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.