CONSUMERS INTERNATIONAL

TRAVAILLONS ENSEMBLE POUR LE CHANGEMENT

BRIEFING DE LA JOURNÉE MONDIALE DES DROITS DES CONSOMMATEURS 2019 :

DES PRODUITS CONNECTÉS DE CONFIANCE

QU'EST-CE QU'UN PRODUIT CONNECTÉ ?

Un produit connecté ou « intelligent » est capable de se connecter, de partager et d'interagir avec son utilisateur et d'autres appareils. Les produits connectés sont reliés les uns aux autres ainsi qu'à Internet par l'intermédiaire de différents protocoles de communication[1]. Les produits connectés les plus populaires auprès des consommateurs sont les smartphones, les consoles de jeux vidéo, les télévisions connectées, les traqueurs d'activité, les thermostats, les jouets et les véhicules. Ces appareils sont capables de recueillir et d'analyser les données des utilisateurs et de les transmettre à d'autres dispositifs connectés dans un réseau. Ces réseaux de produits connectés sont ce que l'on appelle l'Internet des Objets (IdO).

Les produits connectés offrent aux consommateurs la promesse de plus de commodité, d'efficacité et de services personnalisés. Les smartphones sont l'un des appareils connectés les plus populaires car en plus de pouvoir envoyer des SMS et passer des appels, ils permettent d'enregistrer le nombre de pas effectués, la localisation et même le rythme cardiaque de leur utilisateur. Qui plus est, ils peuvent faire office de hub centralisé permettant à l'utilisateur de connecter d'autres appareils intelligents tels que des imprimantes, des haut-parleurs, des systèmes de sécurité domotiques ou des traqueurs de santé.

Plus important encore, pour les consommateurs des pays en développement où l'accès à Internet par haut-débit fixe à domicile est limité[2], les personnes vont avoir davantage tendance à utiliser des smartphones pour des tâches essentielles telles que les paiements, l'envoi et la réception de fonds, les communications, l'accès aux salaires et aux emprunts, etc. En d'autres termes, la capacité à se connecter à internet de façon sûre, sécurisée et abordable depuis un téléphone est particulièrement importante pour les consommateurs qui en dépendent pour des services essentiels.

Après les smartphones, les systèmes de sécurité domotiques et les dispositifs de suivi de santé connectés sont également populaires. Par exemple, les traqueurs d'activité surveillent les niveaux d'activité, les habitudes de sommeil et le rythme cardiaque des utilisateurs, de façon à les aider à mieux appréhender leur santé personnelle. Chez soi, les systèmes de sécurité connectés rassemblent des caméras, des verrous et des capteurs de mouvement sans fil. Si ces dispositifs enregistrent une activité inhabituelle, ils peuvent transmettre des alertes aux habitants de la maison par l'intermédiaire de leur smartphone.

Il existe également de plus en plus de produits connectés offrant des solutions sur-mesure pour les personnes souffrant de handicaps. Par exemple, des montres connectées pour les personnes malvoyantes qui vibrent à la réception d'un e-mail, qu'elles retranscrivent ensuite en braille sur le cadran de la montre[3]. Ou encore, des ampoules connectées reliées à une sonnerie ou un téléphone alertent les personnes malentendantes lorsque le téléphone sonne ou que quelqu'un est à la porte[4].

También existe un número creciente de productos inteligentes que ofrecen soluciones personalizadas para personas con discapacidades. Por ejemplo, los relojes inteligentes para personas con pérdida de visión que vibran cuando el usuario recibe un correo electrónico y luego se traduce en braille en la esfera del reloj. [5] Las bombillas inteligentes, conectadas a un timbre de la puerta o a un teléfono, alertan a las personas sordas cuando suena el teléfono o cuando alguien está en la puerta.[6]

1 Par exemple : Bluetooth, 3G, 4G et Wi-Fi

2 Dans les pays les moins avancés (PMA), seuls 15 % des connexions à Internet passent par des lignes haut débit fixes. En Afrique, seulement 18 % des ménages disposent d'un accès internet à domicile. Le haut débit fixe est défini comme un accès à l'Internet public utilisant des connexions filaires. Cela inclut les modems par câble, l'ADSL, la fibre jusqu'au domicile/bâtiment, d'autres souscriptions câblées, le satellite à large bande et le haut débit terrestre fixe sans fil. ITU, *ITU Facts and Figures 2017* (Faits et chiffres 2017 de l'ITU), 2017

3 Site internet de Dot, https://dotincorp.com/

4 *Deaf community empowered through connected home lighting from Philips Hue* (Plus d'autonomie pour les personnes malentendantes grâce aux ampoules connectées Philips Hue), *Philips,* 29/09/2014

5 Dot sitio web, https://dotincorp.com/

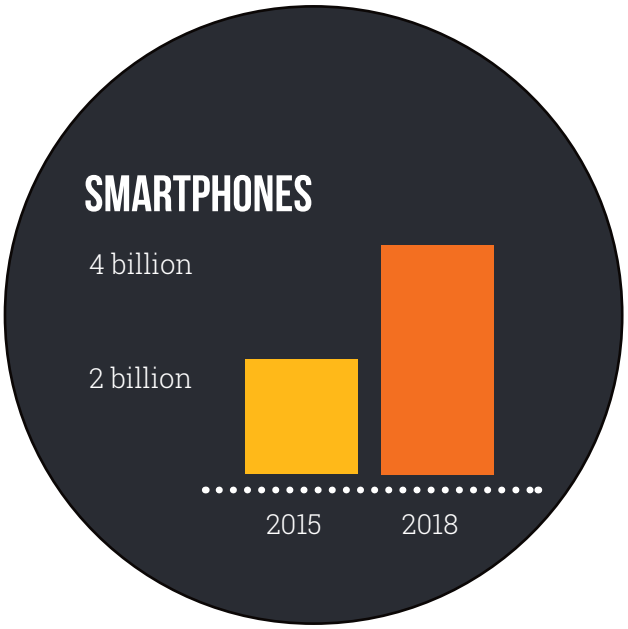
6 'Deaf community empowered through connected home lighting from Philips Hue', *Philips,* 29/09/2014

LE RYTHME D'ADOPTION RAPIDE DES PRODUITS CONNECTÉS

Au cours de la dernière décennie, l'adoption des produits connectés par les consommateurs s'est rapidement accrue, et tout porte à croire qu'elle va continuer à s'accélérer. Selon les enquêtes, il y aurait actuellement 23,1 milliards d'appareils connectés en fonction à travers le monde, un nombre qui devrait tripler d'ici à 2025.[7] De même, les dépenses globales des consommateurs en produits connectés pour la maison devraient presque doubler dans toutes les régions entre 2017 et 2022[8].

En particulier, l'adoption de smartphones à l'échelle mondiale a rapidement augmenté au cours des cinq dernières années. On compte aujourd'hui près de 4 milliards de connexions de smartphones autour du globe, soit près du double d'il y a trois ans. D'ici à 2025, on prévoit que 72 % des internautes accèderont à Internet exclusivement depuis un mobile. Près de la moitié de ces nouveaux utilisateurs viendront de Chine, d'Inde, d'Indonésie, du Nigéria et du Pakistan.[9]

Les connexions internet fixes restent une manière plus coûteuse de se connecter pour les consommateurs des pays en voie de développement[10], et la croissance de l'Internet mobile a été essentielle pour permettre à de nombreuses personnes d'expérimenter pour la première fois Internet et les nombreuses opportunités qu'il propose.[11]



7 *Internet of Things (IoT) connected devices installed based worldwide from 2015 to 2025 (in billions)* (Appareils connectés de l'Internet des Objets (IdO) installés à travers le monde de 2015 à 2025 (en milliards), *Statista*

8 *Forecast consumer spending on smart home systems and services worldwide by region in 2017 and 2022 (in billion US dollars)* (Dépenses prévues des consommateurs en systèmes et services domotiques connectés à travers le monde par région en 2017 et 2022 (en milliards de dollars US)), *Statista,*

9 *From 'mobile only' internet to content strategies: new GSMA study identifies the 'megatrends' shaping mobile industry*, (De l'Internet « exclusivement nomade » aux stratégies de contenu : la nouvelle étude de GSMA identifie les « mégatendances » de l'industrie du mobile) GSMA, 11/09/2018

10 ITU Broadband Commission, *The State of Broadband: Broadband catalyzing sustainable development* (Situation du haut débit : le haut-débit comme catalyseur du développement durable), septembre 2017

11 GSMA, Accelerating affordable smartphone ownership in emerging markets (Accélération de l'accès abordable aux smartphones dans les marchés émergents), juillet 2017

UN ACCÈS CROISSANT

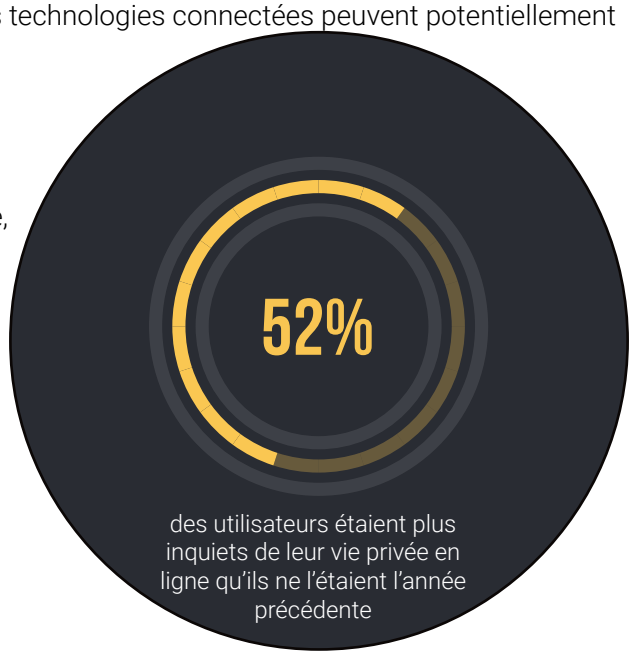
Cependant, l'adoption des produits connectés, y compris des téléphones, a été plus lente dans les pays en voie de développement en raison d'une mauvaise infrastructure de soutien, du coût des appareils et des données, ainsi que des débits plus réduits d'Internet. Pour ce qui est de l'adoption des smartphones, les tarifs des forfaits de données dans les pays en voie de développement sont les plus élevés du monde et représentent un frein à un plus grand développement. À titre d'exemple, un forfait de 1 Go de données en Afrique équivaut à 18 % du salaire mensuel moyen.[12]

Solo cuatro países africanos han alcanzado el objetivo de 1 GB de datos de la Alianza para Internet Accesible (A4AI), que cuesta el 2% de los ingresos mensuales.

Malgré ce retard, les analystes prévoient que l'adoption globale des appareils connectés va augmenter, en grande partie grâce aux investissements visant à améliorer les infrastructures. Selon GSMA, d'ici à 2025, les deux tiers des connexions mobiles à travers le monde se feront sur des réseaux à haute vitesse et 91 % de l'ensemble des connexions au réseau utiliseront la 3G ou la 4G. Ces réseaux seront mieux équipés pour soutenir l'utilisation des appareils connectés et la liaison vers d'autres produits connectés[13].

ASSURER LA CONFIANCE DANS LES PRODUITS CONNECTÉS DÈS LA PREMIÈRE UTILISATION

Par conséquent, à mesure que les capacités des réseaux s'améliorent dans toutes les régions et que l'investissement dans les nouvelles technologies augmente, les technologies connectées peuvent potentiellement devenir grand public. Faute d'une compréhension globale de ce que cela implique aussi bien en termes d'opportunités que de risques, les consommateurs à travers le monde pourraient se retrouver vulnérables. L'incorporation de produits connectés toujours plus nombreux dans notre vie quotidienne exige une compréhension des problématiques de sécurité et de vie privée, et implique le développement d'un cadre de protection du consommateur à même de promouvoir la confiance[14].



PROBLÉMATIQUES DES SMARTPHONES ET APPAREILS CONNECTÉS

Accessibilité : Bien que plusieurs gouvernements aient introduit des mesures telles qu'un abattage des droits de douane de façon à rendre les appareils et téléphones plus accessibles aux consommateurs[15], le coût des données représente toujours un frein à l'accès à Internet. À l'heure actuelle, seuls quatre pays d'Afrique ont atteint l'objectif de 1 Go de données pour 2 % du revenu mensuel promu par l'Alliance pour un Internet abordable (A4AI).[16] En Afrique du sud, le prix élevé des données a engendré des manifestations et déclenché la campagne #DataMustFall sur les réseaux sociaux.[17] Les tarifs des données sont également élevés dans d'autres régions, avec un coût au Go

12 A4AI, *2017 Affordability Report* (Rapport d'accessibilité 2017), 2017

13 GSMA, *The Mobile Economy* (L'économie mobile), 2018

14 OCDE, *The Internet of Things: Seizing the benefits and addressing the challenges. Background report for Ministerial Panel 2.2,* (L'Internet des Objets : tirer les bénéfices et relever les défis. Rapport d'information pour le groupe ministériel) mai 2016

15 *Ghana slashes tariff on imported phones by 50%* (Le Ghana sabre de 50 % les tarifs douaniers sur les téléphones importés), *IT Web Africa,* 18/10/2016

16 *Maurice, Nigéria, Tunisie, Égypte*, selon A4AI

17 *Icasa mulls regulating internet data prices* (Icasa réfléchit à réguler les tarifs de données d'Internet) *Eye Witness News,* 09/2018

représentant respectivement 4 % et 9 % du revenu moyen au Népal et au Nicaragua.[18]

Sûreté et sécurité : Les produits connectés font tous partie de réseaux et de systèmes interconnectés plus larges, dans lesquels la vulnérabilité d'un seul élément peut compromettre l'ensemble. Ces dernières années, on a vu se multiplier les cyberattaques très médiatisées qui ont commencé lorsque des pirates ont accédé à des appareils de consommateurs non sécurisés. En 2016, une cyberattaque majeure a interrompu les services Internet à travers l'Amérique du Nord et l'Europe en s'en prenant à des imprimantes non sécurisées, des box wi-fi et des dispositifs de surveillance de bébés, permettant une propagation rapide du virus qui a infecté près de 65 000 appareils en moins de 24 heures.[19]

Consumer Reports, notre membre américain, a testé Glow, une application qui enregistre les informations sur la santé et la fécondité des femmes. Il a ainsi mis au jour un certain nombre de vulnérabilités qui auraient pu permettre à des personnes ayant des connaissances de base en piratage d'accéder à ces données sensibles, ce que le producteur a rapidement corrigé après ces révélations.

En plus de l'interruption du service et du réseau, les appareils connectés non sécurisés menacent également directement la vie du consommateur. Des chercheurs ont montré qu'il était possible de pirater certains appareils et d'en prendre le contrôle à distance… Dans un exemple, ils sont parvenus à obtenir l'accès à un véhicule connecté et à contrôler le volant, le système de freinage et le verrouillage des portières.

Confidentialité et protection des données : Une étude globale des consommateurs datant de 2018 a montré que 52 % des utilisateurs étaient plus inquiets de leur vie privée en ligne qu'ils ne l'étaient l'année précédente.[20] Dans le même ordre d'idées, 43 % des personnes interrogées dans une autre enquête ont répondu qu'ils souhaitaient en savoir plus sur les données les concernant qui étaient collectées par l'intermédiaire de leurs appareils connectés, tandis que 47 % s'inquiétaient des vols d'identité.[21] Il existe un risque inhérent en matière de confidentialité des données dès lors que des appareils sont capables de (et, de fait, sont conçus pour) communiquer les uns avec les autres et transférer des données de façon autonome à des tiers. Les objets qui composent un système connecté peuvent collecter des données ou des informations qui, en elles-mêmes, sont inoffensives mais, une fois rassemblées et recoupées avec d'autres informations, peuvent révéler des connaissances extrêmement précises sur un individu, ce qui entraîne un accroissement de la traçabilité et du profilage d'un utilisateur.

Transparence : Les consommateurs peuvent comprendre les fonctionnalités de leurs appareils, mais il reste un grand flou sur la manière dont leurs données sont collectées et utilisées, de même que le rapport de ces données avec le modèle d'affaires de l'entreprise. Une étude réalisée par 25 organismes de réglementation internationale a montré que 59 % des appareils n'expliquaient pas de façon adéquate aux clients comment leurs informations personnelles étaient collectées, utilisées et divulguées. Deco Proteste, membre de Consumers International au Portugal, a organisé des achats de téléviseurs connectés en caméra cachée dans des magasins. Il a ainsi été découvert que les consommateurs ne recevaient aucune information préalablement à l'achat sur la manière dont ces appareils collectaient et utilisaient leurs données. Pourtant, accepter la politique de collecte des données du fournisseur est un impératif pour l'utilisation du téléviseur.

Interopérabilité : Pour assurer que les consommateurs puissent tirer le meilleur profit de leurs appareils, il est important que les différents produits connectés qu'ils détiennent soient capables de communiquer les uns avec les autres. Si jamais vous achetez un assistant domotique et découvrez qu'il ne peut pas se connecter aux autres appareils de votre maison, ses fonctionnalités en seront largement limitées. Si les appareils ne fonctionnent efficacement qu'avec ceux fabriqués par la même société, les consommateurs seront prisonniers d'un seul système, ce qui limitera leurs choix et entravera la concurrence.

Mises à jour de sécurité : L'un des problèmes couramment rencontrés avec les appareils connectés est l'absence

18 A4AI, *Mobile Broadband Data Costs* (Coûts des données haut débit mobile), 2017

19 *How a dorm room Minecraft scam brought down the internet* (Comment une arnaque de cours d'école a fait tomber Internet), *Wired,* 13/12/17

20 Centre for International Governance Innovation, *2018 CIGI-Ipsos Global Survey on Internet Security and Trust* (Enquête mondiale sur la sécurité et la confiance envers Internet 2018 CIGI-Ipsos), 2018

21 *Seventy-five per cent of smartphone users read privacy policies as industry gets ready to embrace savvy consumers* (Soixante-quinze pour cent des utilisateurs de smartphones lisent les politiques de confidentialité tandis que le secteur se prépare pour des consommateurs éclairés), *Mobile Ecosystem Forum,* 29/06/2017

de mise à jour de sécurité. Si les mises à jour ne sont pas disponibles, les appareils peuvent devenir vulnérables aux virus ou aux cyberattaques. Pourtant, les sociétés ne sont soumises à aucune exigence en matière de mise à jour et il n'existe aucun accord sur la durée pendant laquelle ils doivent les fournir.

EXEMPLES D'ACTIONS DE NOS MEMBRES

Campagne d'IDEC contre les plafonds de données au Brésil : En 2016, les fournisseurs d'accès à Internet (FAI) brésiliens ont commencé à appliquer des plafonds de données pour les connexions haut débit. Un plafond est une limite dans l'utilisation des données, fixée par un FAI. Une fois la limite atteinte, le FAI peut ralentir le service, voire même interrompre la connexion du consommateur à Internet. IDEC, membre de Consumers International, a mené une campagne aux côtés d'autres associations de consommateurs brésiliennes et groupes de défense des droits numériques pour faire interdire ces plafonds de données. La pression exercée par ces groupes a obligé l'ANATEL, l'organisme de régulation des télécoms, à mettre en place une consultation publique sur la question.

#WatchOut : Le Conseil norvégien des consommateurs (NCC), assisté d'une entreprise de sécurité basée au Royaume-Uni, a testé quatre montres destinées aux enfants[22]. Les tests ont révélé que ces appareils montraient de sérieuses failles de sécurité, des fonctionnalités de sûreté peu fiables et un manque global de protection du consommateur. Deux des appareils présentaient des failles qui auraient permis à un pirate potentiel de prendre le contrôle des applications, et donc d'accéder à la position en temps réel des enfants et de les écouter.

Garantir notre confiance : Conjointement avec l'ANEC, l'ICRT et le BEUC, Consumers International a publié un ensemble de principes[23] mettant en évidence l'importance d'intégrer les droits, la vie privée et la sécurité du consommateur au cœur des réseaux et des appareils de l'IdO. Destinés aux concepteurs, fabricants, décideurs politiques et organismes de régulation, ces principes et recommandations mettent en valeur les risques principaux qui menacent les consommateurs lors de l'utilisation de produits de l'IdO et ce qui peut être fait pour les éviter.

Promouvoir de meilleures mises à jour des smartphones : Consumentenbond, membre néerlandais de Consumers International, a mené Samsung devant les tribunaux pour ne pas avoir fourni des mises à jour de sécurité pour ses Smartphones pendant une durée suffisante. Samsung a fait valoir que ses produits haut de gamme recevaient bien des mises à jour pour une plus longue période.[24]

22 *#WatchOut, Analysis of smartwatches for children* (#WatchOut, Analyse de montres connectées pour enfants), Forbrukerradet, octobre 2017

23 ANEC, ICRT et BEUC, *Securing consumer trust in the internet of things. Principles and Recommendations* (Principes et recommandations en vue d'assurer la confiance du consommateur à l'égard de l'Internet des Objets), 2017

24 *Dutch case against Samsung for lack of updates finally heads to court* (Un litige néerlandais contre Samsung pour manque de mises à jours finit devant les tribunaux), *Android Police,* 26/03/2018

Test-Achats a piraté la maison connectée : Avec l'aide des pirates éthiques de Surecloud, notre membre belge Test-Achats a mis à l'épreuve 19 produits connectés populaires pour la maison[25] et a ainsi découvert que près de la moitié des produits testés présentaient de sérieuses failles de sécurité. Ces failles ont permis aux pirates de prendre le contrôle des appareils à distance et d'intercepter les données transmises à travers le réseau.

Action en faveur de services mobiles plus équitables au Rwanda : Avec toujours plus de consommateurs rwandais qui utilisent leurs appareils mobiles pour accéder aux services bancaires et aux services essentiels du gouvernement, notre membre ADECOR estime qu'il est de plus en plus important d'assurer non seulement la protection et la sécurité des données des consommateurs, mais aussi que les téléphones mobiles soient de bonne qualité et que les services restent abordables. Conjointement avec des consommateurs, des représentants de la société civile ainsi que des opérateurs mobiles et internet, ADECOR a compilé une liste de recommandations visant à améliorer les services mobiles. Ces recommandations préconisent notamment d'intégrer des représentants des consommateurs dans le contrôle des opérateurs téléphoniques ainsi qu'un appel à l'Office Rwandais de Normalisation (RSB) pour aider à prévenir l'importation de téléphones mobiles de mauvaise qualité.

***Which?* a enquêté sur la sécurité des jouets connectés :** Entre 2016 et 2017, *Which?* a enquêté aux côtés d'autres associations de consommateurs et des chercheurs en sécurité[26] sur la sécurité des jouets connectés. Leurs recherches ont montré que plusieurs jouets populaires présentaient de graves failles de sécurité. Les jouets équipés de haut-parleurs et de microphones étaient particulièrement préoccupants ; faute d'authentification Bluetooth sur le Toy-Fi Teddy, des pirates ont pu se connecter au jouet, envoyer des messages vocaux à l'enfant et écouter ses réponses.

Consumer Reports s'est penché sur les voitures connectées : Les analyses de Consumer Report, membre américain de Consumers International, montrent que les voitures connectées recueillent des volumes importants de données sur les conducteurs et leurs passagers. Les recherches sur les modèles de voiture lancés en 2018 ont montré que 32 des 44 marques proposaient un type de connexion de données sans fil ou un autre. Cependant, en dépit de l'augmentation du volume de données collectées, les réglementations autour de la propriété de ces données ne sont pas claires[27]. Consumers Union, la division légale de Consumer Reports, estime que le Congrès devrait voter des lois donnant aux consommateurs américains une forte protection légale en matière de vie privée.[28]

LES RÉPONSES POLITIQUES AUX OPPORTUNITÉS ET DÉFIS PRÉSENTÉS PAR LES PRODUITS

25 *Maison connectée, maison en danger !*, *Test-Achats*, May 2018
26 *Smart toys - should you buy them?* (Faut-il acheter des jouets connectés), *Which?*, 2017
27 *Who Owns the Data Your Car Collects?* (Qui détient les données que collecte votre voiture ?) *Consumer Reports, 02/05/2018*
28 *Data protection by design and default* (La protection des données dès la conception et par défaut), *ICO,* 2017

CONNECTÉS

Comme nous l'avons décrit ci-dessus, les produits connectés sont plus ou moins adoptés selon les régions du monde. De la même manière, la réponse des gouvernements aux défis et opportunités qu'il représente diffère elle aussi significativement d'un pays à l'autre.

Dans l'union européenne et aux États-Unis, nous commençons à voir se développer un cadre réglementaire spécifiquement destiné à la sécurité et la confidentialité des produits connectés. En Asie Pacifique, parallèlement à une demande croissante des consommateurs, on assiste à une forte implication gouvernementale et à des investissements dans les technologies connectées. Par exemple, le Japon, la Corée du Sud, l'Inde, la Malaisie et Singapour ont tous développés des stratégies nationales en matière d'IdO. En Amérique latine, en Afrique et au Moyen-Orient, le marché des appareils connectés n'en est encore qu'à ses premiers balbutiements (à l'exception de pays tels que la Turquie, les Émirats Arabes Unis et le Brésil) et la réponse gouvernementale à ce sujet est relativement limitée dans ces régions.

Ci-dessous, nous soulignons une sélection des développements récents les plus significatifs en matière de gouvernance et de réglementation de l'IdO :

Attribution raisonnée des fréquences : Les fréquences désignent une bande de radiofréquences attribuées à l'industrie mobile ou à d'autres secteurs à des fins de communication sur les ondes. Afin de réduire le coût des connexions sans fil, les fréquences doivent être attribuées aux industries de manière concurrentielle et non discriminatoire.[29] Au Brésil, l'autorité nationale de régulation des télécommunications, ANATEL, a développé un plan d'allocation des fréquences qui attribue des fréquences à certains services à mesure que la demande augmente. L'apport du public dans les plans est également pris en compte.

RGPD et protection de la vie privée dès la conception : Le principe de la protection de la vie privée dès la conception est désormais une obligation en vertu du Règlement général sur la protection des données (RGPD) de l'union européenne. Répondre à l'exigence de protection de la vie privée dès la conception implique d'incorporer la confidentialité et la protection des données au produit dès le début de son développement, plutôt que de l'intégrer à la va-vite dans les dernières phases.

Directive de l'UE sur la sécurité des réseaux et des systèmes informatiques : Cette directive est

29 *2017 Affordability Report* (Rapport d'accessibilité 2017), *A4AI*, 2017

entrée en vigueur en mai 2018. Elle exige des fournisseurs de services numériques (boutiques en ligne, moteurs de recherche et services de cloud computing) qu'ils mettent en œuvre des mesures de sécurité basée sur le risque pour les appareils de l'IdO intégrés dans leurs réseaux.[30]

Règlement européen sur la vie privée et les communications électroniques (ePR) : Le règlement européen sur la vie privée électronique s'applique aux communications entre machines (IdO). Les fournisseurs d'IdO doivent obtenir le consentement des utilisateurs finaux pour accéder aux informations associées aux appareils connectés[31].

Recommandations en matière de sécurité de l'IdO par la Federal Trade Commission (FTC) des États-Unis : La FTC a déclaré que les fournisseurs d'IdO devaient prendre des mesures afin d'assurer la sécurité des appareils de l'IdO contre les accès non autorisés. Les recommandations de la FTC exigent entre autres des fournisseurs qu'ils conçoivent des spécifications de mots de passe complexes et uniques, limitent le nombre de tentatives de connexion et sécurisent le stockage des informations sensibles.[32]

Normes de protection de la vie privée dès la conception : L'Organisation internationale de normalisation (ISO) en est aux premiers stades de développement d'une nouvelle norme pour la protection des consommateurs dans l'Internet des Objets (IdO). Cette norme fournira des conseils en matière de vie privée dès la conception pour les biens et services à destination des consommateurs.

Si vous recherchez d'autres exemples de politiques relatives à l'IdO, vous pouvez consulter l'index numérique de Consumers International. Notre index numérique est une collection en ligne de politiques et d'initiatives concernant le consommateur numérique qui proviennent des décideurs, des entreprises et de la société civile. En parcourant l'index, vous trouverez près de 200 politiques couvrant 10 domaines spécifiques, dont l'Accès et l'inclusion, la Protection des données et de la vie privée, la Sécurité, ainsi que la Concurrence et le choix. Faites une recherche sur l'Internet des Objets pour faire apparaître toutes les politiques pertinentes.

30 *Commission asks Member States to transpose into national laws the EU-wide legislation on cybersecurity* (La commission demande aux États membres de transposer la législation relative à la cybersécurité dans les lois nationales dans tous les pays de l'union européenne), *European Commission,* 19/07/2018

31 *The new EU ePrivacy Regulation: what you need to know* (Nouvelle réglementation européenne sur la vie privée électronique : ce qu'il faut savoir), *i-scoop,* 2017

32 Commission de sécurité des produits et des consommateurs de la FTC, *The Internet of Things and Consumer Product Hazards: Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection* (L'Internet des objets et les risques pour les consommateurs : commentaires du bureau de la protection des consommateurs de la Federal Trade Commission). 2018