Dictamen del Comité Económico y Social Europeo sobre «Confianza, privacidad y seguridad de los consumidores y las empresas en el internet de las cosas»

(dictamen de iniciativa)

(2018/C 440/02)

Ponente: **Carlos TRIAS PINTÓ**

Coponente: **Dimitris DIMITRIADIS**

Decisión del Pleno	15.2.2018
Fundamento jurídico	Artículo 29. 2 del Reglamento interno
	Dictamen de iniciativa
Sección competente	Sección de Mercado Único, Producción y Consumo
Aprobación en sección	4.9.2018
Aprobado en el pleno	19.9.2018
Pleno n.º	537
Resultado de la votación	182/3/2
(a favor/en contra/abstenciones)	

1. **Conclusiones y recomendaciones**

1.1. El internet de las cosas (en adelante, IoT, por sus siglas en inglés), a partir de la interconectividad de personas y objetos, representa un inmenso abanico de oportunidades para los ciudadanos y las empresas, que deben venir acompañadas de una serie de garantías y controles para asegurar una implantación satisfactoria.

1.2. Teniendo en cuenta que uno de los pilares del IoT radica en la toma de decisiones automática sin intervención humana, debe garantizarse que estas no socavan los derechos de los consumidores ni conllevan en modo alguno riesgos de carácter ético o contrarios a principios y derechos humanos fundamentales.

1.3. El CESE solicita a las instituciones europeas y a los Estados miembros que:

1.3.1. velen por la protección de la seguridad y la privacidad, a través de la elaboración de los marcos regulatorios adecuados, que contemplen estrictas medidas de seguimiento y control;

1.3.2. delimiten con claridad la responsabilidad de todos los profesionales en la cadena de suministro del producto y en los flujos de información asociados al mismo, evitando los vacíos legales cuando concurren diversos productores y distribuidores;

1.3.3. establezcan recursos adecuados y mecanismos efectivos de coordinación entre la Comisión Europea y los Estados miembros para garantizar una aplicación coherente y armonizada tanto de la normativa que se someta a revisión como de la nueva regulación, abordando en paralelo el entorno internacional;

1.3.4. vigilen el desarrollo de las tecnologías emergentes relacionadas con el IoT, para garantizar un nivel elevado de seguridad, plena transparencia y una accesibilidad equitativa;

1.3.5. fomenten las iniciativas de normalización europeas e internacionales para garantizar la fiabilidad, disponibilidad, resistencia y mantenimiento de los productos;

1.3.6. vigilen los mercados y preserven el *level playing field* en la implementación del IoT, evitando la concentración de poder económico transnacional en los nuevos actores tecnológicos;

1.3.7. se comprometan a promover acciones de sensibilización y capacitación en competencias digitales, de la mano de la investigación fundamental e innovación en la materia;

1.3.8. garanticen la plena aplicación y una utilización eficaz de los sistemas de resolución alternativa de litigios o de resolución de litigios en línea (RAL y RLL), y

1.3.9. aseguren la existencia, la aplicación y el funcionamiento eficaz de un sistema europeo de acciones colectivas que permita las órdenes de cesación y la obtención de una indemnización en aquellos casos en que el uso del IoT cause daños o perjuicios de carácter colectivo, como se desprende del Nuevo Marco para los Consumidores.

1.4. La confianza de los consumidores vendrá asociada tanto al estricto cumplimiento de la legislación correspondiente como a la comunicación de buenas prácticas empresariales en materia de privacidad y seguridad, y es deber de las instituciones engarzarlas con las estrategias de responsabilidad social corporativa y de inversión socialmente responsable.

1.5. El impacto social y económico del IoT se acrecentará positivamente en la medida en que se entrelace adecuadamente con el desarrollo de políticas socioambientales en el marco de la economía colaborativa, la economía circular y la economía de la funcionalidad.

2. **Antecedentes y contexto**

2.1. Durante los quince últimos años, la irrupción de internet ha producido transformaciones en todos los ámbitos de la vida cotidiana, afectando a los diferentes hábitos de consumo. Se prevé que en los próximos diez años la revolución del internet de las cosas alcance los sectores energético, agropecuario o de transportes, así como los más tradicionales de la economía y la sociedad, lo cual lleva a diseñar políticas integrales que aborden de forma inteligente esta disrupción tecnológica.

2.2. El concepto de IoT surgió en el Instituto de Tecnología de Massachusetts (MIT), y su idea radica básicamente en un mundo lleno de dispositivos totalmente interconectados de manera que puedan automatizarse en conjunto los distintos procesos interoperables. Por su parte, la Unión Europea lleva preparándose para abordar la convergencia digital y los nuevos desafíos del IoT desde el lanzamiento del plan «i2010: Una sociedad de la información europea para el crecimiento y el empleo» ([1]), hasta el reciente Plan de Acción de IoT (véase el documento *Advancing the Internet of Things in Europe*, que formó parte en 2016 de la Comunicación «Digitalización de la industria europea. Aprovechar todas las ventajas de un mercado único digital») ([2]).

2.3. El CESE se ha pronunciado en numerosas ocasiones sobre la cuarta revolución industrial, marcada por la convergencia de tecnologías digitales, físicas y biológicas, y se remite en particular al Dictamen emitido en 2017 ([3]). De hecho, el IoT es el ámbito predilecto de aplicación de las formas más avanzadas de IA y donde los principios definidos por el CESE son puestos a prueba, en particular el principio de que los seres humanos tengan en todo momento control.

2.4. Los dispositivos del IoT carecen a menudo de las normas de autenticación necesarias para mantener la seguridad de los datos de usuario. Esto da lugar a la aparición de problemas, al quedar expuestos a fallos de seguridad los dispositivos, los datos y los miembros de la cadena de suministro.

2.5. Las tecnologías emergentes, como la cadena de bloques, pueden resolver problemas de seguridad y confianza: pueden utilizarse para rastrear las mediciones de los datos procedentes de sensores y evitar no solo la duplicación con cualquier otro dato malintencionado sino también preservar la integridad y la trazabilidad de las modificaciones; un libro de contabilidad distribuido puede permitir la identificación de dispositivos del IoT, la autenticación y la transferencia de datos segura, sin fallas; los sensores del IoT pueden utilizarse para intercambiar datos a través de una cadena de bloques en lugar de un tercero; el uso de contratos inteligentes permite la autonomía de los dispositivos, así como la identidad individual y la integridad de los datos; los costes de creación y funcionamiento se reducen al no haber intermediarios; por último, los dispositivos del IoT de la cadena de bloques proporcionan el historial de los dispositivos conectados, muy útil si es necesario resolver problemas ([4]).

([1]) COM(2005) 229 final.
([2]) COM(2016) 180 final.
([3]) Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad (DO C 288 de 31.8.2017, p. 1).
([4]) Véase Khwaja Shaik, *Why blockchain and IoT are best friends*, https://www.ibm.com/us-en/?lnk=m; sobre las innovaciones en el sector financiero europeo, véase DO C 246 de 28.7.2017 p.8.

2.6. Por otra parte, se están desarrollando tecnologías de contabilidad distribuida de código abierto para el intercambio de información y valor entre máquinas en el IoT. No permiten la minería de datos pero utilizan una arquitectura inspirada en un concepto matemático llamado gráfico acíclico dirigido (DAG), que evita las comisiones y propicia que la red aumente su capacidad conforme se incremente el número de usuarios.

2.7. Estamos ante un hecho con un gran potencial económico y social ([5]), que presenta grandes oportunidades pero también importantes desafíos asociados a riesgos implícitos, con un carácter multidisciplinar y transversal que afecta por igual a empresas y consumidores, administraciones y ciudadanos. Por ello, el tratamiento de este asunto debe contemplar un enfoque común y, a la vez, particularizado en todo aquello que resulte singular para una u otra condición. Al respecto, basta apuntar que Naciones Unidas estimaba para 2020 en cincuenta mil millones los dispositivos interconectados, con aplicaciones para consumidores a través de televisores, refrigeradores, cámaras de seguridad, vehículos, etc.

2.8. Las aplicaciones del IoT ya arrojan beneficios económicos y sociales en el marco de un mundo globalizado, entre otros, más servicios sensibles al contexto socioeconómico, ciclos de retroalimentación más cortos, reparaciones a distancia, soportes para la toma de decisiones, mejor asignación de recursos o un control remoto de servicios. Sin embargo, hay factores asociados muy sensibles, tales como la privacidad y la seguridad, la asimetría informativa y la transparencia de las transacciones, responsabilidades complejas, bloqueos de productos y sistemas, o también, un incremento de los productos híbridos que puede afectar en términos de propiedad y exponer a los consumidores a la aplicación de contratos a distancia, con la consiguiente merma de garantías.

2.9. Los ingentes desafíos legales a los que se enfrentan la UE y sus Estados miembros se explican por el hecho de que muchas de las características específicas del IoT (altos niveles de complejidad y alta interdependencia, el elemento de autonomía, los componentes de generación y/o procesamiento de datos, y una dimensión abierta) son compartidas con otras tecnologías digitales emergentes como la *blockchain*, la impresión en 3D y la computación en la nube. En opinión del CESE, el documento de trabajo de la Comisión Europea ([6]) sobre la responsabilidad de las tecnologías digitales emergentes da un paso más en la dirección adecuada.

2.10. En definitiva, maximizar beneficios y minimizar los riesgos asociados al IoT conlleva facilitar información accesible, clara, concisa y precisa, promoviendo en particular la inclusión y la conectividad digital de los consumidores más vulnerables, mediante el diseño de productos y servicios plenamente trazables que incorporen normas integradas de confianza, privacidad y seguridad.

3. **Confianza de consumidores y empresarios en el IoT**

3.1. El IoT es un complejo ecosistema que permite la interconexión de dispositivos procedentes de diferentes fabricantes, distribuidores o desarrolladores de *software*, lo que puede generar dificultades para determinar la responsabilidad en situaciones de incumplimiento normativo, o de daños materiales u otros daños a terceros o a sistemas causados por productos defectuosos o por el uso indebido de los productos en la red por parte de terceros, excluidos los usuarios finales. Incluso cabe la posibilidad de que muchos de los operarios que participan en la cadena de valor global del producto no cuenten con suficientes conocimientos y experiencia en temas de seguridad o de protección de datos para dispositivos en red.

3.2. Por ello se requiere un nuevo enfoque de las responsabilidades orientado a garantizar que tanto los consumidores como las empresas que adopten aplicaciones de IoT estén protegidos en un entorno en el que productos con una configuración adecuada puedan volverse defectuosos e inseguros como resultado de incidentes de seguridad digital o utilizarse indebidamente (por ejemplo, por piratas informáticos). Este entorno debe permitir anticipar, prevenir y protegerse de aquellas decisiones automatizadas que puedan vulnerar los fundamentos éticos y los derechos humanos universalmente reconocidos.

([5]) Digital McKinsey estima que el IoT tiene un impacto económico potencial de 3,9 a 11,1 billones USD anuales.
([6]) SWD(2018) 137.

3.3. El CESE aplaude tanto la revisión de la aplicación de la Directiva de 1985 en materia de responsabilidad por los daños causados por productos defectuosos ([7]) como la reciente creación del grupo de expertos *multistakeholder* sobre responsabilidad y nuevas tecnologías, para garantizar un equilibrio justo entre los intereses de los productores y los consumidores. Un nuevo marco de responsabilidad deberá contemplar de forma clara la trazabilidad de la responsabilidad y la seguridad tanto a lo largo de la cadena de valor del producto como durante su ciclo de vida, incorporando la sostenibilidad como nuevo factor que obligará a contemplar la actualización, mejora, portabilidad, compatibilidad, reutilización, reparación o readaptación del producto.

3.4. También debe ser objeto de consideración específica para el IoT la determinación de responsabilidad de todos los profesionales en la cadena de suministro del producto, evitando los vacíos legales cuando concurren diversos productores y distribuidores. El CESE considera imprescindible especificar claramente los procedimientos que los consumidores deben seguir en cada caso, promoviendo los mecanismos de resolución alternativa de litigios (ADR, por sus siglas en inglés).

3.5. El CESE hace hincapié en la importancia de la información precontractual y la transparencia de las cláusulas que se estipulen, así como de las instrucciones de uso de los dispositivos, con advertencia explícita de los posibles riesgos asociados y de la cobertura de los mismos.

3.6. La interoperabilidad y compatibilidad de los dispositivos y *software* asociados debe garantizarse, para evitar bloqueos y posibilitar al consumidor comparar proveedores. El CESE remarca que este factor también es clave para establecer un *level playing field* entre grandes empresas y pymes.

3.7. Finalmente, el CESE aboga por respetar la neutralidad de la red y exhorta a la Comisión a que ejerza una estricta vigilancia de la conducta de mercado.

4. **Privacidad de los consumidores en el IoT**

4.1. Los consumidores han visto reforzada la capacidad de ejercer control sobre sus datos personales y preferencias de privacidad con el nuevo Reglamento General de Protección de Datos (RGPD) ([8]). El usuario de un dispositivo debe tener el control de cómo se utilizan los datos que genera y quién puede acceder a ellos, teniendo en cuenta que la diversidad de datos, así como la agregación y vinculación a otros datos, suponen un grave riesgo para la privacidad en el ecosistema del IoT.

4.2. Conviene tener presente la incidencia que la multiplicidad de productos, servicios o entidades puede tener en la privacidad y en la protección de datos cuando estos se transfieren de forma autónoma con arreglo a su interconectividad. Y del mismo modo, en aquellos casos en los que se trata o reelabora la información a partir de datos inicialmente inocuos, se podría llegar a adquirir un conocimiento preciso de hábitos, ubicaciones, intereses y preferencias de los individuos, lo que incrementa la accesibilidad y rastreabilidad del perfil del usuario.

4.3. Las garantías jurídicas deben asegurar la plena capacidad de los usuarios para ejercer sus derechos de privacidad y protección de datos personales sin limitación alguna, evitando así potenciales daños como las prácticas discriminatorias, la comercialización invasiva, la pérdida de privacidad o las violaciones de seguridad. Por otra parte, los consumidores deberían tener información sobre el valor económico de sus datos y reservarse el derecho de poder compartirlos.

4.4. Como ya dispone el RGPD, empresas y reguladores deberán revisar periódicamente el alcance de la recopilación de datos personales y evaluar en qué medida los datos procesados son proporcionados y necesarios para la realización del servicio. Los aspectos e impactos de privacidad deben evaluarse a lo largo de toda la concepción, ciclo de diseño y desarrollo de un producto conectado y el ecosistema en red en el que opera (privacidad por diseño). Por consiguiente, los principios de protección de datos desde el diseño y por defecto deben aplicarse de manera coherente en el IoT.

4.5. Así mismo, de forma predeterminada, la configuración de cualquier producto conectado debe establecerse en el nivel más alto de protección de la privacidad (por diseño y por defecto), evitando el seguimiento no deseado del comportamiento de los usuarios y sus ocupaciones.

([7]) COM(2018) 246 final.
([8]) Vigente desde el 25 de mayo de 2018.

4.6. En todo caso, los consumidores deberán conocer de forma fehaciente los datos que se recopilan, quienes acceden a ellos y la utilidad que se les pretende dar mientras la relación de producto o servicio se mantenga activa, así como la política de privacidad aplicable y si los algoritmos utilizados afectan a la calidad, el precio o el acceso a un servicio.

5. **Seguridad de consumidores y empresarios en el IoT**

5.1. La interconectividad de dispositivos que caracteriza el ecosistema del IoT puede alentar el desarrollo de prácticas tecnológicas ilegales o indeseables, convirtiéndose en un espacio propicio para la vulnerabilidad y su propagación viral. Por ello debe acometerse la seguridad de forma integral, en todos y cada uno de los componentes del sistema.

5.2. La oferta de productos y actualizaciones vinculadas a la ciberseguridad deberá ser justificada y brindar cobertura no solo a dispositivos individuales, sino extenderse también a los riesgos de seguridad que comporta la interconectividad con otros dispositivos en el IoT, no reduciéndose por razón de su número los estándares de calidad de dicha seguridad.

5.3. A este respecto, la propuesta de Reglamento relativo a la Agencia de Ciberseguridad de la UE ([9]) incluye un marco de certificación de las tecnologías de la información y la comunicación que permitirá la definición de esquemas de certificación de seguridad y etiquetado para diferentes tipos de productos, entre los que se encuentran los del IoT. Si bien el CESE aplaude esta medida, también expresa su preocupación por el hecho de que no tenga carácter obligatorio.

5.4. Las medidas de ciberseguridad deberían abarcar los riesgos contra cualquier tipo de vulnerabilidad y, en particular, el *hackeo*, el acceso no permitido o el mal uso, así como en lo relativo a los medios de pago y los fraudes financieros. A este respecto, el CESE respalda las competencias atribuidas al grupo de expertos *multistakeholder*sobre responsabilidad y nuevas tecnologías.

5.5. Asimismo, deberá contemplarse la seguridad personal de los consumidores ante riesgos como el uso de proximidad, las bandas de frecuencia compartidas, la exposición a campos electromagnéticos o posibles interferencias con equipos vitales conectados. El CESE aboga por aplicar medidas de vigilancia y retirada preventiva ante riesgos que afecten a la salud y la seguridad de los consumidores o a sus intereses personales y económicos.

5.6. Las empresas deberán adoptar estándares de buenas prácticas, como la seguridad por diseño y por defecto, y someterse a evaluaciones externas independientes. En caso de incidentes de seguridad o violaciones de datos, las empresas estarán obligadas a notificar dichas incidencias, incluyendo información relativa a la responsabilidad por daños e incumplimiento normativo.

5.7. Las empresas deberán facilitar a los consumidores información sencilla y accesible que les permita tomar decisiones adecuadas y adoptar prácticas seguras, proporcionando las actualizaciones de seguridad que resulten esenciales a lo largo del ciclo de vida del producto.

5.8. Debe abordarse la falta de normas coherentes en relación con las redes de IoT. Es preciso desarrollar tecnologías avanzadas de banda ancha y de nueva generación que mejoren las actuales infraestructuras.

6. **Propuestas de acción en el marco de las políticas públicas** ([10])

6.1. Los poderes públicos, en el ejercicio de sus competencias en los diferentes ámbitos territoriales de la Unión Europea, deberán participar activamente en la elaboración de las políticas y planes de acción del IoT con el objetivo de lograr un equilibrio entre las distintas partes interesadas, anticipando las problemáticas y paliando prudencialmente los posibles efectos adversos. El CESE propone:

6.1.1. crear entornos de prueba (*sand boxes*), es decir, espacios físicos, *clusters*, etc., para los proyectos piloto y las pruebas de concepto; Estos deberían tener como objetivo ensayar no solo tecnologías, sino también los modelos de reglamentación ([11]).

([9]) Véase el COM(2017) 477 final.

([10]) Véase el informe del Grupo del Banco Mundial, *Internet of Things: The New Government-to-Business Platform* (informe sobre el internet de las cosas, la nueva plataforma gobierno-empresa).

([11]) Véase https://ec.europa.eu/digital-single-market/en/news/eu-and-eea-member-states-sign-cross-border-experiments-cooperative-connected-and-automated.

6.1.2. financiar infraestructuras tecnológicas que permitan el desarrollo de proyectos innovadores de IoT en el marco del nuevo programa «Horizonte Europa»;

6.1.3. designar institutos y agencias independientes como facilitadores y supervisores de los proyectos del IoT. El CESE se congratula de las medidas contempladas a este respecto en el Reglamento de 2017 relativo a la ciberseguridad y demanda a la Comisión que impulse de forma eficaz y con los recursos presupuestarios adecuados los procesos de normalización para la industria digital ([12]);

6.1.4. impulsar asociaciones y plataformas de colaboración público-privadas, en las que participen la comunidad científica, la industria y los consumidores;

6.1.5. alentar las inversiones en el desarrollo de modelos empresariales locales que aprovechen los beneficios del IoT y faciliten que se aborden aspectos tan complicados como la protección y la propiedad de los datos;

6.1.6. llevar a cabo acciones de capacitación en el ámbito empresarial desde la óptica de la corresponsabilidad. Es preciso garantizar que la seguridad y la privacidad por diseño y por defecto se integren en los productos y servicios de las TIC, de acuerdo con el principio del «deber de diligencia» que propugna el nuevo Reglamento sobre ciberseguridad. A este respecto, el CESE saluda la prevista elaboración de **códigos de conducta**, complementarios a la acción normativa;

6.1.7. fomentar las iniciativas de normalización europeas e internacionales para garantizar que los sistemas de IoT dispongan de las características esenciales, es decir, fiabilidad, inocuidad, disponibilidad, resistencia, mantenibilidad y utilización. En particular, la normalización es esencial para la rápida realización de procesos de fabricación industrial altamente digitalizados;

6.1.8. garantizar un acceso asequible y de alta calidad a los usuarios del IoT, en particular, a la población más vulnerable o que resida en áreas menos pobladas;

6.1.9. impulsar campañas de sensibilización y programas educativos para facilitar la adopción del IoT por parte de las empresas y de los consumidores, habilitando la adquisición de las capacidades y competencias precisas ([13]), con especial atención a los colectivos vulnerables y a la diversidad;

6.1.10. emprender iniciativas en el ámbito educativo para una adecuada prevención, dada la incorporación precoz de la población infantil a los entornos digitales;

6.1.11. realizar análisis y estudios diagnósticos del impacto del IoT en los nuevos modelos de producción y consumo sostenibles;

6.1.12. garantizar la plena aplicación y una utilización eficaz de los sistemas de resolución alternativa de litigios o de resolución de litigios en línea (RAL y RLL), y

6.1.13. asegurar la existencia, la aplicación y el funcionamiento eficaz de un sistema europeo de acciones colectivas que permita las órdenes de cesación y la obtención de una indemnización en aquellos casos en que el uso del IoT cause daños o perjuicios de carácter colectivo, como se desprende del Nuevo Marco para los Consumidores.

6.2. Asimismo, el CESE demanda a la Comisión que evalúe la normativa relacionada directa o indirectamente con el IoT y, en su caso, mejore los actos legislativos en vigor. En ese sentido, el ***New Deal for Consumers*** debería poner también la lupa tanto sobre los dispositivos que se conectan como sobre las redes y su seguridad, así como sobre los datos asociados a los dispositivos.

6.3. Finalmente, el CESE señala la importancia de dotarse de mecanismos de cooperación y coordinación entre los Estados miembros para una aplicación eficiente y uniforme de las regulaciones previstas, así como para los convenios que la Unión Europea deba establecer fuera de su territorio debido a la ubicación de las sedes de empresas y proveedores, con especial énfasis en el intercambio de mejores prácticas. La política internacional sobre flujos de datos transfronterizos debe coordinarse para que los países involucrados puedan establecer normas de protección igualmente elevadas en sus leyes nacionales, tanto sustantivas como procesales.

Bruselas, 19 de septiembre de 2018.

El Presidente
del Comité Económico y Social Europeo
Luca JAHIER

([12]) DO C 197 de 8.6.2018, p. 17.
([13]) DO C 434 de 15.12.2017, p. 36.