**

Selon les dernières estimations, la 5G ne devrait pas être lancée en Inde avant mi-2022, voire 2023[1]. Toutefois, les principaux opérateurs téléphoniques ainsi que des grandes entreprises et des PME ont déjà lancé des solutions IdO en Inde :

- depuis 2016, Tata Communications déploie un réseau dédié à l'IdO reposant sur la technologie LoRaWAN, couvrant 40 villes et 219 millions de personnes en juin 2019. Ce déploiement est réalisé en collaboration avec l'entreprise française Kerlink, spécialiste des solutions IdO pour les villes intelligentes ;
- en février 2018, le premier opérateur téléphonique indien, Reliance Jio, et Samsung ont annoncé un partenariat[2] pour déployer un réseau IdO en bande étroite (NB-IdO) en Inde et le développement de cas d'usage, notamment sur le suivi des véhicules, les appareils ménagers connectés, les compteurs intelligents et la surveillance ;
- en avril 2021, le deuxième opérateur téléphonique Bharti-Airtel a lancé Airtel IoT, une plateforme intégrée permettant de connecter et contrôler des objets connectés en grand nombre. La plateforme est construite pour la 5G, et compatible avec 4G, 2G et NB-IoT, via l'utilisation de la technologie e-SIM.
- au lendemain de l'annonce de Bharti-Airtel, le troisième opérateur indien, Vi, a également annoncé[3] des solutions IdO compatibles avec la 5G, à destination des entreprises de l'industrie, des bâtiments intelligents, de la mobilité et de l'énergie.
- la PME indienne SenRa Tech s'est associée en juin 2021 avec l'entreprise française Actility pour déployer des solutions LoRaWAN pour les villes intelligentes, l'industrie, les bâtiments intelligents et la logistique en Inde et dans le monde.

[1] Voir l'article « 5G Delay can still be an opportunity for India » de *TelecomTalk* en date du 9 novembre 2021.

[2] Voir l'article « Reliance Jio partners with Samsung to bring IoT to India, take LTE to 99% population by Diwali » de *BusinessToday.In* en date du 27 février 2018.

[3] Voir l'article « Vodafone-Idea launches 5G-ready IoT solution for enterprises » de *Mint* en date du 8 avril 2018.

2. Existe-t-il une politique publique dédiée portant sur l'IdO ?

Le gouvernement indien a lancé en 2015 la politique publique *Digital India* visant à donner accès à internet à l'ensemble des citoyens indiens via la construction d'infrastructures numériques, à promouvoir la numérisation des services publiques, ainsi que la production locale de produits électroniques.

Dans ce cadre, plusieurs feuilles de routes et politiques publiques contribuant au développement de l'IdO ont été lancées :

- En mai 2015, le ministère des Télécommunications (Department of Telecommunications – DoT) a publié une feuille de route nationale sur la télécommunication d'objet à objet (M2M) couvrant les volets normatifs, réglementaires et de politiques publiques et formulant plusieurs recommandations, dont certaines ont déjà été mises en œuvre :
  - mettre en place un comité rassemblant toutes les parties prenantes ;
  - soutenir la normalisation des communications M2M, notamment concernant la cryptographie, la qualité, la sécurité et le respect de la vie privée ;
  - publier un plan de numérotation national M2M ;
  - traiter les questions relatives à la qualité de service des communications M2M, les exigences d'itinérance et de spectre spécifiques au M2M ;
  - proposer un processus d'enregistrement des fournisseurs de service M2M, et publier des directives pour les transferts de SIM, l'itinérance, etc. spécifique à l'IdO ;
  - définir les bandes de fréquence pour la communication par courant porteur de ligne (CPL) pour différentes industries ;
  - finaliser le processus de certification des produits M2M ;
  - soutenir les projets pilotes M2M ;
  - soutenir le développement des compétences ;
  - établir des centres d'innovation dédiés au M2M ;
  - soutenir les entrepreneurs indiens développant et commercialisant des produits M2M via des financements, du mentoring, etc. ;
  - ajouter les produits M2M aux produits bénéficiant d'un accès privilégié au marché ;
  - soutenir le développement des produits et services M2M auprès des ministères indiens pertinents ;
  - définir et mettre en place des procédures pour mesurer la consommation énergétique des objets connectés ;

  - mettre à jour les directives sur les émissions de rayonnement électromagnétique des objets connectés sur la base des recherches réalisées par les agences pertinentes.

- En 2015, le MeitY a publié un projet de politique IdO avec quatre objectifs : (i) développer l'industrie IdO indienne pour atteindre 15 milliards de dollars de chiffre d'affaires en 2020, (ii) soutenir la formation pour les compétences spécifiques à l'IdO pour le marché domestique et l'international, (iii) soutenir la recherche et développement, et (iv) développer des produits IdO pour répondre aux besoins indiens dans le domaine de l'agriculture, la santé, la qualité de l'eau, les catastrophes naturelles, les transports, la sécurité, l'automobile, la logistique, les villes intelligentes, les compteurs électriques, les déchets, etc. Ce projet ne s'est pas concrétisé dans une politique publique formalisée, mais certaines de ces réflexions ont été reprises par ailleurs, par exemple pour la mission Smart Cities indienne.
- La mission Smart Cities a été lancée en juin 2015 avec un budget de 5,5 milliards de dollars sur cinq ans et l'objectif de développer 100 villes intelligentes en Inde. Plusieurs composantes de la mission soutiennent le développement de l'IdO, notamment le parking intelligent, les systèmes de transport intelligents, l'e-santé, la sécurité des femmes, les réseaux intelligents, l'éclairage urbain intelligent, les déchets, la maintenance des villes intelligentes, l'affichage dynamique et l'eau.
- En septembre 2017, l'Autorité indienne de régulation des télécommunications (TRAI) a publié à la demande du DoT des recommandations sur le spectre, l'itinérance et la qualité de service dans les communications M2M.
- En mai 2018, le DoT a publié un document réglementant les caractéristiques des cartes SIM utilisées uniquement pour les services de communication M2M, et précisant les informations à recueillir préalablement à la délivrance de cartes SIM M2M fournisseurs de services de communication M2M. Ce texte comprend notamment la non-transférabilité des connexions mobiles, le fait que les appels/SMS ne peuvent provenir que d'un ensemble prédéfini de numéros, et l'obligation d'adresses IP prédéfinies pour les données. Les numéros d'urgence tels que ceux de la police et des ambulances sont exemptés de ces restrictions.
- En septembre 2018, le DoT a publié un projet de politique nationale de communications proposant six objectifs spécifiques pour l'IdO : (i) 5 milliards d'objets connectés en 2022, (ii) créer une feuille de route pour les technologies émergentes tels que la 5G, l'intelligence artificielle, la robotique, l'IdO et le cloud, (iii) simplifier le cadre réglementaire et l'obtention de licences tout en conservant des exigences appropriées de sécurité pour les services IdO, (iv) donner un numéro d'identification unique à 13 chiffres pour toutes les connexion IdO, (v) réserver des spectres pertinents, sous licence et sans licence, pour les service IdO, et (vi) développer le marché des services de connectivité IdO dans les secteurs prioritaires (agriculture,

ville intelligente, réseaux de transport, logistique, réseaux électriques, etc.) en incorporant les meilleures pratiques internationales.

- En juin 2021, le DoT a publié un projet de directive pour réglementer le processus d'enregistrement des fournisseurs de service IdO et des fournisseurs de connexions WPAN/WLAN pour les services M2M. Ce projet a fait l'objet de consultation avec les parties prenantes et est en cours d'amendement par le DoT.

3. Le développement de l'IdO dans le pays a-t-il fait ou va-t-il faire l'objet de débats publics ?

À ce stade, l'IdO n'a pas fait l'objet en Inde d'un large débat public quant aux enjeux autour des données et son impact environnemental. La protection de la vie privée est actuellement réglementée en Inde par l'Information Technology Act (ITA) de 2000, et les Information Technology (Reasonable Security Practices and Procedures and Sensistive Personal Data or Information) Rules de 2011. D'après l'article 43A de l'ITA, une entité ne mettant pas en place et ne maintenant pas des pratiques et procédures de sécurité raisonnable vis-à-vis des données ou informations personnelles possédées ou traitées par un moyen informatique est tenue de compenser toute personne qui aurait subi un préjudice de ce fait.

Toutefois, l'ITA a été jugé inadéquat par un jugement de la Cour suprême en 2017 érigeant la vie privée comme un droit fondamental et demandant le développement d'un cadre réglementaire spécifique à la protection des données. Le gouvernement indien a publié un premier projet de loi en 2018, puis une version amendé en décembre 2019. Ce projet est à l'étude depuis lors par un comité conjoint de représentants de la chambre haute et de la chambre basse du Parlement indien et pourrait être voté lors de la session d'hiver débutant fin novembre 2021. Ce projet de loi a fait l'objet de nombreux commentaires de la part de la société civile indienne et des entreprises, notamment sur la définition de ce qui constitue des données sensibles et doit être localisé en Inde, sur l'accès large donné aux agences gouvernementales aux données, sur l'inclusion de données non personnelles dans le projet de loi et sur l'indépendance et les pouvoirs de la future Autorité de protection des données. L'IdO n'a toutefois pas fait l'objet d'une attention spécifique à ce stade.

Le potentiel de **transformation sociale** de l'Internet des objets est principalement mis en avant en Inde sous la forme **du développement de l'économie et de l'industrie**[1], alors que le gouvernement indien s'est fixé l'objectif d'un PIB de 5 000 milliards de dollars en 2025, dont 1 000 milliards pour l'économie numérique et met en œuvre depuis 2014 des politiques centrées sur le développement de l'industrie domestique (*Make in India* et *Aatmarnirbhar Bharat*). L'IdO est ainsi vu comme un facteur de croissance, à même

[1] Voir par exemple l'étude de Deloitte/CII (2018), *Harnessing the power of Internet of Things to transform Industry in India*.

d'améliorer la performance de différents secteurs de l'économie, dont l'agriculture, la santé, l'énergie, la ville intelligente, l'industrie manufacturière, etc., et de fournir de nouvelles sources de revenus aux opérateurs téléphoniques.

Concernant les impacts environnementaux, la fondation Shakti en lien avec PWC et l'entité semi-publique India Smart Grids Forum a publié en 2018 une étude sur l'efficacité énergétique de l'IoT. L'étude estime la consommation énergétique des objets connectés en veille pour dix cas d'usage (ampoule intelligente, système d'éclairage urbain, irrigation, prises, compteurs, thermostats, chauffe-eaux, réfrigérateurs, télévision et systèmes de domotique) et propose des recommandations pour la réduire. À l'exception de cette étude, les autres documents identifiés se concentrent principalement sur les bénéfices de l'IdO en termes de réduction de la consommation énergétique pour certains cas d'usage. On peut citer notamment une étude de l'agence publique Bureau of Energy Efficiency en lien avec GIZ sur les bâtiments résidentiels intelligents et celle du think tank CEEW sur l'air conditionné[1].

L'Inde est le seul pays d'Asie du Sud à disposer d'un règlement spécifique sur les déchets électroniques**.** Ce règlement de 2011 fixe des règles pour le transport, le stockage et le recyclage des déchets. Il introduit également le concept de responsabilité élargie du producteur, selon lequel les fabricants de produits électroniques doivent assumer la responsabilité financière et/ou physique de la gestion de l'élimination de leurs produits en fin de vie. En 2016, les règles ont été élargies afin d'introduire des « organisations de responsabilité du producteur » visant à collecter et à recycler les déchets électroniques, ainsi que des programmes de rachat des déchets électroniques, de cautions et d'échanges. Une modification des règles en 2018 a introduit des objectifs de collecte annuels pour les producteurs : par exemple à partir de 2023 les producteurs doivent collecter au moins 70 % en masse de leurs produits arrivant en fin de vie. Toutefois, à ce jour une large partie (jusqu'à 95 %[2]) des déchets électroniques serait encore collectée et traitée par le secteur informel en Inde.

Par ailleurs, le gouvernement indien a publié ces dernières années plusieurs études sur la promotion de l'efficacité énergétique et de l'économie circulaire, mais sans cibler spécifiquement l'IdO :

– une étude de juin 2017 du think tank gouvernemental NITI Aayog et de la délégation de l'Union européenne en Inde sur l'efficacité en matière de ressources, suivie par la

[1] Bureau of Energy Efficiency/GIZ (2021), *Report on National Policy Roadmap for Home Automation Technologies for Residential Energy Efficiency*, juillet et CEEW (2021), *Internet of Things and its Impact on India's Air-Conditioning Servicing Landscape*, octobre.

[2] GIZ (2017), *Building the Link: Leveraging Formal-Informal Partnerships in the Indian E-Waste Sector*, octobre.

publication en janvier 2019 d'une étude intitulée *Resource Efficiency & Circular Economy – Current Status and Way Forward* ;

- la publication en 2019 par le ministère de l'Environnement, des Forêts et du Changement climatique d'un projet de politique sur l'efficacité en matière de ressources ;
- la publication en 2019 par la TEC d'un « code de bonnes pratiques volontaire pour un secteur telecom soutenable » à destination des fournisseurs de services de télécommunication et incitant à développer des solutions de long terme pour réduire l'empreinte carbone et optimiser la consommation d'énergie ;
- l'étude de mai 2021 du MeitY visant à développer l'économie circulaire des produits électroniques et électriques.

Des initiatives sont également mises en place au niveau local, telle la municipalité du sud de Delhi qui a lancé en juin 2021 un portail en ligne afin de collecter les déchets électroniques, en rémunérant les habitants en fonction du type d'objet.

4. Quelle est la prise en compte des dimensions cybersécurité et enjeux géostratégiques ?

L'Inde est particulièrement ciblée par les attaques cyber, en constante augmentation ces dernières années du fait, entre autres, de la numérisation grandissante de l'économie. Le Data Security Council of India estime qu'entre 2016 et 2018 l'Inde était le deuxième pays du monde le plus affecté par des cyberattaques[1]. Ces attaques s'inscrivent également dans un contexte de tensions géopolitiques avec certains pays voisins. Ainsi, au printemps 2020 au plus fort des tensions indo-chinoises l'Inde a observé une augmentation de 86 % du nombre de cyberattaques[2] et la moitié d'entre elles utilisaient l'IdO comme porte d'entrée. Quelques mois plus tard, la ville de Mumbai, capitale économique du pays, a subi en octobre 2020 une coupure de courant géante, causée d'après l'entreprise américaine spécialisée dans la cybersecurité Recorded Future par une cyberattaque menée par une entité liée au gouvernement chinois[3].

Afin de lutter contre le risque cyber, le MeitY a publié en 2013 une politique nationale en matière de cybersécurité avec pour objectif de construire un cyberespace sécurisé et résilient pour les citoyens, les entreprises et le gouvernement. Cette politique nationale vise la création d'un écosystème de la cybersécurité en Inde (dont la création d'une agence

[1] DSCI (2020), *National Cyber Security Strategy 2020*, Data Security Council of India.

[2] Voir l'article « India needs IoT security standards » du *Financial Express* en date du 2 novembre 2020.

[3] Voir l'article « Did Chinese hackers cause Mumbai's power failure in October? » de *Wire* en date du 1er mars 2021.

nationale dédiée – le National Cyber Coordination Centre (NCCC) – en 2014), le développement d'un cadre normatif (notamment les normes ouvertes) et réglementaire, le développement de mécanismes de détection des attaques en temps réel, le développement des compétences, etc. Cette politique nationale doit faire l'objet d'une mise à jour par le NCCC, initialement annoncée pour 2020, mais qui n'a pas encore été publiée à date de novembre 2021.

L'agence publique sous tutelle du DoT en charge des normes et spécifications pour le secteur des télécommunications en Inde, le Telecommunication Engineering Centre (TEC), a publié en 2019 un rapport présentant des recommandations sur les principes de sécurité par construction *(security by design*) pour les objets de l'IdO. Ces recommandations identifient les défis suivants pour les objets connectés :

- les objets connectés peuvent être installés dans des **environnements peu sécurisés** permettant un accès physique ;
- **les fabricants d'objets connectés n'ont pas forcément une grande expérience des enjeux de sécurité**, qui ne font pas forcément l'objet d'une attention particulière lors du développement des objets ;
- les objets connectés ont généralement des **ressources limitées** (mémoire, capacité de calcul, alimentation électrique), ce qui limite les dispositifs de sécurité pouvant être mis en œuvre ;
- **le développement d'une « racine de confiance »** (*root of trust*) sur les objets connectés ;
- **la fragmentation des normes et règlements** ;
- **le déploiement sur des infrastructures critiques**, en complément du déploiement commercial ;
- **la multiplication des parties prenantes de l'IdO** : la présence d'un seul objet connecté non sécurisé peut mettre en danger l'intégralité du réseau ;
- **la sécurité physique des biens et des personnes** (automobile, ville intelligente, etc.) ;
- **le marché très compétitif des objets connectés** se traduit par une forte pression sur les prix des fabricants qui peut conduire à des compromis en matière de sécurité ;
- **le manque d'expertise en matière de sécurité** des objets et réseaux de l'IdO ;
- **le déploiement des mises à jour de sécurité des objets déjà déployés** ;
- la complexité liée à l'adoption de bonnes pratiques en matière de sécurité pour **l'ensemble des maillons de la chaîne d'approvisionnement**.

Par ailleurs, NITI Aayog a publié en septembre 2020 un article[1] sur les enjeux et défis en matière de cybersécurité liés au développement de la 5G et de l'IdO, et TEC a publié en octobre 2021 un code de bonnes pratiques pour la sécurisation de l'IdO à destination des fabricants d'objets connectés, des fournisseurs d'accès, des développeurs d'application mobiles et les vendeurs.

À noter également l'existence d'une coopération active avec la France sur la cybersecurité avec la tenue régulière d'un dialogue cyber, dont la quatrième édition a eu lieu en octobre 2021, et l'endossement en août 2019 au plus haut niveau d'une feuille de route bilatérale sur la cybersécurité et le numérique.

Documents additionnels :

- Telecom Engineering Centre (TEC) a publié différents rapports techniques accessibles à https://www.tec.gov.in/M2M-IoT-technical-reports.
- Telecommunications Standards Development Society, India (TSDSI) a publié plusieurs rapports techniques sur des cas d'usage indiens accessibles à https://tsdsi.in/tr/.
- Bureau of Indian Standards (BIS), l'organisme normatif indien a contribué au développement de normes dans le domaine de l'Internet des objets via son comité technique LITD 27.
- Le rapport *Future of IoT* (2019) de l'organisation professionnelle FICCI.
- L'étude du Broadband India Forum sur le potentiel de création d'emplois dans les secteurs de l'agriculture et des soins de santé en Inde grâce à l'adoption de l'Internet des objets.
- Une Liste des initiatives en matière de recherche dans le domaine de l'IdO du Department of Science and Technology.

[1] NITI Aaylog (2020), « 5G & IoT vs cyber security – Addressing the elephant in the room », septembre.

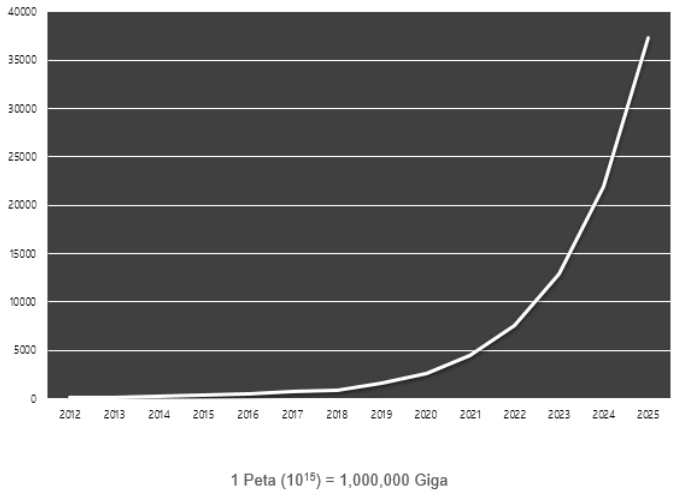
Étude de cas : Israël

Questionnaire : Internet des objets (IdO) –Israël

1. Quelle est l'ampleur du développement de l'Internet des objets ?

Il ne semble pas exister en Israël d'étude officielle ou privée chiffrant le nombre d'objets connectés. Il n'est par conséquent pas possible de détailler l'utilisation qui en est faite par les professionnels (B2B) ou par les consommateurs (B2C). Comme pour l'Europe, la possible explosion de l'IdO est l'objet de commentaires mais aucun chiffre n'est avancé pour démontrer cette tendance et seul, le ministère des Télécommunications se risque à une estimation de 100 000 connexions par km^2 à terme, sans toutefois détailler ce qui relève uniquement de l'IdO. La préoccupation des autorités publiques porte davantage sur les infrastructures : retard de la fibre optique[1], problème lié à la privatisation du secteur des télécommunications qui reste largement dominé par un seul opérateur (Bezeq[2]) et développement de la 5G. Le comparatif de l'OCDE qui place mal Israël est ici souvent souligné[3]. Dans ce contexte, l'accès des ménages à internet par fibre optique prend le pas sur celui des entreprises jugées aptes à se débrouiller par elles-mêmes. Selon le Speedtest Global Index, Israël est positionné en septembre 2021 à la 56^e place pour ses réseaux mobiles et 26^e place pour les réseaux fixes.

Israeli Mobile Data Consumption



Source : ministère israëlien des Communications

[1] En 2019, 10 % seulement des ménages étaient reliés à la fibre optique, contre 35 % à 40 % en 2021.

[2] Bezeq contrôlerait environ 80 % des revenus du secteur.

[3] Israël a 28,2 reliés pour 100 habitants, contre une moyenne OCDE de 33,2.

L'organisme israélien ISOC-IL [1] (statut d'association reconnue d'utilité publique) chargé de gérer l'extension « .il » reconnaît l'importance de l'IdO et estime que le pays doit passer à une version 6 des IP[2]. Il s'agit en effet de répondre à une augmentation rapide et prévisible de la demande mais aucune distinction n'est cependant faite s'agissant de la part qui sera imputable directement à l'IdO. Ses recommandations sont :

- que le ministère des Communications doit finaliser le transfert vers le IPv6 en 2022 ;
- l'accélération des dispositifs du réseau de la 5G, puis des fibres optiques, à des prix compétitifs, notamment pour les zones industrielles, le commerce et l'agriculture ;
- que le gouvernement doit promouvoir une régulation transversale de la cyberprotection relative à l'IdO.

2. Existe-t-il une politique publique dédiée portant sur l'IdO ?

Il n'existe aucune instance chargée par l'État d'étudier spécifiquement l'IdO. Les enjeux de l'IdO sont donc suivis par plusieurs autorités publiques. En l'occurrence, l'Autorité de protection de la vie privée au ministère de la Justice, la Direction nationale de la cybersécurité sous la tutelle directe du Premier ministre, le ministère des Communications et enfin l'Autorité de la protection des consommateurs et du commerce équitable. Il n'y a pas non plus d'aides publiques ciblées pour ce secteur, malgré les recommandations de l'ISOC-IL. Certaines subventions ou aides fiscales peuvent toutefois bénéficier au secteur des « objets connectés » dans le cadre du soutien à la haute technologie et à la R & D. C'est l'Agence de l'innovation d'Israël qui les gère pour l'essentiel. Des secteurs dans lesquels l'IdO représente une importante composante de la modernité font même l'objet de priorités : l'agriculture, l'énergie, la mobilité ou les besoins des villes. En tant qu'acteur mondial de la R & D, Israël se positionne favorablement dans le secteur de l'IdO par rapport à la concurrence internationale.

Il existe à notre connaissance une seule étude officielle publiée (uniquement en hébreu) portant en partie sur l'IdO. Elle fait suite à un débat sur le sujet organisé par le comité des sciences et de la technologie de la Knesset[3]. Elle a été réalisée par le ministère des Communications en avril 2019 et concluait que les infrastructures dans leurs configurations actuelles ne pourraient répondre à la demande supplémentaire provenant du développement des télécommunications, notamment en raison de l'IdO. Ce ministère préconisait donc une restructuration interne mais cette dernière n'a pas encore été mise en œuvre.

[1] Israel Internet Association ISOC-IL.

[2] Le ministère des Communications applique l'adoption du protocole IPv6 depuis juillet 2019 : « Acceleration of the Implementation of Technology – IP Version 6, in the State of Israel », communiqué de presse, 2 janvier 2020.

[3] Protocole numéro 160 du comité du 19 février 2018.

Il n'existe pas non plus de législations spécifiques sur l'IdO et aucune discussion à notre connaissance n'est en cours sur le sujet au sein du gouvernement. Là encore, la priorité porte sur l'accès des ménages aux infrastructures et le contrôle du quasi-monopole de Bezeq (qui dispose notamment toujours du monopole des lignes fixes).

3. Le développement de l'IdO dans le pays a-t-il fait ou va-t-il faire l'objet de débats publics ?

L'Autorité de protection de la vie privée est chargée de veiller à la protection des données personnelles contenues dans les fichiers informatiques ou papiers, aussi bien publics que privés. Cette institution a été placée sous la tutelle du ministère de la Justice. Elle n'a qu'un rôle de surveillance et de recommandation[1]. Son poste de président est vacant depuis deux ans. La protection des données fait l'objet de débats restreints (presse ou les réseaux sociaux) et ne semble pas inquiéter le public israélien, qui garde une bonne opinion de son État, et a pris l'habitude de donner son numéro d'identité national pour toute démarche administrative, pour payer en ligne même auprès d'entreprises privées mais aussi pour faire la queue à la banque ou à la poste. Il n'y a pas eu de manifestations publiques importantes sur cette question. Le risque associé au contrôle des données personnelles ne constitue pas, dès lors, un obstacle au développement de l'IdO. Le sentiment général qui prévaut semble être celui d'une nécessité pour la modernisation et la sécurisation du pays.

Israël a connu en revanche une opposition plus marquée, pour des raisons d'atteinte à la santé, au déploiement de la 5G, jugé par le ministère compétent comme nécessaire au développement de l'IdO. Cette opposition, selon les autorités, est caractérisée par le syndrome du *NIMBY* (*not in my back yard* ou « pas près de chez moi »). Quelques installations ont fait l'objet de destructions ou de dégradations. Les recours dans le cadre des autorisations administratives (*zoning demands*) ont été longs et nombreux. Pour répondre au besoin pressant de déploiement de la 5G, le gouvernement a récemment allégé les procédures permettant leurs installations sans permis grâce à une ancienne procédure accélérée d'adoption parlementaire (*Omnibus Law of Arrangements*).

L'impact environnemental de l'IdO et des technologies associées reste à ce stade marginal dans le débat public. Le gouvernement n'en fait pas référence dans ses objectifs généraux

[1] Dans le cadre de l'activité conjointe des organisations internationales de protection de la vie privée, ainsi que la GPEN (*Global Privacy Enforcement Network*), l'Autorité de protection de la vie privée a mené une enquête auprès des entreprises israéliennes engagées dans le domaine de l'IdO. Au cours du projet, les inspecteurs de l'Autorité ont examiné plus de 50 entreprises et appareils dans le domaine de l'IdO et ont approché 18 entreprises exigeant des informations et des documents afin d'obtenir les informations requises et de les examiner. Les résultats du test ont montré que les fabricants et distributeurs israéliens testés informaient mieux leurs clients que la moyenne internationale la manière dont les informations personnelles étaient collectées par l'appareil et ses utilisations, comment les informations étaient stockées et comment les informations étaient supprimées ainsi que les coordonnées.

de lutte contre le réchauffement climatique. Son nouveau plan « environnement » d'octobre 2021 n'en fait pas mention non plus. L'excès de consommation électrique en raison du développement des objets connectés ne semble pas à ce stade faire l'objet de débats publics[1]. L'étude faite par ISOC-IL reconnaît cependant le risque d'augmentation de la consommation électrique qu'induiront les produits connectés mais considère qu'en même temps ces produits pourront amener à des économies d'énergie s'ils permettent une régulation de la consommation (aménagement de l'éclairage public, etc.). Il souhaite à cet égard que le ministère de la Protection de l'environnement soit largement impliqué[2].

Les investissements massifs des géants du net (Amazon, Microsoft, Oracle et Google) en Israël ont grandement contribué à l'émergence des hautes technologies comme principal moteur économique du pays. Leur nationalité leur confère confèrent encore une certaine bienveillance de la part de l'opinion publique israélienne. Quelques rares voix (ONG) se font entendre sur le coût environnemental de la gestion du froid dans un climat désertique et chaud ou sur l'acquisition des terrains nécessaires dans un pays qui manque d'espaces[3].

4. Quelle est la prise en compte des dimensions cybersécurité et enjeux géostratégiques ?

Les risques de cybersécurité sont largement discutés en Israël, qui est un des grands centres mondiaux du secteur mais qui est aussi un des pays les plus attaqués. Pour les questions de cyber liées à l'IdO, le comité de science et de technologie de la Knesset a abordé le sujet lors d'une seule discussion en février 2018, sans que cela donne suite à des décisions concrètes par le gouvernement. Le « *Israel National Cyber Directorate* » a publié une page d'information en ligne sur l'IdO à destination du grand public[4]. Nos interlocuteurs ont confirmé que le sujet était discuté entre spécialistes mais qu'il n'y avait pas une législation ou une réglementation ciblant exclusivement l'IdO. Les nombreux objets connectés fonctionnant sur des systèmes à faible portée, les risques seraient perçus

[1] Avec la transition de la production électrique du charbon vers le gaz, grâce à la production nationale *offshore*, Israël estime être dans une position plutôt vertueuse à cet égard.

[2] Voir le Policy Paper d'octobre 2021 de l'ISOC-IL (p. 74-79). Selon la recommandation de l'ISOC-IL, le ministère de la Protection de l'environnement devrait accompagner la mise en œuvre des technologies de l'IdO, tout en évaluant les augmentations qui en résulteraient et en les comparant aux avantages économiques et environnementaux qu'elles sont supposées apporter.

[3] Voir l'article « Tech giants battle for data center real estate in Israel » du journal anglophone *Globe Business Israel*, 27 septembre 2021 : « *The public still perceives data centers as harmless, air-conditioned high-tech office spaces, rather than industrial plants, with most ignoring the environmental consequences brought about by this construction.* »

[4] הגנה על מוצרים חכמים - הגנה על מוצרי IOT | מערך הסייבר הלאומי (www.gov.il)

comme limités. Si à ce jour, aucun dispositif de protection spécifique à l'IdO[1] ne semble avoir été mis en place par les autorités, la bonne protection des réseaux et des sites sensibles constitue en revanche une obligation d'importance nationale qui impacte l'IdO.

Dans le secteur privé, les craintes liées à la cybersécurité des objets connectés semblent plus nombreuses que dans la sphère publique. Gil Shwed, PDG de Check Point Software Technologies (entreprise israélienne de premier plan dont la valeur est estimée à 1,8 milliard de dollars), a détaillé la sophistication croissante et rapide des cybermenaces qui atteignent désormais les équipements de cinquième génération alors que la grande majorité des plateformes ne sont protégées qu'au niveau de la troisième génération. Surtout, l'expansion du télétravail et la multiplication des objets connectés accroîtraient la surface des attaques et le nombre des vulnérabilités.

Au plan national, Israël peut compter sur un écosystème d'une cinquantaine d'entreprises spécialisées (et du campus de Beer Sheva), dont le travail en collaboration est indispensable en vue de développer des réponses innovantes en matière de protection cyber. La cybersécurité est un des piliers centraux de la haute technologie israélienne et le rayonnement économique du pays lui doit beaucoup. 90 % des objets connectés n'étant pas protégés, l'avenir israélien de cette filière semble donc très ouvert.

[1] Aucune mention directe à ce sujet n'a été trouvée dans la presse ou dans le *Plan national de mise en œuvre du changement climatique 2026-2022* – תכנית יישום לאומית להתמודדות עם משבר האקלים (www.gov.il).

Étude de cas : le Japon

Questionnaire : Internet des objets (IdO) – Japon

1. Quelle est l'ampleur du développement de l'Internet des objets ?

On compte environ 1 milliard d'objets connectés à internet (tous objets confondus) au Japon en 2021 (contre 800 millions en 2018), dont près de la moitié correspondent à des connexions de machine à machine (M2M) et 194 millions d'objets connectés grâce à une technologie de télécommunication mobile. En termes de télécommunications, le marché japonais est très mature, avec un taux de pénétration des souscriptions de 142 % fin 2019, une couverture mobile nationale de 99,99 % de la population et seulement 11 000 citoyens non couverts (mars 2020).

Sur le segment des particuliers (B2C), la récente baisse du prix des abonnements de télécommunications (poussée par le gouvernement) ainsi que l'émergence de la 5G promettent une expansion certaine des usages et services liés aux objets connectés. Néanmoins, le marché de l'IdO qui cible les particuliers ne semble pas être le plus développé, car on constate que la propension du consommateur final japonais à payer pour le service associé est assez faible : si l'utilisation ne remplit pas un « vrai » besoin, la technologie peut être perçue comme « gadget » et donc non indispensable. En conséquence, le coût marginal de développement pour le fabricant n'est pas toujours assez bas par rapport au volume vendu.

En revanche, le marché B2B est en croissance, tiré par des secteurs comme l'automobile (véhicules connectés), l'énergie (compteurs connectés), la livraison (drones), la sécurité ou encore la santé. Environ 14 % des entreprises japonaises déclarent utiliser l'IdO en 2020 pour leur activité et 10 % envisagent de l'utiliser dans un avenir proche. Cette tendance touche toutefois davantage les grandes entreprises que les PME[1].

Le développement de l'IdO au Japon repose principalement sur les technologies suivantes :

- pour l'IdO en temps réel et haut débit, les cas d'usage japonais s'appuient presque uniquement sur la 5G. Le coût financier et en énergie de ces solutions les limite à des secteurs spécifiques comme les véhicules connectés, le médical ou encore les *smart cities*. Si la crise de Covid-19 a ralenti la progression de la couverture 5G du pays et mis en pause un certain nombre de projets, la dynamique de développement de la 5G devrait reprendre avec la sortie de crise ;

[1] Voir le Livre blanc (2020) du ministère japonais des Affaires intérieures et des communications (MIC) sur le secteur des télécommunications et du numérique.

- pour l'IdO de masse s'appuyant sur des technologies LPWA, de nombreux cas d'usage se développent au Japon : logistique et gestion de chaînes d'approvisionnement, monitoring d'équipements (notamment compteurs de gaz, compteurs d'eau), monitoring à distance d'infrastructures (publiques et privées), systèmes de prévisions de catastrophes naturelles, agriculture, services de monitoring des personnes (enfants, seniors), etc.

Les technologies LPWA au Japon sont les suivantes :

- Sigfox : très utilisé au Japon ;
- ELTRES : technologie développée par Sony, qui n'existe qu'au Japon ;
- les technologies cellulaires comme le LTE-M des opérateurs historiques (NTT Docomo, Softbank, KDDI), et dans une moindre mesure le NB-IoT ;
- LoRa : en perte de vitesse au Japon et dont l'usage est de plus en plus limité à des réseaux privés.

Le développement du marché de l'IdO est indissociable du développement du numérique de façon générale, le Japon affichant un retard par rapport à la plupart des pays développés[1]. Dans un pays qui privilégie historiquement le recours au papier, au sceau (tampon hanko pour certifier les documents) et au présentiel, la crise du Covid-19 a incité les acteurs publics comme privés à accélérer la transformation numérique et notamment une transition vers des systèmes de production connectés – et donc le recours plus fréquent à l'IdO. Si de plus en plus d'entreprises innovantes font usage de l'IdO, certains secteurs traditionnels apparaissent encore relativement frileux.

2. Existe-t-il une politique publique dédiée portant sur l'IdO ?

Il n'existe pas de politique publique japonaise spécifiquement dédiée à l'IdO. **Les initiatives publiques qui promeuvent l'IdO s'inscrivent dans le cadre d'une politique plus large de transformation numérique du Japon.** Bien avant la prise de conscience liée à la crise sanitaire, le Japon a développé depuis plusieurs années le concept de « Société 5.0 », une société où les technologies nouvelles permettront de résoudre les difficultés et d'affronter le déclin démographique et le vieillissement de la population, en permettant l'automatisation, l'interopérabilité, la coopération homme-machine, le tout grâce aux nouvelles technologies (robotique, IA, IdO, mobilité autonome, etc.).

[1] Voir l'article « Will new agency save Japan from "digital defeat" ? » de la NHK (septembre 2021) sur la dématérialisation des procédures administratives ou l'article « Even after pandemic, Japan's labor market faces shortages and mismatches » du *Japan Times* (août 2021) reprenant un rapport du ministère japonais de l'Économie, du Commerce et de l'Industrie (METI) qui s'alarme de la pénurie de main-d'œuvre dans le secteur des télécommunications.

Parmi les initiatives de soutien au développement de l'IT et du numérique, on peut citer la mise en place en juin 2019 des « *New IT Policy Principles for the Digital Age* » qui énoncent deux objectifs principaux :

- dérouler un plan d'action permettant au Japon de faire la course en tête à l'échelle internationale à l'ère du numérique ;
- résoudre les défis de la société japonaise avec la transformation numérique.

Au-delà de ces principes généraux, **les dispositifs de soutien public à la transformation numérique, qui peuvent avoir un impact sur le développement de l'IdO au Japon, sont principalement des certifications et des subventions**.

À titre d'exemple :

- un système de certification incite les distributeurs de GPL à s'équiper de compteurs connectés[1] ;
- une certification (« DX Brand ») récompense chaque année les entreprises qui ont utilisé des solutions numériques pour augmenter leur productivité[2] ;
- une subvention du METI[3] permet depuis 2017 de financer les PME qui intègrent des solutions numériques à leur système de production, notamment celles qui souhaitent opérer la transition vers le télétravail ou bien intégrer des solutions IdO.

S'il n'existe pas de régulation spécifique à l'IdO, on peut citer les **réglementations relatives aux technologies radio, sur lesquelles s'appuient les solutions IdO**, édictées par l'Association of Radio Industries and Businesses (ARIB)[4] et par le MIC, et plus largement, les réglementations relatives à la protection des données personnelles[5].

Le **manque de main-d'œuvre qualifiée** est également régulièrement identifié comme un enjeu de première importance, notamment concernant les ingénieurs en IA, IdO et autres industries de pointe, car il s'agit d'un des obstacles principaux à la transformation numérique des entreprises[6]. Le pays souffre d'une pénurie croissante de main-d'œuvre

[1] Voir les éléments explicatifs, en japonais.

[2] Voir le site dédié, en japonais.

[3] Voir le site dédié, en japonais.

[4] Les technologies LPWA susmentionnées respectent généralement le standard ARIB STD-T108.

[5] L'*Act on the Protection of Personal Information* (2003, dernière version en vigueur amendée en 2017 ; la version amendée en 2020 prendra effet en avril 2022) que la *Personal Information Protection Commission* passe en revue tous les trois ans depuis un amendement en date de 2015.

[6] Voir le rapport de l'OCDE (2021), *Creating Responsive Adult Learning Opportunies in Japan*, février, sur les difficultés du marché de l'emploi japonais.

dans le secteur IT : le METI chiffrait en 2020 à 300 000 le nombre de travailleurs manquants et prévoyait une pénurie de 450 000 travailleurs à l'horizon 2030.

L'intelligence artificielle fait notamment l'objet d'une stratégie dédiée, incluant un soutien public à la formation d'ingénieurs dans le secteur.

Concernant l'IdO, le MIC a mis en place, depuis 2017, à l'échelle régionale à travers tout le territoire, **des séminaires et groupes de travail pour les utilisateurs d'objets connectés ainsi que l'organisation d'hackathons et de démonstrations de produits et services** à l'intention de jeunes visant à devenir des développeurs et/ou travailler dans le domaine des objets connectés.

Le gouvernement japonais a également mis sur pied en décembre 2017 un **groupe de travail pour étudier les prérequis techniques des infrastructures à mettre en place pour répondre à la croissance des objets connectés**. L'objectif de ce groupe de travail était de déterminer les conditions d'utilisation de services IdO de manière stable et sécurisée.

3. Le développement de l'IdO dans le pays a-t-il fait ou va-t-il faire l'objet de débats publics ?

L'opinion publique japonaise apparaît surtout préoccupée par les questions de **sécurité des données** (le concept de *Data Free Flow with Trust*, promu par les autorités japonaises dans les enceintes multilatérales depuis sa présidence du G20, est d'ailleurs de plus en plus central dans la communication du Japon). Selon un sondage réalisé par le MIC en 2020 auprès des utilisateurs d'objets connectés, plus de 60 % des répondants ont fait part de leur inquiétude quant à l'utilisation de leurs données personnelles. La plupart des entreprises qui font appel à des solutions IdO demandent également le stockage des données sur le territoire japonais et les autorités japonaises sont particulièrement attentives à ce qu'il n'y ait pas de fuite vers d'autres pays. Cela est vrai pour l'IdO comme pour les autres aspects de la transformation numérique[1], de sorte que **la problématique des données personnelles est assez présente dans la presse**[2].

En termes de **débat sociétal, l'IdO est surtout évoqué comme un élément de la transformation numérique** et, en tant que tel, il est présenté comme un moyen de répondre aux enjeux suivants :

[1] L'Agence du numérique, si elle a choisi Amazon et Google pour déployer son *cloud* gouvernemental, a ainsi insisté pour que les serveurs soient hébergés au Japon.

[2] Des scandales récents, notamment ceux relatifs à Recruit ou Line, ont poussé le législateur à plus de sévérité dans la protection des données personnelles. Voir *The Japan Times* (2020), « Japan's government adopts bill to tighten rules on personal data », 11 mars.

- ***smart city* (projet de *super cities*)** : dans un contexte de vieillissement de la population japonaise, l'IdO est présenté comme une solution permettant de rendre la vie quotidienne plus accessible et plus facile pour les résidents. L'IdO appliqué aux bâtiments (gestion de l'air conditionné, de l'électricité et du gaz, ordures, toilettes) est aussi présenté comme plus efficace pour la collectivité car il permet d'économiser des ressources. Le METI reconnaît également les bénéfices conséquents de l'IdO pour accroître la sécurité et réduire le nombre d'accidents, ainsi que pour la prévention et la gestion des catastrophes naturelles.
- **digitalisation de secteurs stratégiques clés** : face au manque de manque d'œuvre, le gouvernement a mis en place plusieurs programmes de subventions dans des secteurs critiques, comme la construction, afin de pouvoir faciliter l'introduction de nouvelles technologies. De manière générale, le gouvernement compte largement sur des solutions numériques et robotiques pour améliorer la productivité des entreprises et automatiser la production.
- **télétravail** : fortement accélérée par la pandémie de Covid-19, la croissance du télétravail va de pair avec davantage de monitoring rendu possible grâce à l'IdO, afin que l'employé puisse être aussi performant à distance qu'en présentiel. Le gouvernement s'est fixé pour objectif d'atteindre 70 % de télétravail dans les années à venir.

Concernant **l'enjeu environnemental**, il existe à ce jour peu d'études ou de données chiffrées au Japon et le développement de l'IdO n'a pas vraiment fait l'objet de débats publics sur les questions d'impact environnemental.

L'IdO ou l'IA (et la transformation numérique de manière plus générale) sont en fait plutôt identifiés comme des moyens permettant de soutenir et de promouvoir la transition énergétique des consommateurs finaux : le METI a préconisé l'utilisation des technologies IdO pour mieux gérer l'offre et la demande d'électricité ; pour optimiser le transport mondial de marchandises ; pour réduire les déchets des entreprises, des collectivités et des ménages ; ou encore pour réduire les émissions de carbone.

Certaines préfectures et municipalités japonaises ont également lancé leurs propres programmes pour encourager l'investissement dans des équipements permettant des économies d'énergie (chaudières plus efficaces, systèmes d'éclairage LED, fours industriels, installations de cogénération dans les PME). Certains programmes peuvent ainsi couvrir jusqu'à un tiers des coûts initiaux d'installation des équipements énergétiques (jusqu'à 1 million de yens, soit environ 8 000 euros). Ces initiatives demeurent toutefois encore assez dispersées.

Le gouvernement reconnaît que **la diffusion de nouveaux services numériques, tels que l'IdO ou le développement de villes intelligentes, nécessitera une augmentation**

significative des capacités de traitement des données et de la consommation d'énergie (notamment pour la 5G). Afin de limiter cet impact, il encourage le développement de *green data centers*, recourant à la technologie optoélectronique, pour réduire la consommation.

L'un des principaux défis de l'IdO est aussi celui de la **diminution de la consommation en batteries et de leur recyclage** : l'éparpillement de millions d'objets, potentiellement dans des sites naturels, rend nécessaire de pouvoir les récupérer facilement et de les traiter, ce qui doit se penser dès la conception de l'objet. Pourtant, cette problématique tend à être traitée dans le débat public moins sous l'angle de l'impact environnemental que comme un enjeu de sécurité économique.

4. Quelle est la prise en compte des dimensions cybersécurité et enjeux géostratégiques ?

Le gouvernement japonais a adopté le 28 septembre 2021 une **nouvelle stratégie nationale en matière de cybersécurité**. Cette nouvelle version, la troisième depuis 2015, couvre une période de trois ans. La nouvelle stratégie vise à s'adapter aux évolutions du contexte japonais depuis 2018, dont l'un des principaux paramètres identifiés est précisément la transformation numérique en cours et le développement de l'économie numérique, grâce, notamment, à la diffusion des services numériques par le biais de l'intelligence artificielle, des objets connectés ou encore de la réalité augmentée et de la réalité virtuelle.

Une agence spécialisée en cybersécurité (NISC) est rattachée au cabinet du Premier ministre depuis 2015 et une cellule cybersécurité est rattachée au MIC[1]. Cette dernière cellule a notamment préparé en **2020 des recommandations vis-à-vis des risques cyber liés aux technologies IdO.**

Les enjeux liés à la cybersécurité dans le domaine de l'IdO sont essentiellement pris en compte au Japon sous l'angle de la protection des **données personnelles**[2]. Un système de **notification des utilisateurs** d'appareils connectés présentant des risques de piratage a été mis en place en 2019[3], et un système de certification des appareils sécurisés est en

[1] Voir le site de l'Agence, basée sur le *Basic Act on Cybersecurity*, et les recommandations de la cellule rattachée au MIC, en japonais.

[2] Voir le rapport (2021) du MIC, en japonais.

[3] Le système NOTICE envoie une notification aux opérateurs si un appareil connecté a un mot de passe trop faible ou a été attaqué. L'opérateur doit ensuite à son tour envoyer une notification à l'utilisateur. Les lois à l'origine du système NOTICE sont le *Telecommunications Business Act* , le Règlement sur les terminaux ainsi que la loi relative au NICT (tous en japonais).

préparation depuis 2020[1], afin d'encourager les entreprises à développer la sécurité de leurs appareils connectés.

Au-delà du sujet des données personnelles, le risque majeur lié aux objets connectés concerne **l'obtention frauduleuse de mots de passe des objets** ou la prise de contrôle de ces derniers. Afin de limiter ces risques, le gouvernement a révisé l'ordonnance liée à l'accès aux terminaux connectés pour ajouter des standards techniques plus élevés.

Au niveau international, le Japon ne semble pas avoir exprimé de position clairement identifiée au sujet de l'IdO.

Le Japon est toutefois l'un des pays leaders en faveur de la normalisation des technologies de télécommunication, qu'elles soient fixes ou mobiles. Le MIC est ainsi partie prenante sur les sujets d'infrastructures IT au sein des organisations suivantes : G7/G20, APEC, APT, ASEAN, ITU, ONU, OMC et OCDE.

Le Japon n'est pas opposé à l'adoption de technologies étrangères pour accélérer le développement de l'IdO sur son territoire, impliquant donc un assouplissement de certaines réglementations ; dans le même temps, il tend aussi pousser certains standards spécifiques au Japon, susceptibles à terme de ralentir le développement du secteur.

Plus généralement, le nouveau gouvernement a décidé de placer les enjeux de sécurité économique au cœur de sa nouvelle stratégie de croissance. Le Premier ministre F. Kishida a ainsi créé un ministère de la Sécurité économique, dont le titulaire, M. Kobayashi est chargé de coordonner la préparation d'un projet de loi sur la sécurité économique en 2022.

Lors de la première réunion du Conseil pour la promotion de la sécurité économique, qui s'est tenue le 19 novembre 2021, le gouvernement a partagé trois principaux objectifs avec les ministres concernés : améliorer l'autonomie économique du Japon, en rendant les chaînes d'approvisionnement plus résilientes et en assurant la fiabilité des infrastructures-clés ; encourager les technologies clés telles que l'intelligence artificielle et les technologies quantiques ; et enfin assurer la supériorité et le caractère indispensable des technologies japonaises.

[1] Des lignes directrices ont été mises en place depuis 2021 et devraient bientôt faire l'objet d'une certification.

Étude de cas : le Nigéria

Questionnaire : Internet des objets (IdO) – Nigéria

1. Quelle est l'ampleur du développement de l'Internet des objets ?

Ampleur du développement de l'IdO au Nigéria et principales caractéristiques

Plusieurs caractéristiques sociodémographiques font du Nigéria un pays propice au développement de l'IdO. Les classes moyennes supérieures et aisées (10 dollars/jour à 20+ dollars/jour), bien qu'affaiblies par les diverses crises (sanitaire, monétaire), demeurent significatives (11 % en 2019, soit environ 20 millions de personnes selon Ipsos Nigéria en 2019). La part des revenus allouée aux dépenses en internet (données mobiles, Wi-Fi) représente 13 % et les données mobiles sont le deuxième poste de dépenses de la population (10 %) après les produits alimentaires (14 %). La jeunesse (âge médian : 18,1 ans en 2020) et la croissance de la population (2,58 % en 2020), qui est par ailleurs de plus en plus urbaine (52 % en 2020, avec environ 1 % de population urbaine supplémentaire chaque année), font du Nigéria un pays propice au déploiement et à l'ancrage de cette technologie dans les usages quotidiens, domestiques comme industriels.

Ainsi, au Nigéria, l'IdO est en forte croissance, malgré les inégalités d'accès aux solutions numériques et aux réseaux en général à l'échelle du pays. Le secteur y est estimé à 1 milliard de dollars en 2025, mais peu de chiffres existent concernant le nombre d'objets connectés aujourd'hui et dans les années à venir. Le développement du réseau nécessiterait au moins 10 000 à 15 000 passerelles/modems (« *gateways* »), chacune pouvant alimenter jusqu'à 1 000 terminaux connectés. Ce développement, selon un entrepreneur sur place, doit se faire d'abord directement par les entreprises spécialisées dans le domaine (fournisseurs d'IdO, fabricants de terminaux) avant que les opérateurs d'envergure nationale ne prennent le relais (MTN, Airtel, etc.).

Le secteur Oil & Gas est certainement celui ou les opportunités économiques sont les plus importantes à court terme. Les fournisseurs d'IdO sur place offrent des solutions de suivi de nombreux paramètres essentiels pour les installations pétrolières et gazières, *onshore* et *offshore* (pression, quantité disponible, température, etc.). Le potentiel est important en *upstream*, *midstream* et *downstram*.

Le seul marché de l'*upstream* pour l'IdO représente 1 milliard de dollars (« *well head monitoring* »). Le *midstream* est moins riche mais exploitable (monitoring du stockage en citernes car les pipelines sont en mauvais état, transport, logistique). Le *downstream* présente aussi un très fort potentiel de croissance, notamment les bouteilles de gaz intelligentes (traçage, ouverture de vanne à distance), plus sûres et économes, ainsi que d'autres usages pour les stations-service.

Le secteur de l'électricité est également porteur. Les *smart grids* sont en cours de développement au Nigéria, comme dans le reste de l'Afrique de l'Ouest, et font intervenir l'IdO dans la collecte de données et l'allocation des sources d'électricité (photovoltaïque, fioul, réseau) via un « contrôleur ». La croissance du secteur[1] est encouragée par de nombreux projets, financements et initiatives (notamment de la part de l'AFD).

Si le modèle commercial de l'IdO est aujourd'hui quasi exclusivement du B2B, le B2B2C, voire le B2C ont des marges de progression certaines sous réserve de financements. Il existe plus de 40 millions de bâtiments d'habitation au Nigéria et une forte croissance urbaine. Les usages domestiques (notamment détecteurs de fumée, sécurité et sûreté) sont donc amenés à croître et se diversifier, sans pour autant devenir comparables aux usages B2B en volume ou en valeur. Ainsi il est peu probable que la domotique (par exemple, la maison intelligente) croisse fortement compte tenu d'une main-d'œuvre domestique bon marché. Toutefois, il est à noter que la pénétration des solutions de sécurité domestique en IdO (détection des feux, intrusion, etc.) est de 12 % au Nigéria.

En B2B, des investissements pourraient donner un nouvel élan au secteur. Le développement de l'IdO dans tous les secteurs en général est freiné par le manque de CAPEX disponible (et à bas coûts). Cela freine aussi le déploiement des *smart grids*. Il existe par exemple des opportunités de développement de l'ordre de 270 millions de dollars pour les stations-service (9 000 stations dans le pays), sans compter les revenus d'entretien des installations. Les investissements publics notamment pourraient permettre à l'IdO de répondre à des besoins en soutien aux infrastructures locales (réseaux d'eau, signalisation routière intelligente, etc.).

2. Existe-t-il une politique publique dédiée portant sur l'IdO ?

Politiques publiques et régulation

Selon les personnes interrogées sur place, il n'existe pas d'encouragement réel de la part des acteurs publics. Il peut parfois exister un **manque de connaissance du secteur et de la technologie par les agents publics**, notamment celles en charge de la délivrance de permis (*license*) nécessaires pour opérer l'IdO au Nigéria.

Il existe peu ou pas de politiques dédiées à la protection des données mais ce sujet ne semble pas le plus préoccupant pour la population. La cybersécurité demeure toutefois, et de manière générale, une question amenée à gagner en importance et en attention.

[1] Le taux d'électrification du Nigéria est de 56,3 %, et le réseau national ne distribue que 5 GW pour une demande d'environ 50 GW. 80 millions de personnes n'ont ainsi toujours pas accès à l'électricité au Nigéria.

3. Le développement de l'IdO dans le pays a-t-il fait ou va-t-il faire l'objet de débats publics ?

Implications socioéconomiques et environnementales

La question de la protection des données, bien qu'elle fasse l'objet d'une attention particulière des milieux économiques et des acteurs du digital, n'est pas un sujet central quand l'on évoque l'IdO. Cela est principalement dû au fait que ses usages sont jusqu'à présent limités au B2B (pas ou peu de collecte de données personnelles par l'IdO). Par ailleurs la protection des données personnelles, si elle peut être un sujet de droit, est moins un sujet de société.

L'IdO répond à des problématiques d'emploi et de pénibilité du travail. La collecte de données permise par l'IdO peut limiter l'exposition du personnel à des risques (enlèvements, attaques, maladies ; ex. aux abords des pipelines dans la région du Delta).

Les effets environnementaux pourraient être globalement positifs, mais ne sont pas mesurés. Il est quasi impossible pour l'heure d'évaluer précisément les effets de l'IdO sur l'environnement (pas d'études sur le sujet, pas de mesures pour l'heure). Les usages de l'IdO sont toutefois à même de réduire l'empreinte carbone des entreprises : moins de déplacements pour la récupération de données qui se fait directement en ligne. Les solutions d'optimisation de durée de vie des batteries, l'utilisation de batteries durables, des cas d'usage pour la réduction de la consommation d'énergie, peuvent permettre des externalités positives de l'IdO sur l'environnement au Nigéria. Par ailleurs, les usages susceptibles de consommer beaucoup d'énergie seront limités : concentrés dans les grandes villes, ils toucheront les populations les plus riches.

Les usines peuvent accueillir des dispositifs de mesure et de contrôle par IdO et réduire ainsi leur consommation d'énergie. Le levier des *smart grids* est aussi à l'œuvre et permet une allocation optimisée des sources d'énergie. L'IdO peut aussi réduire les déchets (*waste management*) et le gaspillage de ressources (engrais notamment). Le gaspillage important de l'eau (conduits en mauvais état, quand ils existent) rend ces solutions très bénéfiques (anticipation et détection des fuites). L'IdO pourra également permettre un premier suivi en temps réel des niveaux de pollution (air, eau, sols, etc.), ce qui est une première étape vers une meilleure protection de l'environnement.

Le secteur agricole, levier d'externalités environnementales positives, n'est pas encore prêt à accueillir cette technologie[1]. Il faudrait attendre cinq à dix ans pour que les agriculteurs adoptent ces solutions (monitoring de la terre, arrosage intelligent, etc.).

[1] Bamigboye F. et Ademola E. (2018), « Internet of Things: The Present Status, Future Impacts and Challenges in Nigerian Agriculture », 1rst IFIP International Internet of Things Conference (IFIPIoT), septembre.

Les éleveurs sont aussi concernés (géolocalisation du bétail, optimisation des périodes de reproduction). Les agriculteurs et éleveurs sont encore trop peu enclins à prendre le risque d'investir dans une technologie qu'ils ne connaissent pas, et ont une mentalité conservatrice avec une forte aversion au risque. Il est toutefois à noter qu'une feuille de route officielle émise par l'Agence nationale de développement des technologies de l'information (NITDA) souligne le fort potentiel de l'IdO dans le secteur agricole.

Le sujet environnemental apparaît en général loin d'être une priorité pour le Nigéria. En somme, il semble que le recours aux technologies sobres en énergie (LoRaWAN, LTE-M) est le plus à même de faire du développement de l'IdO un phénomène bénéfique pour l'environnement au Nigéria.

4. Quelle est la prise en compte des dimensions cybersécurité et enjeux géostratégiques ?

Cybersécurité

La question n'a pas été spontanément évoquée par les personnes interrogées. Il semble que la prédominance pour l'heure d'un IdO en LoRaWAN, transportant très peu de données (de l'ordre de 12 Ko montants et 8 Ko descendants), rend le piratage des terminaux moins probable. Ce risque ne semble pas de nature à freiner le développement de cette technologie.

BIBLIOGRAPHIE

Rapports et documents institutionnels

Académie des sciences (2021), *Rapport sur la 5G et les réseaux de communications mobiles*, Groupe de travail de l'Académie des sciences sur les réseaux du futur, juillet.

Ademe et Arcep (2022), *Évaluation de l'impact environnemental du numérique en France et analyse prospective*, note de synthèse, janvier.

ADF et Fing (2021), *Livre blanc de l'Internet des objets*, non publié mais communiqué à l'occasion de l'audition de la Fing le 30 septembre 2021.

AFNIC et Institut de la souveraineté numérique (2021), *Internet des objets et souveraineté numérique. Perspectives industrielles et enjeux de régulation*, rapport, mars.

AIE (2021), *Total Energy Model 2.0 for Connected Devices*, IEA 4E EDNA, programme de coopération technique de l'Agence internationale de l'énergie, février.

AIE (2017), *Digitalisation and Energy*, rapport technique, Agence internationale de l'énergie, novembre.

AIE (2016), *Energy Efficiency of the Internet of Things. Policy Options*, document préparé pour l'IEA 4E EDNA, Agence internationale de l'énergie, juillet.

ANSSI (2021), *Recommandations relatives à la sécurité des (systèmes d') objets connectés*, guide ANSSI, août.

Arcep (2021), « Tableau de bord des expérimentations 5G en France », Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.

Arcep (2020), « Introduction à la 5G : les usages et les fréquences », Autorité de régulation des communications électroniques, novembre.

Arcep (2016), *Préparer la révolution de l'Internet des objets. Document n° 1 : une cartographie des enjeux*, Livre blanc, Autorité de régulation des communications électroniques, novembre.

Arcep et Anct (2021), *Baromètre du numérique, édition 2021. Enquête sur la diffusion des technologies de l'information et de la communication dans la société française*.

Banque des territoires et Groupe Caisse des dépôts (2021), *Les réseaux IoT en zone peu dense. État des lieux de l'IoT en France avec un focus sur les zones peu denses*, guide, janvier.

Batut C. et Tabet Y. (2020), « Que savons-nous aujourd'hui des effets économiques du télétravail ? », *Trésor Éco*, n° 270, Direction générale du Trésor, novembre.

Cantwell M. (2019), « Consumer Online Privacy Rights Act (COPRA) bill text », projet de loi soumis au Sénat des États-Unis.

Chevrollier G. et Houllegate J.-M. (2020), *Pour une transition numérique écologique*, rapport d'information n° 155 (2019-2020) fait au nom de la commission de l'aménagement du territoire et du développement durable, Sénat, juin.

Citizing, KPMG et Virtus management (2020), *Étude relative à l'évaluation des politiques publiques pour réduire l'empreinte environnementale du numérique*, étude réalisée à la demande de la commission de l'aménagement du territoire et du développement durable du Sénat, juin.

CNIL (2021), « Intelligence artificielle : avis de la CNIL et de ses homologues sur le futur règlement européen », Commission nationale de l'informatique et des libertés, 8 juillet.

CNIL (2021), « La CNIL rend son avis sur la proposition de loi "sécurité globale" », Commission nationale de l'informatique et des libertés, 3 février.

CNIL (2020), *À votre écoute. Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux*, coll. « Livre blanc », n° 1, Commission nationale de l'informatique et des libertés, septembre.

CNUCED (2019), *Digital Economy Report 2019. Value Creation and Captures: Implications for Developing Countries*, Conférence des Nations unies sur le commerce et le développement.

CNUCED (2021), *Technology and Innovation Report 2021. Catching Technological Waves: Innovation with Equity*, Conférence des Nations unies sur le commerce et le développement.

Comité national pilote d'éthique du numérique (2021a), « Agents conversationnels : enjeux d'éthique », communiqué de presse, 9 novembre.

Comité national pilote d'éthique du numérique (2021b), « Agents conversationnels : enjeux d'éthique », Avis n° 3, septembre.

Comité national pilote d'éthique du numérique (2021c), « Le "véhicule autonome" : enjeux d'éthique », Avis n° 2, avril.

Comité sénatorial américain du commerce, de la science et des transports (2019), « Fact Sheet: Chairman Wicker's Discussion Draft The United States Consumer Data Privacy Act », 3 décembre.

Commission européenne (2021a), *Preliminary Report. Sector Inquiry into Consumer Internet of Things*, Commission staff working document, juin.

Commission européenne (2021b), *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union*, 21 avril.

Commission européenne (2020), *Rapport sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité*, rapport de la Commission au Parlement, au Conseil et au Comité économique et social européen, COM(2020) 64 final, 19 février.

Commission européenne (2019a), « Règles relatives aux contrats de vente de biens entre les vendeurs et les consommateurs », octobre.

Commission européenne (2019b), « Directive (UE) 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques », *Journal officiel de l'Union européenne*, 22 mai.

Commission européenne (2018), *Vers un espace européen commun des données*, EUR-Lex-52018DC0232-EN-EUR-Lex SWD (2018) 125, avril.

Commission européenne (2014), « Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques », *Journal officiel de l'Union européenne*, 22 mai.

Commission européenne (2012a), « Directive 2012/27/EU du Parlement européen et du Conseil du 25 octobre 2012 relative à l'efficacité énergétique », *Journal officiel de l'Union européenne*, 14 novembre.

Commission européenne (2012b), « Directive 2012/19/UE du Parlement européen et du Conseil du 4 juillet 2012 relative aux déchets d'équipements électriques et électroniques (DEEE) », *Journal officiel de l'Union européenne*, 24 juillet.

Commission européenne (2010), « Directive 2010/31/UE du Parlement européen et du Conseil du 19 mai 2010 sur la performance énergétique des bâtiments », *Journal officiel de l'Union européenne*, 18 juin.

Conseil général de l'économie (2019), *Réduire la consommation énergétique du numérique*, rapport, décembre.

Conseil national de l'industrie (2020), *Contribution et éclairage du CSF Infrastructures numériques sur la question environnementale associée au numérique et à la 5G*, septembre.

Consortium Civiteo – Datactivist – Innopublica – KPMG – Parme Avocats pour le compte de la DGE, la FFTélécoms, Sycabel, InfraNum et AFNUM (2021), *De la Smart City à la réalité*

des territoires connectés. L'émergence d'un modèle français ?, rapport, coll. « Les dossiers de la DGE », octobre.

CSES et Tech4i2 (2020), *Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment*, rapport final pour la Commission européenne, avril.

Dedryver L., Hamelin J., Couric V. et Farella-Champeix J. (2020), « Maîtriser la consommation du numérique : le progrès technologique n'y suffira pas », document de travail, n° 2020-15, France Stratégie, octobre.

Département du Numérique, de la Culture, des Médias et du Sport du gouvernement britannique (2018), « Code of Practice for Consumer IoT Security », 14 octobre.

DGCCRF (2022), « Traçabilité », Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes, 1er février.

Duchesne C., Morel M., Cytermann L., Aureau T. et Vachey L. (2015), *Rapport relatif aux données d'intérêt général*, Conseil général de l'économie et IgF, septembre.

ETSI (2016), *SmartM2M. IoT Standards Landscape and Future Evolutions*, rapport technique, European Telecommunications Standards Institute.

EU-OSHA (2019), « Le numérique et la sécurité et la santé au travail : un programme de recherche de l'EU-OSHA », 16 décembre.

EU-OSHA (2018), *Foresight on New and Emerging Occupational Safety and Health Risks Associated with Digitalisation by 2025*, rapport, Luxembourg, Publications Office of the European Union, novembre.

Eurofound (2021a), *Digitisation in the Workplace*, Luxembourg, Publications Office of the European Union, octobre.

Eurofound (2021b), *The Digital Age: Implications of Automation, Digitisation and Platforms for Work and Employment*, Luxembourg, Publications Office of the European Union, coll. « Challenges and prospects in the EU », décembre.

Eurofound (2020), *Employee Monitoring and Surveillance: The Challenges of Digitalisation*, Luxembourg, Publications Office of the European Union, décembre.

Eurostat (2020), « Statistiques communautaires sur la société de l'information »

Fischer D. (2019), « Developing Innovation and Growing the Internet of Things Act bill text », projet de loi soumis au Sénat des États-Unis.

France Stratégie (2018), *Intelligence artificielle et travail*, rapport à la ministre du Travail et au secrétaire d'État chargé du numérique, mars.

FTC (2015a), « What's the security shelf-life of IoT? », Federal Trade Commission, février.

FTC (2015b), *Internet of Things: Privacy and Security in a Connected World*, Federal Trade Commission Staff Report, janvier.

GeSi et Accenture Strategy (2015), *SMARTer 2030: ICT Solutions for 21st Century Challenges*, rapport.

GeSI (2019), *Digital with a Purpose: Delivering a SMARTer2030*, septembre.

GPO (2021a), « S. 2750: Precision Agriculture Loan Program Act of 2021 », U.S. Government Publishing Office, 15 septembre.

GPO (2021b), « H. R. 981: IoT Readiness Act of 2021 », U.S. Government Publishing Office, 11 février.

GPO (2020), « Public Law 116-207, 116th Congress. An Act to establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes », U.S. Government Publishing Office, 4 décembre.

GPO (2015), « S. RES. 110 – Expressing the sense of the Senate about a strategy for the Internet of Things to promote economic growth and consumer empowerment », U.S. Government Publishing Office, 24 mars.

GreenIT.fr (2019), *Empreinte environnementale du numérique mondial*, septembre.

GSMA et Carbon Trust (2019), *The Enablement Effect. The Impact of Mobile Communications Technologies on Carbon Emission Reductions*, décembre.

Hischier R. et Hilty L. (2019), *The Challenges of Scaling the Internet of Things*, rapport technique, ETH Zurich, août.

Inria (2021a), *Internet des objets. Défis sociétaux et domaine de recherche scientifique pour l'Internet des Objets (IoT)*, Livre blanc, n° 5, Institut national de recherche en sciences et technologies du numérique, décembre.

Inria (2021b), « Industrie 4.0 : opérateur et robot sont-ils faits pour s'entendre ? », Institut national de recherche en sciences et technologies du numérique, 7 décembre.

Inria (2020), « Ministerio de Ciencia y Corfo lanzan Startup Ciencia », Institut national de recherche en sciences et technologies du numérique, 25 mai.

Légifrance (2021a), « Loi n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France (1) », *Journal officiel de la République française*, 16 novembre.

Légifrance (2021b), « Arrêté du 27 octobre 2021 portant cahiers des charges des éco-organismes, des systèmes individuels et des organismes coordonnateurs de la filière à responsabilité élargie du producteur des équipements électriques et électroniques », *Journal officiel de la République française*, 31 octobre.

Ministère estonien des Affaires économiques et des Communications (2019), *Cybersecurity Strategy – Republic of Estonia, 2019-2022*, décembre.

Mois G., Folea S. et Sanislav T. (2017), « Analysis of Three IoT-Based Wireless Sensors for Environmental Monitoring », *IEEE Transactions on Instrumentation ans Measurement*, vol. 66(8), août, p. 2056-2064.

NIST (2019), *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, National Institute of Standards and Technology – U.S. Department of Commerce, juin.

NIST (2015), *De-Identification of Personal Information*, par Simson L. Garfinkel, National Institute of Standards and Technology – U.S. Department of Commerce, octobre.

NSCAI (2021), *Final Report*, National Security Commission on Artificial Intelligence.

NTIA (2017), « U.S. Department of Commerce releases Green Paper proposing approach for advancing growth of Internet of Things », National Telecommunications and Information Administration, janvier.

OCDE (2022, à paraître), *Measuring the Internet of Things*, Working Party on Measurement and Analysis of the Digital Economy, Draft report d'octobre 2021.

OCDE (2021a), « Recommandation du Conseil sur la connectivité à haut débit », adoptée en février 2021.

OCDE (2021b) , « What happened to jobs at high risk of automation? », *Policy brief on the future of work*, janvier.

OCDE (2021c), « 12. Machine to machine subscriptions (Dec. 2020) », *OECD Broadband Portal*, base de données.

OCDE (2019), *The Road to 5G Networks. Experience to Date and Future Developments*, OECD Digital Economy Papers, n° 284, Paris, Publications de l'OCDE.

OCDE (2018), *IoT Measurement and Applications*, OECD Digital Economy Papers, n° 271, Paris, Publications de l'OCDE.

OCDE (2015a), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, Paris, Publications de l'OCDE, octobre.

OCDE (2015b), *Digital Economy Outlook 2015*, Paris, Publications de l'OCDE, juillet.

OCDE et AIE (2014), *More Data, Less Energy. Making Network Standby More Efficient in Billions of Connected Devices*, Paris, Publications de l'AIE, juin.

OPECST (2018), « Les objets connectés », *Les notes scientifiques de l'office*, n° 1, Office parlementaire d'évaluation des choix scientifiques et technologiques, mars.

Pérez R., Sergio C. et Terry E. (2019), *IoT in LAC 2019: Taking the pulse of the Internet of Things in Latin America and the Caribbean*, BID.

Publications universitaires

Aubert de Vincelles C. (2019), « Nouvelle directive sur la conformité dans la vente entre professionnel et consommateur : à propos de la directive 2019/771/UE du 20 mai 2019 » *La semaine juridique – édition générale*, n° 28, 15 juillet, p. 1338-1342.

Benghozi P. et Mellier G. (2016), « The Internet of Things: A New Paradigm for Regulation? », *Journal of Law and Economic Regulation*, vol. 9(1), janvier.

Bieser J., Salieri B., Hischier R. et Hilty L. M. (2020), *Next Generation Mobile Networks. Problem or Opportunity for Climate Protection?*, université de Zurich et Empa, octobre.

Das S. et Mao E. (2020), « The global energy footprint of information and communication technology electronics in connected Internet-of-Things devices », *Sustainable Energy, Grids and Networks*, vol. 24(3), décembre.

Freitag C., Berners-Lee M., Widdicks K. *et al.* (2021), *The climate impact of ICT: A review of estimates, trends and regulations*, rapport, université de Lancaster, février.

Ingemarsdotter E., Jamsin E et Balkenende R. (2020), « Opportunities and challenges in IoT-enabled circular business model implementation – A case study », *Resources, Conservation and Recycling*, vol. 162, novembre.

Laurent M., Pelov A. et Toutain L. (2021), « Les protocoles de l'Internet au service de l'interopérabilité de l'Internet des objets », *Enjeux numériques*, n° 16, Annales des Mines, décembre.

Lux A., Marchal P. et Perrin N. (2021), « Lunettes connectées : de nouveaux risques pour les salariés ? », *Hygiène et sécurité du travail*, n° 264, INRS, octobre.

Malenfer M., Govaere V., Bingen A. et Trionfetti M.C. (2020), « Impact des outils numériques sur les conditions de travail : l'exemple du commerce en ligne », *Hygiène et sécurité du travail*, n° 258, INRS, mars.

Malmodin J. et Lundén D. (2018), « The Energy and Carbon Footprint of the Global ICT and E & M Sectors 2010-2015 », *Sustainability*, 10(9), mai.

Marsot J. et Marchal P. (2019), « Équipements de protection individuelle et objets connectés : principaux enjeux pour la santé-sécurité au travail », communication scientifique aux journées des innovations 2019 de la FNTP, INRS.

Morel V., Cunche M. et Le Métayer D. (2019), « A generic information and consent framework for the IoT », Trustcom 2019, 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Rotorua, Nouvelle-Zélande, août.

Pirson T. et Bol D. (2021), « Assessing the embodied carbon footprint of IoT edge devices with a bottom-up life-cycle approach », *Journal of Cleaner Production*, vol. 322, novembre.

Ponce Del Castillo A. (2020), « Le travail à l'ère de l'IA : pourquoi la réglementation est nécessaire pour protéger les travailleurs », *Notes de prospective*, n° 8, ETUI, février.

Singla B., Mishra S., Singh A. et Yadav S. (2019), « A study on smart irrigation system using IoT », *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 5(2), avril, p. 1416-1418.

Zolynski C. (2019), « Contrats de fourniture de contenus et de services numériques : à propos de la directive (UE) 2019/770/UE du 20 mai 2019 (2019) », *La semaine juridique – édition générale*, n° 47, 25 novembre, p. 2062-2065.

Ouvrages, littérature grise et études

Benghozi P.-J., Bureau S. et Massit-Folléa F. (2009), *L'Internet des objets. Quels enjeux pour l'Europe*, Paris, Maison des sciences de l'homme.

CAA (s.d.), *Les systèmes de gestion de circulation*, volume 1, *Le problème de la congestion urbaine au Canada*.

CISCO (2020), *Annual Internet Report (2018–2023) White paper*, mars.

Deloitte (2018), *IoT para el sector empresarial en América Latina*, Centro de Estudios de Telecomunicaciones de América Latina (cet.la), juillet, 250 pages.

Lévy J.-D., Lancrey-Javal G. et Prunier A. (2021), *Développement du numérique et enjeux environnementaux : une possible cohabitation ?*, rapport de Harris Interactive pour SQLI Digital Experience, mai.

Mandon R. et Bellit S. (2021), *Vos données valent-elles de l'or ? L'Internet industriel des objets à l'épreuve du réel*, Paris, Presse des mines, coll. « Les docs de la fabrique ».

Mattatia F., Berthault D. et Degos L. (2022), *Code du numérique. Édition 2022*, Paris, Lexis-Nexis, coll. « Code bleu », 1re éd.

Microsoft (2021), *IoT Signals*, rapport, 3e éd., octobre.

Mordor Intelligence (2021), *Connected Toys Market. Growth, Trends, Covid-19 Impact, and Forecasts (2021-2026)*, rapport, octobre.

Pitron G. (2021), *L'enfer numérique. Voyage au bout d'un like*, Paris, Les liens qui libèrent.

Signals Research Group (2019), *A Global Perspective of 5G Network Performance. Our Analysis of Network Performance and User Experience Results from sub-7.125 Ghz and Millimeter Wave 5G Networks in Europe, Asia, and North America*, octobre.

The Shift Project (2021), *Impact environnemental du numérique : tendance à 5 ans et gouvernance de la 5G. Mise à jour des scénarios prospectifs des impacts du numérique mondial et propositions pour le déploiement d'une 5G raisonnée*, note d'analyse, mars.

The Shift Project (2018), *Lean ICT. Pour une sobriété numérique*, rapport, octobre.

Toledano J. (2020), *GAFA. Reprenons le pouvoir !*, Paris, Odile Jacob.

Wiener N. (1962), *Cybernétique et société. L'usage humain des êtres humains*, Paris, Éditions des Deux rives.

Xerfi et Precepta (2021), *Les marchés de l'IoT professionnel à l'heure de la maturité. Quels usages et stratégies gagnantes à l'horizon 2025 ?*, étude, décembre.

Articles (presse et web)

Abadie A. (2021), « Catastrophes naturelles : la mise en garde de l'ACPR sur une hausse significative des primes d'assurance », *L'Argus de l'assurance*, 4 mai.

Apec (2017), « L'internet des objets – tendance métiers dans l'industrie », Association pour l'emploi des cadres, 27 juin.

BCG (2021), « How tech offers a faster path to sustainability », 14 octobre.

BusinessWire (2020), « Worldwide Spending on the Internet of Things Will Slow in 2020 Then Return to Double-Digit Growth, According to a New IDC Spending Guide », 18 juin.

Cabinet Deroulez (2020), « Droit applicable à l'IoT – La "discontinuité des normes" est un facteur de complications mais également d'insécurité juridique pour les acteurs de l'IoT », 11 juin.

Coutance P. (2021), « La 5G non cellulaire et non opérée de Wirepas obtient la certification de l'UIT », *VIPress.net*, 21 octobre.

Dongxu C. et Wanxiang Y. (2020), « 5G Power: Creating a green grid that slashes costs, emissions & energy use », Huawei, juillet.

Forbes (2012), « How The Internet Of Things Will Change Almost Everything », par E. Savitz, 17 décembre.

Froese M. (2018), « Global IoT market to reach $318 billion by 2023, says GlobalData », *Windpower Engineering and Development*, 19 novembre.

Futura Planète (2021), « Réchauffement climatique et catastrophe naturelles : le risque a été multiplié par 5 en 50 ans ! », par D. de Schaepmeester, 6 septembre.

Garcia-Montero C. (2021), « Le Royaume-Uni, champion de la domotique en Europe », Journal du net, 8 avril.

Gartner (2019), « Gartner says global government IoT revenue for endpoint electronics and communications to total $21 billion in 2022 », communiqué de presse, 30 juin.

Globes (2021), « Tech giants battle for data center real estate in Israel », 27 septembre.

IoT Analytics (2021), « State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion », 22 septembre.

Les Échos (2019), « Risques naturels : le digital au secours de la prévention », par H. Vialatte, 18 avril.

Le Monde (2021), « Téléphonie mobile : espoirs, promesses et doutes autour de la 5G », par A. Sénécat, 24 octobre.

Le Monde (2017), « Comment mesurer le coût d'une catastrophe naturelle comme Irma », par A.-A. Durand, 15 septembre.

Petrov C. (2022), « 49 Stunning Internet of Things statistics 2021. The Rise of IoT », *TechJury*, 4 janvier.

Rizzato F. (2020), « 5G users on average consume up to 2.7x more mobile data compared to 4G users », *Open Signal*, 21 octobre.

Gloss K. (2021), « Navigate IoT regulations at local and global levels », *IoT Agenda*, 27 septembre.

Sites Internet

BCG (s.d.), page « Industry 4.0 ».

Connected Finland, https://www.connectedfinland.fi/en/

Commission européenne (s.d.), page « Radio Equipment Directive (RED) ».

Corfo : www.corfo.cl

Cybersecurity : https://tietoturvamerkki.fi/en/

IERC (s.d.), page « Internet of Things ».

Exponential Roadmap Initiative : https://exponentialroadmap.org/

IoT Analytics : https://iot-analytics.com/

Nega Octet : https://negaoctet.org/

Subsecretaría de Telecomunicaciones (s.d.), page « Observatorio Nacional 5G ».

Wirepas : https://www.wirepas.com/

Directeur de la publication
Gilles de Margerie, commissaire général
Directeur de la rédaction
Cédric Audenis, commissaire général adjoint
Secrétaires de rédaction
Olivier de Broca, Gladys Caré
Contact presse
Matthias Le Fur, directeur du service Édition/Communication/Événements
01 42 75 61 37, matthias.lefur@strategie.gouv.fr

RETROUVEZ LES DERNIÈRES ACTUALITÉS DE FRANCE STRATÉGIE SUR :


www.strategie.gouv.fr


@strategie_Gouv


france-strategie


francestrategie


@FranceStrategie_


StrategieGouv

Les opinions exprimées dans ce rapport engagent leurs auteurs et n'ont pas vocation à refléter la position du gouvernement

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FRANCE STRATÉGIE
ÉVALUER. ANTICIPER. DÉBATTRE. PROPOSER.

Institution autonome placée auprès du Premier ministre, France Stratégie contribue à l'action publique par ses analyses et ses propositions. Elle anime le débat public et éclaire les choix collectifs sur les enjeux sociaux, économiques et environnementaux. Elle produit également des évaluations de politiques publiques à la demande du gouvernement. Les résultats de ses travaux s'adressent aux pouvoirs publics, à la société civile et aux citoyens.

FRANCE STRATÉGIE – 20, AVENUE DE SÉGUR – TSA 90725 – 75334 PARIS CEDEX 07 TÉL. 01 42 75 60 00