GARANTIZAR LA CONFIANZA DE LOS CONSUMIDORES EN LA INTERNET DE LAS COSAS

PRINCIPIOS Y RECOMENDACIONES, AÑO 2017

INTRODUCCIÓN

Las aplicaciones diseñadas para los consumidores de la Internet de las cosas pueden aportar beneficios sociales y económicos a las personas en todo el mundo, entre los que se incluyen servicios con mayor capacidad de respuesta, ciclos de retroalimentación más breves, arreglos o reparaciones desde lugares remotos, más comodidad, apoyo en la toma de decisiones, una mejor asignación de los recursos, control a distancia de los servicios y conocimientos sobre el comportamiento.

Sin embargo, hay algunos motivos para inquietarse: la privacidad y la seguridad, la falta de transparencia, las complejidades en materia de responsabilidad, productos y sistema con efecto cautivo (lock-in), y un aumento de los productos híbridos que debilita las normas sobre propiedad y que deja expuestos a los consumidores a tener que cumplir contratos remotos, a la pérdida del control y al riesgo de que sus dispositivos queden obsoletos de forma imprevista si se acaba el soporte.

Los posibles beneficios se alcanzarán solo si los servicios y productos pueden diseñarse basándose en la confianza y la privacidad y se ofrecen con seguridad integrada, de modo que los consumidores sientan que son adecuados y seguros de usar. Para crear un próspero y confiable entorno de Internet de las cosas para los consumidores será esencial trabajar en conjunto en las áreas que describimos a continuación.

Cada encabezado contiene los desafíos y oportunidades más importantes que se presentan a los consumidores en esa área en particular, y va acompañado de un conjunto de principios a partir de los cuales se elaborarán recomendaciones específicas en términos de políticas, normas, pruebas y prácticas empresariales.

Crédito de la fotografía: Canadapanda / Shutterstock.com

1. CONECTIVIDAD E INCLUSIÓN

A medida que los productos conectados se vuelven cada vez más presentes en la vida de las personas, se irá volviendo cada vez más esencial para todos los consumidores contar con acceso a una conexión a Internet asequible y de calidad tanto a nivel nacional como internacional, y tanto móvil como fija. Hoy más que nunca es necesario que los proveedores de acceso a Internet no ralenticen ni bloqueen injustificadamente, ni discriminen, el acceso a algunas aplicaciones o servicios.

1.1 Los consumidores deberían tener acceso a una conexión a Internet asequible y de alta calidad y velocidad que les permita aprovechar las oportunidades que les ofrece la tecnología de la Internet de las cosas.

1.2 Debe prestarse particular atención a garantizar el acceso para los grupos de consumidores marginados, menos favorecidos y vulnerables, y también el de quienes viven en zonas geográficas alejadas o desatendidas, y las mediciones de dicho acceso deben reflejar a los grupos de bajos ingresos y aplicar igualdad demográfica.

1.3 Los países deberían abordar todo aquello que influya sobre la asequibilidad, como por ejemplo, el costo de los dispositivos y la aplicación de límites a los datos abusivos que pueden mantener los precios de las conexiones a tasas artificialmente elevadas.

1.4 Debe respetarse el principio de la neutralidad en la red.

2. INFORMACIÓN Y TRANSPARENCIA

Para que exista un entorno de Internet de las cosas en el que los consumidores puedan confiar es indispensable que cuenten con la información correcta para comprender cómo funcionan los productos y servicios digitales y que puedan tomar las correspondientes decisiones. Sin embargo, es particularmente difícil obtener una información a la que se pueda tener fácil acceso y que sea clara, concisa, significativa y comprobable, que ofrezca claridad plena en el momento que se las personas la necesiten.

Para los consumidores se volverá más problemático el depender únicamente del concepto de “notificación y consentimiento” en lo que se refiere a la entrega de información y posibilidades de elegir en la Internet de las cosas, teniendo en cuenta el potencial que existe en cuanto a que grandes cantidades de datos granulares sean utilizadas desde muchos tipos diferentes de dispositivos y con la participación de varios proveedores.

2.1 Debería destacarse, y ponerse al alcance de todos, información clara, sucinta y de fácil comprensión acerca de los productos, proveedores y procesos de la Internet de las cosas junto a los respectivos derechos de los consumidores.

2.2 Esta información debería permitir a los consumidores comprender las implicancias de su uso de los productos de la Internet de las cosas, y facilitarles una toma de decisiones confiada e informada. Esto quiere decir, en particular, que se debería informar a los consumidores acerca de todo aquello que un producto puede o no puede hacer sin conexión.

2.3 Antes de la compra, debe destacarse toda la información que resulte crucial.

3. PROPIEDAD Y USO

La tecnología digital ha cambiado la naturaleza de muchos servicios y productos debido a que el software de conexión viene integrado en un número cada vez mayor de productos de consumo de uso general. La Internet de las cosas pone a prueba las expectativas establecidas sobre propiedad, ya que la mayoría de los productos o bien contiene un importante componente vinculado a los servicios, o se transforma en servicios, por lo que quedan sujetos a un mayor control sobre su uso, puesta en común, modificación y traspaso a servicios alternativos. Los proveedores pueden imponer sanciones de forma remota gracias a la naturaleza centralizada del control que ejercen sobre el software y las plataformas, y los consumidores están escasamente facultados para oponerse a estas sanciones o a las decisiones que se toman en relación con ellos basándose en su uso. Se producen otros problemas cuando el proveedor del software cambia de dueño y pone fin al soporte del producto, o cuando tiene procesos diferentes para la gestión de datos.

3.1 Las cláusulas contractuales y la tecnología que definen el uso de un producto o servicio de la Internet de las cosas debe ser justo a la luz de las legítimas expectativas de los consumidores, y deben garantizarse los derechos a un uso legítimo.

3.2 Los controles sobre el uso de un producto que pueden ejercer los productores deberían ser legítimos, justos y proporcionales, y las empresas deberían ceñirse a los debidos procesos.

3.3 En función de la naturaleza y funcionalidad de un producto determinado, debe garantizarse plenamente que todas las funciones básicas puedan llevarse a cabo aun cuando no se cuente con conexión a Internet.

4. SEGURIDAD Y PROTECCIÓN

La Internet de las cosas le entrega a los piratas informáticos nuevas vulnerabilidades que pueden explotarse en más entornos, y, debido a la gran cantidad de interconexiones entre los dispositivos y sistemas, es posible que permitan también una ruta más rápida hacia diversos dispositivos. Debe garantizarse la seguridad en todas las partes de un sistema conectado, ya que las vulnerabilidades en cualquier componente de dicho sistema tienen potencial de poner en riesgo al sistema completo. Los consumidores dependerán cada vez más de los fabricantes en lo que respecta a las actualizaciones y mantenimiento de la seguridad.

En muchas jurisdicciones, la actual legislación y las normas que rigen la seguridad de los productos cubren la seguridad de dispositivos individuales, pero pueden no ser adecuadas para proteger a los consumidores con respecto a los riesgos para la seguridad de la Internet de las cosas, ya que los dispositivos forman parte de un sistema mayor. Será necesario adoptar disposiciones y normas complementarias para garantizar la seguridad general de un sistema cuando los dispositivos son controlados y operados como parte de un más amplio sistema de Internet de las cosas. Este sistema más amplio conlleva también el riesgo de una conexión de menor calidad y menor seguridad, puesto que son más y más los componentes y dispositivos que comparten las mismas bandas de frecuencia.

ESTABLISHED EXPECTATIONS OF OWNERSHIP ARE CHALLENGED IN THE INTERNET OF THINGS

4.1 Deben ampliarse el concepto de "seguridad" en general y la legislación específica sobre seguridad de los productos conforme a sectores con el fin de que queden reflejadas la nueva seguridad cibernética, la seguridad de los datos y las inquietudes relativas a seguridad.

4.2 Las medidas de seguridad cibernética de la Internet de las cosas deberían entregar protección ante toda vulnerabilidad que afecte la seguridad, en particular, ante el pirateo, los accesos no autorizados y el uso indebido.

4.3 Las medidas de seguridad relativas a los datos y a la identidad de la Internet de las cosas deberían, entre otras cosas, proteger la información relacionada con pagos, con recursos financieros y con identidad personal contra todo fraude o uso indebido.

4.4 Las medidas de seguridad de los productos de la Internet de las cosas deberían proteger la seguridad personal de los consumidores, reflejando los riesgos que presentan el uso en estrecha proximidad, las bandas de frecuencia compartidas, el riesgo de exposición a campos electromagnéticos, y el potencial de interferencia con equipos conectados esenciales.

4.5 Los consumidores no deberían asumir el riesgo de los nuevos progresos en la tecnología de la Internet de las cosas, los mecanismos de supervisión del mercado deberían ser adecuados a su propósito y capaces de garantizar que los productos conectados poco seguros o con posibilidades de ser inestables no lleguen al mercado o sean retirados de inmediato cuando se identifique un peligro.

4.6 Las empresas deberían adoptar prácticas recomendables tales como la seguridad desde la concepción y predeterminada, y someterse a evaluaciones independientes de cumplimiento. En caso de producirse incidentes o vulneraciones de seguridad, deben someterse a responsabilidades de notificación oportuna y adecuada, normas sobre responsabilidad y compensación, y a sanciones en los casos de negligencia.

4.7 Companies and regulators should develop systems that make it easier for consumers to adopt safe and secure practices in the internet of things , for example simple settings, warnings and updates.

4.8 Deberían elaborarse normas internacionales que garanticen que las empresas que operan en la Internet de las cosas proporcionen las actualizaciones esenciales relativas a seguridad en todos los productos durante toda su vida útil y durante un plazo específico y razonable tras la venta.

5. RESPONSABILIDAD

La Internet de las cosas puede conectar dispositivos de diferentes fabricantes, distribuidores, o desarrolladores de software. Cuando se presentan problemas, establecer responsabilidades en virtud de las leyes y normas tradicionales puede dificultarse mucho en este complejo ecosistema de dispositivos conectados. Además, es posible que muchos participantes en cada etapa de la cadena, desde el diseño, la producción y la entrega, no cuenten con la experiencia de diseñar conformándose a la protección y seguridad de datos para dispositivos conectados.

Es necesario un nuevo enfoque hacia la responsabilidad para garantizar que los consumidores estén protegidos en un entorno en el que los productos (a) pueden fallar o ser inseguros debido a incidentes en la seguridad digital; (b) son capaces de tomar cada vez más decisiones, adelantarse y realizar pronósticos sin la intervención humana.

5.1 Es necesario que exista un marco de responsabilidades claro y robusto, que proteja a los consumidores en caso de que resulten afectados por productos o servicios conectados poco seguros. Allí donde corresponda, deberían refrendarse, reemplazarse o actualizarse las reglas del derecho de responsabilidad civil que rige las normas sobre seguridad y responsabilidad a medida que se presentan nuevos riesgos.

5.2 Debería dejarse en claro qué entidad es la responsable del desempeño y la seguridad en cada punto de la entrega del producto conectado, y durante toda la vida útil de este. Deberían existir normas claras sobre responsabilidad que garanticen que los consumidores sean plenamente compensados en caso de resultar perjudicados debido a un producto defectuoso.

5.3 Las reglas sobre responsabilidad deben cubrir todos los tipos de productos, productos de contenido digital y servicios (digitales y otros) que componen el ecosistema de la Internet de las cosas.

5.4 Deben evitarse, o al menos ampliarse, los plazos de responsabilidad a fin que cubran la vida útil prevista de un producto. También deben evitarse los umbrales de compensación con objeto de permitir una aplicación flexible de las indemnizaciones.

5.5 Todos los profesionales que intervienen en la cadena de suministro de un producto deberían compartir la responsabilidad si su actividad ha afectado la seguridad de este. Esto debería reflejar el enfoque orientado al riesgo de la ley sobre responsabilidad del producto, y evitarse los problemas en la identificación del responsable cuando el producto ha sido confeccionado por varios productores y colaboradores.

5.6 Allí donde los reclamos o problemas involucran la participación de varios proveedores o sectores, debe dejarse en claro a quién deben acudir los consumidores en busca de ayuda. Allí donde los proveedores provengan de diferentes sectores es necesario que existan mecanismos alternativos de resolución de disputas (ADR, por su sigla en inglés), y, de ser posible, estos mecanismos debería ofrecer un único contacto para los consumidores.

6. PROTECCIÓN DE LOS DATOS Y SEGURIDAD EN LÍNEA

Los consumidores deberían poder ejercer el control sobre sus datos personales y preferencias sobre privacidad. También es importante considerar los efectos de que una diversidad de productos, servicios y organizaciones acumulen información sobre las personas, así como los derechos de estas en su calidad de consumidores y ciudadanos.

Como principio, el usuario o propietario/usuario de un dispositivo debería tener el control de la forma en que se usan los datos que genera, y quién lo hace. La enorme diversidad de datos de diferentes tipos y magnitudes que pueden, no solo ser recopilados en la Internet de las cosas, sino que también pueden acumularse y fusionarse con otros datos, presenta un gran riesgo a la privacidad. Los objetos dentro del sistema conectado de la Internet de las cosas pueden recopilar datos o información que en sí mismos son inocuos, pero que, cuando se recopilan y analizan junto a otra información, pueden revelar conocimientos bastante exactos de algunas cosas tales como hábitos, ubicación e intereses de las personas, además de otra información y preferencias personales, lo que se traduce en mayor trazabilidad y perfilamiento de los usuarios.

Uno de los riesgos más importantes de la Internet de las cosas en relación con la privacidad de los datos surge del hecho que los dispositivos son capaces de comunicarse entre sí y de transferir datos de manera autónoma a un asociado externo (como por ejemplo, a un fabricante de dispositivos), y son incluso diseñados para esto. Con aplicaciones hechas con software de marca operando en segundo plano, se volverá más difícil que las personas detecten si se están procesando sus datos, y cuándo y cómo se hace esto, lo que puede limitar de gran manera la capacidad de los afectados para ejercer sus derechos a la privacidad y protección de su información.

6.1 Deben protegerse y ratificarse los derechos de los consumidores a la privacidad y a la protección de la información a fin que se aborden perjuicios tales como las prácticas discriminatorias, el mercadeo invasivo, la pérdida de privacidad y la exposición a riesgos de seguridad.

6.2 Las empresas y legisladores de la Internet de las cosas deberían revisar y reevaluar periódicamente la magnitud de la recopilación de datos personales y evaluar hasta qué punto los datos procesados son proporcionales y necesarios para la entrega del servicio que ofrecen.

6.3 Deben evaluarse e integrarse los aspectos e impactos relativos a la privacidad durante todo el ciclo, desde la concepción, al diseño y luego al desarrollo, de un producto conectado, y el ecosistema en el que opera (privacidad desde la concepción). En forma predeterminada, cualquier producto conectado debe configurarse desde el inicio en el más alto nivel de protección de la privacidad (privacidad por defecto),

evitándose la trazabilidad no deseada del comportamiento y de las actividades de los usuarios.

6.4 Debe ponerse sobre alerta a los consumidores acerca de las implicancias de la forma en que pueden usarse los datos recopilados por los productos y servicios de la Internet de las cosas y deben ofrecerse formas sencillas y eficaces de ejercer el control y mitigar los riesgos.

6.5 Los datos de los consumidores les pertenecen a ellos. Estos deben tener control pleno sobre los datos que salen de sus productos conectados y sobre su uso. Las empresas deberían ofrecer formas seguras y sencillas para que los consumidores tengan acceso a sus datos y los controlen, incluida la posibilidad de transferir sus datos a otros servicios si les parece adecuado.

Los consumidores deben ser capaces de aprovechar el valor económico de sus datos y tener otras oportunidades para intercambiarlos conforme a sus preferencias, expectativas y derechos jurídicos.

6.6 Se debería informar claramente a los consumidores acerca de qué información se recopilará, con quién se compartirá y a qué fin será destinada mientras dure la relación asociada al producto o servicio entregado. Como mínimo, los productos y servicios conectados que usan datos personales deberían regirse por políticas claras, integrales, y fáciles de comprender.

6.7 Debería informarse claramente a los consumidores si los algoritmos utilizados por los productos de la Internet de las cosas toman decisiones sobre ellos que afecten la calidad, el precio o el acceso a un servicio, y cómo se lleva a cabo esto.

6.8 Los legisladores deberían garantizar que el uso de algoritmos sea legítimo y no discrimine tomando decisiones perjudiciales basándose en información acerca de los consumidores. Los legisladores deberían considerar marcos adecuados para abordar problemas en caso de que surjan, los cuales deberían incluir el derecho a impugnar las decisiones automatizadas que tienen efectos legales.

6.9 Deberían implementarse organismos nacionales de protección de datos independientes y con recursos adecuados que tengan relevancia para la Internet de las cosas. Deberían aplicarse plenamente las leyes sobre protección de la información, y, en caso necesario, si se identifica algún perjuicio para los consumidores, estas deberían fortalecerse. Dada la importancia primordial de los datos en el contexto de la Internet de las cosas, es esencial que existan organismos independientes de protección de datos que puedan cumplir su mandato de proteger la información de los consumidores.

6.10 Deberían coordinarse políticas internacionales transfronterizas sobre flujo de datos de manera que los países involucrados establezcan normas de protección igualmente estrictas en sus legislaciones nacionales tanto de fondo como relativas a procedimientos.

7. GESTIÓN Y COMPENSACIÓN DE RECLAMOS

Los servicios interconectados pueden aumentar la comodidad eliminando la fricción de sus tareas relativas a los consumidores cuando hay participación de varios proveedores. Sin embargo, resulta difícil identificar cuál proveedor es el responsable de los fallos o problemas, al igual que el comprobar los reclamos relativos a calidad o desempeño de cosas cuyo funcionamiento depende de varios asociados dentro de la cadena. Estas dificultades no deberían afectar el derecho de los consumidores a obtener compensación.

7.1 El derecho a compensación por los productos y servicios de la Internet de las cosas no debería ser inferior a aquellos derechos disponibles en otras formas de comercio. La gestión de reclamos y los mecanismos de compensación deberían ser accesibles, asequibles, independientes, justos, responsables, oportunos y eficaces.

7.2 Las empresas que ofrecen productos y servicios en la Internet de las cosas deberían tener implementados contundentes mecanismos de resolución de disputas que no impongan retrasos o cargas irracionales a los consumidores.

7.3 Debería estar disponible el recurso a la compensación independiente para tratar aquellos reclamos que no se resuelven en forma satisfactoria a través de los mecanismos internos. Debe quedar claro el lugar al que los consumidores pueden acudir en busca de ayuda.

7.4 Allí donde los productos y servicios son transversales a diferentes jurisdicciones o sectores, los legisladores deberían trabajar más allá de esas fronteras jurisdiccionales o sectoriales a fin de apoyar la resolución transfronteriza de las disputas. También debe quedar claro el lugar al que los consumidores pueden acudir en busca de ayuda.

7.5 Debería estar disponible al público la información acumulada asociada a los reclamos y a su resolución.

7.6 Debería proporcionarse la resolución de disputas en línea sin excluir la posibilidad de hacerlo a través de otros canales.

8. COMPETENCIA Y POSIBILIDAD DE ELEGIR

Si la integración vertical y la concentración de mercado se convierten en la norma en la Internet de las cosas, será cada vez más posible que las personas queden cautivas de los productos de un proveedor determinado o en un ecosistema cerrado (efecto lock-in). Eso tiene implicancias para los consumidores que desean elegir entre diferentes aplicaciones o servicios, usar un servicio independiente de reparaciones, o vincularse a otras aplicaciones o fuentes de datos de su preferencia.

Las leyes y políticas sobre competencia deben ser adecuadas al propósito de garantizar que la Internet de las cosas sea competitiva a nivel de todos sus subsectores. Es frecuente que los consumidores tengan limitados sus derechos a usar en la forma que ellos deseen los datos que ellos mismos crean por medio de transacciones o el uso de sus dispositivos o de servicios que han comprado. Por ejemplo, a menudo resulta difícil, o imposible, tener portabilidad de datos o de contenido entre distintos proveedores. Por lo mismo, es fundamental garantizar la portabilidad de los datos, no solo para entregarles a los consumidores el control de su propia información sino también para fomentar la competencia entre los distintos servicios.

Crédito de la fotografía: Prachaya Roekdeethaweesab / Shutterstock.com

La interoperabilidad también es un elemento esencial para evitar que los consumidores queden atados a ecosistemas cerrados dentro de la Internet de las cosas. Las autoridades sobre competencia tienen una importante función que desempeñar en la promoción de un entorno dinámico y favorable para el desarrollo de la Internet de las cosas.

8.1 Deben implementarse normas sobre interoperabilidad y compatibilidad de los dispositivos y el software a fin de evitar el efecto cautivo y aumentar la capacidad de los consumidores para comparar fácilmente a los proveedores y cambiar de proveedor.

8.2 Debe ser posible la transferencia de datos entre servicios a fin de facilitar el cambio entre proveedores al tiempo que se respetan los derechos de los consumidores en cuanto a la protección de su información.

8.3 Debería prestarse atención a garantizar que el elemento de conectividad de un servicio de Internet de las cosas no se convierta en un mecanismo de cautiverio para los consumidores, y que estos puedan cambiarse fácilmente entre los distintos proveedores de conectividad.

8.4 Las instancias que legislan sobre competencia deberían considerar soluciones relativas a la competencia, como por ejemplo, exigir interoperabilidad o acceso a los datos por parte de los

competidores, una medida que estaría destinada a mitigar los efectos de la concentración de datos y el predominio de algunos participantes.

9. VIDA ÚTIL

La infatigable innovación y la competencia por lograr una participación de mercado implican tecnologías subyacentes que no detienen su avance en los dispositivos, desarrollándose procesadores más veloces, mejores cámaras y mejores baterías, entre otros. La falta de actualizaciones y la discontinuación del soporte técnico pueden hacer que productos plenamente funcionales queden rápidamente obsoletos.
Esto quiere decir que se acorta la vida útil de la mayoría de los aparatos eléctricos, lo que tiene implicancias para el uso y la eliminación de recursos, ya que apenas una fracción de los residuos electrónicos llega a reciclarse. Los residuos electrónicos suelen ser muy tóxicos, filtran metales pesados y peligrosos químicos en los suelos cercanos a los vertederos y liberan gases de efecto invernadero y emisiones de mercurio cuando se incineran. Por otro lado, los consumidores están cada vez menos satisfechos: una encuesta realizada recientemente para el estudio reveló que cerca de una tercera parte de los encuestados no se encontraba satisfecha con respecto a la vida útil de sus aparatos.

9.1 Es necesario que sea fácil modernizar los productos conectados a fin de reducir las posibilidades de que se vuelvan obsoletos.

9.2 Con independencia del lugar donde se encuentren los consumidores, deben ponerse a su disposición las actualizaciones.

9.3 En la mayor medida posible, los dispositivos, adaptadores y otros puntos de conexión deberían ser compatibles entre sí, con lo que se reducirían las posibilidades de que nuevas interfaces incompatibles los vuelvan obsoletos.

9.4 Debería entregarse a los consumidores información clara, comparable y verosímil en relación con la vida útil que se prevé para los productos y sus posibilidades de reparación.

9.5 Los productos deberían diseñarse y fabricarse teniendo presente la eficiencia, desde la sustentabilidad de los materiales a los métodos de fabricación con que se producen, y debería entregarse a los consumidores orientación clara sobre el uso, reutilización, reparación, y eliminación más eficientes tanto del producto como de sus partes componentes.

9.6 A los fines de ahorro energético, los productos deberían diseñarse de modo tal que el software que se activa en función del tiempo pueda responder en periodos de latencia o de bajo uso. Los productos de bajo consumo energético deberán tener una favorable acogida.

9.7 Deberían tomarse medidas para garantizar que la eliminación de todo metal pesado y demás sustancias peligrosas presentes en los productos conectados no sea nociva para el medioambiente ni para la salud humana.

RECOMENDACIONES GENERALES

1. MARCO REGULATORIO

La responsabilidad de garantizar que se protejan los derechos en línea, y se respeten las libertades personales y autonomía de los consumidores no es algo que puedan aplicar todos los países de manera aislada, sino que requiere la colaboración internacional de todos los gobiernos, organizaciones internacionales y empresas.

1.1 Las protecciones deberían formar parte integral del marco regulatorio, y deberían ponerse a disposición de los consumidores de la Internet de las cosas mecanismos legales, jurídicos o de supervisión eficaces, proporcionales y accesibles.

1.2 Las autoridades normativas deben cooperar entre los diferentes sectores y a través de las fronteras para abordar los problemas de los consumidores.

1.3 Los marcos de protección deberían, como mínimo, cumplir con los requisitos establecidos en las directrices y recomendaciones internacionales tales como las Directrices de Naciones Unidas de protección del consumidor, y proporcionar el mismo nivel de protección con independencia del lugar y el tipo de actividad. En aquellos lugares donde los requisitos nacionales, locales o regionales son más estrictos, estos deberían respetarse.

1.4 La legislación debería abordar todos los aspectos que se aborden en estos principios en lo que respecta a los nuevos desafíos que surgen del uso de aplicaciones de la Internet de las cosas por los consumidores.

1.5 Los países deberían acordar una manera de progresar juntos en el desarrollo de normas técnicas globales, abiertas y complementarias.

1.6 Asimismo, las autoridades normativas deben tener los conocimientos y capacidades para comprender la tecnología subyacente a la Internet de las cosas. Si no los poseen de manera interna, deberían cooperar con autoridades u organizaciones que sí las tengan.

1.7 Es esencial que se lleven a cabo mediciones serias de la percepción y experiencia de los consumidores con respecto a la Internet de las cosas y de la forma en que esta afecta su confianza y seguridad.

2. CONDUCTA EMPRESARIAL RESPONSABLE Y FUNCIÓN DE LOS ÓRGANOS DE CONTROL

El trato justo a los consumidores debería formar parte integral de los objetivos, la correcta gobernanza y la cultura corporativa de todos los proveedores de aplicaciones de la Internet de las cosas.

2.1 Como principio, las empresas que operan en distintas jurisdicciones deberían aplicar las normas más estrictas a todos sus consumidores, con independencia del lugar donde estos se encuentren.

2.2 Debería desarrollarse y fomentarse el uso de marcos éticos de evaluación del impacto en las actividades de investigación e innovación de la Internet de las cosas, los que deberían basarse en un entendimiento común de todos sus participantes a niveles nacional, regional e internacional. Dichos marcos deberían adecuarse a la evolución tecnológica y responder a las inquietudes sociales.

2.3 Los proveedores de aplicaciones y servicios de la Internet de las cosas deberían ceñirse a los lineamientos sobre prácticas recomendables contenidos en las Directrices de Naciones Unidas de protección del consumidor que establecen que todos los consumidores de productos y servicios digitales deberían recibir un trato equitativo, honesto y justo.

2.4 Debería evitarse toda práctica que aumente el riesgo de perjuicio a los consumidores, y se debería prestar especial atención a las necesidades de los consumidores menos favorecidos, como los niños y las personas con capacidades diferentes.

2.5 Los países deberían contar con órganos de control responsables de todos los aspectos de la protección de los consumidores digitales, incluida la Internet de las cosas. Tales órganos deben tener la autoridad e independencia necesarias para cumplir con sus mandatos y contar con los recursos y capacidades técnicas para responder a la evolución del sector.

3. EDUCACIÓN Y SENSIBILIZACIÓN EN MATERIA

La entrega de educación y sensibilización debería complementar, y no reemplazar, la protección normativa y legislativa. La educación es una responsabilidad común para todos los participantes tanto públicos como privados en el ecosistema de la Internet de las cosas.

3.1 Debería ofrecerse educación y sensibilización con respecto a los dispositivos de la Internet de las cosas y sus implicancias para los consumidores a través de los canales más eficientes, y esto debería hacerse de manera muy focalizada y evaluarse para garantizar que aborden las necesidades específicas de los consumidores.

3.2 La educación y sensibilización sobre la Internet de las cosas debería apoyar a los consumidores para que desarrollen las habilidades y la confianza en su manejo de los riesgos y oportunidades, tomen decisiones informadas, conozcan la manera de obtener ayuda y asesoramiento y tomen medidas para proteger y mejorar su bienestar y su identidad en la Internet de las cosas.

3.3 Las empresas, legisladores, organismos de protección de los consumidores y organizaciones de consumidores deberían colaborar entre sí en el desarrollo de sistemas que ayuden a los consumidores a comprender los riesgos y oportunidades que presentan los productos y servicios conectados.

Estos principios representan el trabajo conjunto de la ANEC, BEUC, Consumers International e ICRT

ANEC
La ANEC es la voz del consumidor europeo en materia de normalización. Representamos los intereses de los consumidores de Europa en la formulación de normas éticas, en especial aquellas que se desarrollan para apoyar la implementación de leyes y políticas públicas en el continente.
www.anec.eu

BEUC – la organización europea de los consumidores
BEUC (Oficina Europea de Uniones de Consumidores) es una organización sin fines de lucro que representa a 43 organizaciones de consumidores nacionales independientes pertenecientes a 31 países de Europa (UE, EEE y países candidatos). Durante más de 50 años, BEUC ha trabajado incansablemente como la voz de los consumidores de Europa. Llevamos la opinión de los consumidores de todo el continente hasta el escenario donde se formulan las políticas de la UE.
www.beuc.eu

Consumers International
Consumers International reúne a más de 200 organizaciones miembros en más de 100 países con el fin de empoderar y defender los derechos de los consumidores de todo el mundo. Somos la voz de los consumidores en los foros normativos internacionales y en el mercado global con el propósito de garantizarles un trato seguro, justo y honesto.
www.consumersinternational.org

ICRT
International Consumer Research & Testing (ICRT) es un consorcio global que reúne a más de 35 organizaciones de consumidores dedicadas a la investigación y realización conjunta de pruebas en el mejor interés de los consumidores. Las organizaciones miembros de ICRT no aceptan publicidad y trabajan con independencia del comercio, la industria y los partidos políticos.
www.international-testing.org