CONSUMERS INTERNATIONAL

AUNANDO ESFUERZOS PARA EL CAMBIO

SESIÓN INFORMATIVA DEL DÍA MUNDIAL DE LOS DERECHOS DEL CONSUMIDOR 2019:

PRODUCTOS INTELIGENTES DE CONFIANZA

¿QUÉ ES UN PRODUCTO INTELIGENTE?

Un producto inteligente puede conectarse, compartir e interactuar con su usuario y otros dispositivos. Los productos inteligentes se conectan entre sí y con Internet a través de diferentes conexiones de comunicación[1]. Los productos inteligentes de consumo más populares son teléfonos inteligentes, consolas de juegos, televisores inteligentes, rastreadores de salud portátiles, termostatos, juguetes y automóviles conectados. Estos dispositivos son capaces de recopilar y analizar datos de usuarios y transmitirlos a otros dispositivos conectados en una red. Las redes de productos inteligentes también se conocen como Internet de las Cosas (IoT).

Los productos inteligentes ofrecen a los consumidores la promesa de conveniencia, eficiencia y servicios personalizados. Los teléfonos inteligentes son uno de los dispositivos inteligentes más populares porque además de enviar mensajes de texto y hacer llamadas, pueden monitorear los pasos, la ubicación e incluso el pulso de los usuarios. Además, pueden actuar como un concentrador central que conecta a un usuario con otros dispositivos inteligentes, como impresoras, altavoces, sistemas de seguridad para el hogar o rastreadores de salud.

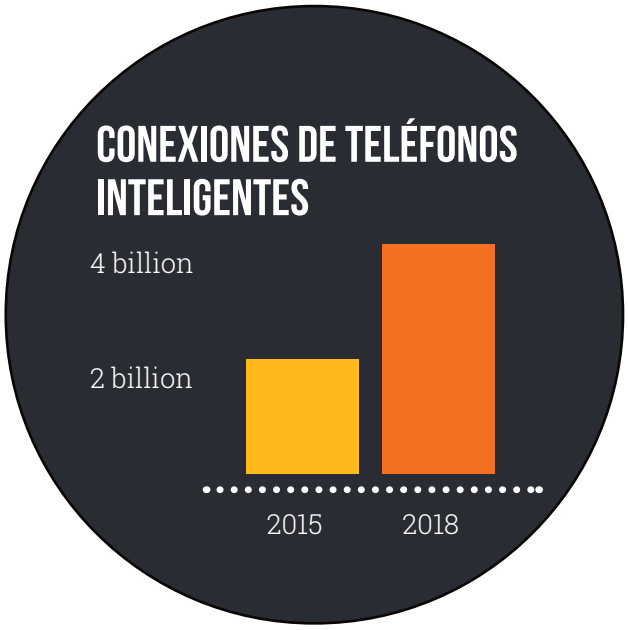
Más importante aún, para los consumidores en los países en desarrollo, donde el acceso a internet a través de banda ancha fija dentro del hogar es limitado[2], es más probable que las personas utilicen teléfonos inteligentes para realizar tareas esenciales, como realizar pagos, enviar y recibir remesas, comunicaciones, acceder a salarios y préstamos, etc. Esto significa que garantizar la asequibilidad y la seguridad de los teléfonos que se conectan a Internet es especialmente importante para los consumidores que confían en ellos para los servicios esenciales.

Aparte de los teléfonos inteligentes, otros dispositivos conectados populares incluyen sistemas inteligentes de seguridad para el hogar y monitores de salud inteligentes. Por ejemplo, los rastreadores de actividad física monitorean los niveles de actividad del usuario, los patrones de sueño y la frecuencia cardíaca, ayudándoles a comprender mejor su salud personal. En el hogar, los sistemas de seguridad inteligentes se componen de cámaras inalámbricas, cerraduras y sensores de movimiento. Si los dispositivos registran una actividad inusual, pueden enviar alertas al propietario a través de su teléfono inteligente.

1 por ejemplo; Bluetooth, 3G, 4G y Wi-Fi

2 En los países menos desarrollados (PMA), solo el 15% de las conexiones a Internet se realizan a través de banda ancha fija. Solo el 18% de los hogares tiene acceso a internet en su hogar en África. La banda ancha fija se define como el acceso a Internet público a través de conexiones por cable. Esto incluye cable módem, DSL, fibra-al-hogar / construcción, otras suscripciones de banda ancha fija (cableada), banda ancha satelital y banda ancha inalámbrica fija terrestre. UIT, Hechos y Cifras de la UIT 2017, 2017

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. [3] 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.[4]



RITMO RÁPIDO DE CAPTACIÓN DE PRODUCTOS INTELIGENTES

Durante la última década, el consumo de productos inteligentes por parte de los consumidores ha aumentado constantemente y los pronósticos muestran que esto continuará. Las encuestas sugieren que actualmente hay 23.1 mil millones de dispositivos conectados instalados a nivel mundial, una cifra que se espera se triplique para 2025.[5] Del mismo modo, se prevé que el gasto mundial de los consumidores en productos inteligentes para el hogar casi se duplicará en todas las regiones entre 2017 y 2022[6].

En particular, la adopción global de teléfonos inteligentes ha aumentado rápidamente en los últimos cinco años. En la actualidad, existen alrededor de 4 mil millones de conexiones de teléfonos inteligentes en todo el mundo, casi el doble que hace tres años. Se prevé que para 2025, el 72% de los usuarios de Internet accederán a Internet exclusivamente a través de dispositivos móviles. Alrededor de la mitad de estos nuevos usuarios provendrán de China, India, Indonesia, Nigeria y Pakistán.[7]

La conexión a Internet de línea fija sigue siendo una forma más costosa de conectarse para los consumidores en los países en desarrollo, por lo que el aumento de Internet móvil ha sido fundamental para permitir la primera experiencia de Internet para muchas personas y las importantes oportunidades que puede ofrecer.[8]

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

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

5 'Internet of Things (IoT) connected devices installed based worldwide from 2015 to 2025 (in billions)', *Statista*

6 'Forecast consumer spending on smart home systems and services worldwide by region in 2017 and 2022 (in billion US dollars)', *Statista,*

7 'From 'mobile only' internet to content strategies: new GSMA study identifies the 'megatrends' shaping mobile industry', *GSMA,* 11/09/2018

8 GSMA, *Accelerating affordable smartphone ownership in emerging markets*, July 2017

EXPANDIENDO EL ACCESO

Sin embargo, la aceptación de todos los productos inteligentes, incluidos los teléfonos, ha sido más lenta en los países en desarrollo debido a la deficiente infraestructura de soporte, la capacidad de pago de los dispositivos y los datos y la menor velocidad de Internet. En términos de uso de teléfonos inteligentes, el costo de los paquetes de datos en los países en desarrollo sigue siendo el más alto del mundo y presenta una barrera para una mayor adopción. Para comprar 1GB de datos en África, por ejemplo, los costos promedio de 18% del ingreso mensual de una persona.[9]

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.

A pesar de este retraso, los analistas predicen que la utilización de dispositivos inteligentes a nivel mundial aumentará, en gran medida gracias a la inversión en infraestructura mejorada. Según GSMA, para 2025, dos tercios de las conexiones móviles en todo el mundo operarán en redes de alta velocidad y el 91% de todas las conexiones de red utilizarán 3G o 4G. Estas redes estarán mejor equipadas para admitir el uso de dispositivos inteligentes y enlazar con otros productos inteligentes.[10]

ASEGURANDO LA CONFIANZA EN PRODUCTOS INTELIGENTES DESDE EL PRIMER USO

Por lo tanto, a medida que las capacidades de la red mejoran en todas las regiones y aumenta la inversión en nuevas tecnologías, la tecnología conectada tiene el potencial de convertirse en la corriente principal. Sin una comprensión completa de lo que esto significa en términos de oportunidades y riesgos, los consumidores en todo el mundo pueden quedar vulnerables. La incorporación de más y más productos inteligentes en la vida de las personas requiere una comprensión de los problemas relacionados con la seguridad y la privacidad y significa desarrollar marcos de protección al consumidor que promuevan la confianza.[11]

LOS PROBLEMAS CON LOS TELÉFONOS INTELIGENTES Y DISPOSITIVOS INTELIGENTES

Asequibilidad: aunque varios gobiernos han introducido medidas como reducir los aranceles de importación para hacer que los dispositivos y teléfonos inteligentes sean más baratos para los consumidores[12], el costo de los datos todavía presenta una barrera para el acceso a internet. Actualmente, 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.[13] En Sudáfrica, el alto precio de los datos ha generado protestas y la campaña de medios sociales #DataMustFall.[14] El precio de los datos también es alto en otras regiones con 1GB que cuestan el 4% y el 9% de las ganancias mensuales en Nepal y Nicaragua respectivamente.[15]

9 A4AI, *2017 Affordability Report*, 2017

10 GSMA, *The Mobile Economy*, 2018

11 OCDE, *The Internet of Things : Seizing the benefits and addressing the challenges. Background report for Ministerial Panel 2.2,* Mayo 2016

12 'Ghana slashes tariff on imported phones by 50%' *IT Web Africa,* 18/10/2016

13 Mauritius, Nigeria, Tunisia, Egypt, de A4AI

14 'Icasa mulls regulating internet data prices', *Eye Witness News,* 09/2018

15 A4AI, *Mobile Broadband Data Costs*, 2017

Seguridad y protección: todos los productos inteligentes son parte de una red y sistemas conectados más grandes, y una vulnerabilidad en cualquier parte puede comprometer todo el sistema. En los últimos años, hemos visto numerosos ataques cibernéticos de alto perfil que comienzan con piratas informáticos que acceden a dispositivos de consumidores no seguros. En 2016, un importante ataque cibernético interrumpió los servicios de Internet en América del Norte y Europa al atacar impresoras no seguras, enrutadores wifi domésticos y monitores para bebés que permiten que el virus se propague rápidamente e infecte a casi 65,000 dispositivos en menos de 24 horas.[16]

El miembro de Consumers International, Deco Proteste en Portugal, realizó compras misteriosas para televisores inteligentes en las tiendas. Descubrieron que no había información de compra previa disponible para los consumidores sobre cómo los dispositivos recolectaban y utilizaban sus datos. Sin embargo, aceptar la política de recopilación de datos del proveedor es esencial para poder usar el televisor.

Además de la interrupción de la red y el servicio, los dispositivos inteligentes no seguros también ponen en riesgo la seguridad del consumidor. Los investigadores han demostrado que pueden piratear dispositivos y controlarlos de forma remota. En un ejemplo, los investigadores de seguridad pudieron acceder a un automóvil conectado y controlar el volante, el sistema de frenos y las cerraduras de las puertas.

Protección y privacidad de los datos: un estudio de consumidores globales de 2018 reveló que el 52% de los usuarios está más preocupado por su privacidad en línea en comparación con el año anterior.[17] Mientras que el 43% de los encuestados de una encuesta diferente dijeron que querían saber más sobre los datos recopilados sobre ellos a través de sus dispositivos conectados y al 47% les preocupaba el robo de identidad.[18] Un riesgo significativo para la privacidad de los datos se debe a que los dispositivos pueden (y, de hecho, se diseñan) comunicarse entre sí y transferir los datos de forma autónoma a terceros. Los objetos dentro de un sistema conectado pueden recopilar datos o información que son inocuos por sí mismos, pero que, cuando se recopilan y analizan con otra información, pueden revelar un conocimiento bastante preciso de un individuo, lo que resulta en un aumento de la trazabilidad y el perfil del usuario. Nuestro miembro estadounidense, Consumer Reports, probó Glow, una aplicación que registra información personal sobre la salud y la fertilidad de las mujeres y encontró una serie de vulnerabilidades que permitían que alguien con habilidades básicas de piratería accediera a esta información confidencial, que el fabricante corrigió rápidamente luego de las revelaciones.

Transparencia: los consumidores pueden entender la funcionalidad del dispositivo, pero la forma en que se recopilan y utilizan sus datos y cómo se relaciona con el modelo de negocios de una empresa a menudo no está clara. Un estudio realizado por 25 reguladores internacionales de privacidad mostró que el 59% de los dispositivos no explicó adecuadamente a los clientes cómo se recopiló, utilizó y divulgó su información personal.

Interoperabilidad: Asegurar que los diferentes productos inteligentes que los consumidores poseen puedan comunicarse entre sí es importante para que los consumidores aprovechen al máximo sus dispositivos. Si comprara un asistente para el hogar y descubriera que no podía conectarse a otros dispositivos en su hogar, esto limitaría severamente su funcionalidad. Si los dispositivos solo funcionan de manera efectiva con otros fabricados por la misma compañía, los consumidores pueden estar sujetos a un solo sistema, lo que limita la elección y la competencia.

Actualizaciones de seguridad: un problema común con los dispositivos conectados es la falta de actualizaciones de seguridad. Si las actualizaciones no están disponibles, los dispositivos pueden volverse vulnerables a los virus o ataques cibernéticos, sin embargo, no hay un requisito para que las compañías proporcionen actualizaciones y no hay un acuerdo sobre cuánto tiempo deben proporcionarlos.

16 'How a dorm room Minecraft scam brought down the internet', *Wired,* 13/12/17

17 Centro para la Innovación en Gobernanza Internacional, *2018 CIGI-Ipsos Global Survey on Internet Security and Trust*, 2018

18 'Seventy-five per cent of smartphone users read privacy policies as industry gets ready to embrace savvy consumers', *Foro de Ecosistemas Móviles,* 29/06/2017

EJEMPLOS DEL TRABAJO DE NUESTROS MIEMBROS

IDEC hizo campaña contra los límites de datos en Brasil: en 2016, los proveedores de servicios de Internet (ISP) en Brasil comenzaron a implementar límites de datos para las conexiones de banda ancha. Un límite de datos es un límite de uso de datos establecido por el ISP. Una vez que se alcanza el límite, el ISP puede ralentizar el servicio o incluso desconectar al consumidor de Internet. IDEC, miembro de Consumers International, junto con otros grupos de derechos digitales y de consumidores de Brasil, hizo una campaña para prohibir los límites de datos. La presión de estos grupos llevó al regulador de telecomunicaciones ANATEL a establecer una consulta pública sobre el tema.

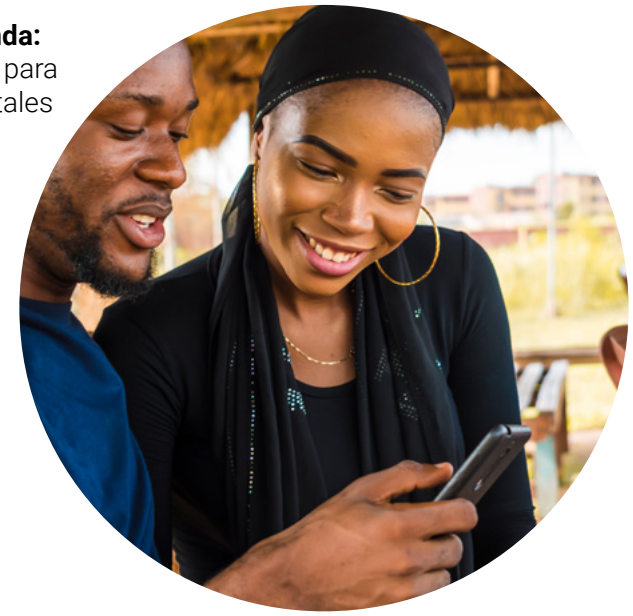
#WatchOut: El Consejo de Consumidores de Noruega (NCC) y una empresa de seguridad con sede en el Reino Unido probaron cuatro relojes inteligentes vendidos para niños[19]. La prueba reveló que los dispositivos tenían serias fallas de seguridad, características de seguridad poco confiables y falta de protección del consumidor. Dos de los dispositivos tenían fallas que permitían a un posible atacante tomar el control de las aplicaciones y así obtener acceso a la ubicación y el audio en tiempo real de los niños.

Asegurando nuestra confianza: Consumers International junto con ANEC, ICRT y BEUC publicaron una serie de principios[20] destacando la importancia de hacer que los derechos de los consumidores, la privacidad y las funciones principales de seguridad de las redes y dispositivos de IoT. Los principios y recomendaciones están dirigidos a desarrolladores, fabricantes, responsables políticos y reguladores, y resaltan los principales riesgos que enfrentan los consumidores al usar productos de IoT y qué se puede hacer para resolverlos.

Pidiendo mejores actualizaciones en los teléfonos inteligentes: Consumentenbond, miembro holandés de Consumers International, llevó a Samsung a los tribunales por no proporcionar las actualizaciones de seguridad adecuadas para sus teléfonos inteligentes. Samsung argumentó que sus productos de gama alta reciben actualizaciones durante un período de tiempo más largo.[21]

Test-Achats hackeó la casa inteligente: trabajando con hackers éticos en SureCloud, nuestro miembro belga Test-Achats probó 19 productos populares de casas inteligentes[22] y encontró que casi la mitad de los productos probados tenían serias fallas de seguridad. Las fallas de seguridad permitieron a los hackers controlar el dispositivo de forma remota e interceptar los datos que se envían dentro de la red.

Presionando para obtener servicios móviles más justos en Ruanda: cada vez más consumidores en Ruanda utilizan servicios móviles para realizar operaciones bancarias y acceder a servicios gubernamentales esenciales, nuestro miembro ADECOR afirma que es cada vez más importante que no solo garanticen que los datos de los consumidores estén protegidos y seguros, sino que los teléfonos móviles Son de buena calidad y los servicios son asequibles. En colaboración con los consumidores, la sociedad civil, los operadores móviles y de Internet, ADECOR compiló una lista de recomendaciones para mejorar los servicios móviles. Estos incluyen la participación de representantes de los consumidores en la inspección de los operadores de telefonía y el llamado a la Oficina de Normas de Ruanda (RSB) para ayudar a prevenir la importación de teléfonos móviles de baja calidad.



19 #WatchOut, Analysis of smartwatches for children, *Forbrukerradet*, Octubre 2017

20 ANEC, ICRT y BEUC, *Securing consumer trust in the internet of things. Principles and Recommendations*, 2017

21 'Dutch case against Samsung for lack of updates finally heads to court', *Android Police,* 26/03/2018

22 Connected house, house in danger!, *Test-Achats*, May 2018

Which? investigó la seguridad de los juguetes inteligentes: entre 2016 y 2017, Which? junto a otras organizaciones de consumidores e investigadores de seguridad realizaron investigaciones.[23] en la seguridad de los juguetes conectados. Su investigación mostró que varios juguetes populares para niños tenían serias fallas de seguridad. Los juguetes equipados con altavoces y micrófonos fueron de particular interés; sin autenticación Bluetooth en el Toy-Fi Teddy, los piratas informáticos pudieron conectarse al juguete, enviar mensajes de voz al niño y recibir respuestas.

Consumer Reports examinó los autos conectados: el miembro estadounidense de Consumers International, el análisis de Consumer Reports muestra que los autos conectados están reuniendo grandes cantidades de datos sobre los conductores y pasajeros. La investigación sobre modelos de automóviles lanzada en 2018 mostró que 32 de las 44 marcas ofrecen algún tipo de conexión de datos inalámbrica. Sin embargo, a pesar de la creciente cantidad de datos que se recopilan, las reglas legales sobre quién es el propietario de los datos no son muy claras.[24] Consumers Union, la división de defensa de Consumer Reports, cree que el Congreso debería aprobar una legislación para otorgar a los consumidores en los Estados Unidos derechos legales de privacidad.[25]

RESPUESTAS POLÍTICAS A LAS OPORTUNIDADES Y DESAFÍOS DE LOS PRODUCTOS INTELIGENTES

Como se indicó anteriormente, los niveles de utilización de productos inteligentes difieren enormemente en todo el mundo. Reflejando esta variación, las respuestas del gobierno a los desafíos y oportunidades que presentan los dispositivos conectados también difieren enormemente dentro y entre las regiones.

En la UE y los EE. UU., Estamos empezando a ver el desarrollo de marcos regulatorios, especialmente en relación con la seguridad y privacidad de los productos inteligentes. En Asia Pacífico, reflejando la creciente demanda de los consumidores, hemos visto un fuerte apoyo gubernamental e inversión en tecnología conectada. Por ejemplo, Japón, Corea del Sur, India, Malasia y Singapur han desarrollado estrategias nacionales de IoT. En América Latina, África y Oriente Medio, los mercados de dispositivos inteligentes aún están en su infancia (con la excepción de países como Turquía, Emiratos Árabes Unidos y Brasil), por lo que las respuestas del gobierno a los productos de consumo conectados en estas regiones son limitadas.

A continuación, destacamos una selección de los desarrollos recientes más importantes en la gobernanza y regulación de IoT:

Asignación inteligente de espectro: el espectro se relaciona con una gama de frecuencias de radio asignadas a la industria móvil u otros sectores para utilizar para la comunicación a través de ondas. Para reducir los costos de las conexiones inalámbricas, el espectro debe estar disponible para las industrias sobre una base competitiva y no discriminatoria.[26] En Brasil, el regulador nacional de telecomunicaciones ANATEL ha desarrollado un plan de asignación de espectro que asigna bandas a ciertos servicios a medida que crece la demanda. También se tiene en cuenta la opinión pública en los planes.

23 Smart toys - should you buy them?, Which?, 2017

24 'Who Owns the Data Your Car Collects?', *Consumer Reports, 02/05/2018*

25 'Data protection by design and default', *ICO,* 2017

26 *'2017 Affordability Report', A4AI*, 2017

GDPR y Privacidad por Diseño: el principio de privacidad por diseño es ahora una obligación del Reglamento General de Protección de Datos de la UE (GDPR). Cumplir con el requisito de privacidad por diseño significa garantizar que la privacidad y la protección de datos se hayan incorporado al producto desde su inicio, en lugar de atornillarlo al final.

Directiva de la UE sobre seguridad de redes y sistemas de información: la directiva entró en vigor en mayo de 2018. Requiere que los proveedores de servicios digitales (mercados en línea, motores de búsqueda y servicios de computación en la nube) implementen medidas de seguridad basadas en riesgos para dispositivos IoT incorporados en sus redes.[27]

Reglamento de privacidad de la UE: el reglamento de privacidad de la UE se aplica a las comunicaciones de máquina a máquina (IoT). Los proveedores de IoT deben obtener el consentimiento del usuario final para acceder a la información relacionada con el dispositivo conectado.[28]

Recomendaciones de seguridad de IoT de la Comisión Federal de Comercio (FTC) de los Estados Unidos: La FTC ha declarado que los proveedores de IoT deben tomar medidas para proteger los dispositivos de IoT del acceso no autorizado. Las recomendaciones de la FTC incluyen exigir a los proveedores que diseñen especificaciones de contraseñas que sean complejas y únicas, que limiten el número de intentos de inicio de sesión y almacenen la información confidencial de forma segura.[29]

Estándar de privacidad por diseño: La Organización Internacional de Normalización (ISO) se encuentra en las primeras etapas del desarrollo de un nuevo estándar para la protección del consumidor en la Internet de las cosas (IoT). La norma proporcionará orientación sobre la privacidad mediante marcos de diseño para bienes y servicios de consumo.

Si está buscando más ejemplos de políticas de IoT, consulte el Índice Digital de Consumers International. El Índice Digital es una colección en línea de políticas e iniciativas de consumidores digitales de los responsables políticos, empresas y la sociedad civil. Buscando en el Índice, encontrará alrededor de 200 pólizas que cubren 10 áreas que incluyen Acceso e Inclusión, Protección de Datos y Privacidad, Seguridad y Protección y Competencia y Elección. Busque Internet de las Cosas para que aparezcan todas las políticas sobre ese tema.

27 'Commission asks Member States to transpose into national laws the EU-wide legislation on cybersecurity', *Comisión Europea,* 19/07/2018

28 'The new EU ePrivacy Regulation: what you need to know', *i-scoop,* 2017

29 Comisión de Seguridad de Productos del Consumidor 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.* 2018