CONSUMERPRO

BOOSTING PROFESSIONALS
IN CONSUMER PROTECTION

Derechos Digitales

Antecedentes Teóricos

2022- 2023

Digital Rights - Spain
January 2023 - version 1

European Commission

1. ÍNDICE

Este material fue producido en el contexto del Proyecto *Consumer PRO,* que es una iniciativa de la Comisión Europea en el marco del Programa Consumidor Europeo. El apoyo de la Comisión Europea no constituye una aprobación del contenido, que refleja únicamente los puntos de vista de los autores. La Comisión no se hace responsable del uso que pueda hacerse de la información contenida en el mismo.

2. INTRODUCCIÓN AL DOCUMENTO DE ANTECEDENTES TEÓRICOS

Querido lector:

Este documento de antecedentes teóricos es parte de los recursos de capacitación desarrollados para Consumer Pro, una iniciativa de la UE que tiene como objetivo hacer que las organizaciones de consumidores y otros actores en la política del consumidor estén mejor equipados para proteger a las personas consumidoras en su país.

El objetivo de este documento es brindarle a usted y a sus equipos información útil y relevante sobre los derechos digitales. Su contenido ha sido elaborado por expertos en políticas de derechos digitales de BEUC, desde una perspectiva europea y con el fin de proporcionar las claves para:

- Capacitar rápidamente a sus equipos de profesionales;
- Encontrar fácilmente la información pertinente;
- Permitir que su personal informe mejor a los consumidores sobre sus derechos y,
- Sensibilizar a sus ministerios y autoridades nacionales sobre los derechos digitales.

Este documento de antecedentes teóricos forma parte de una serie de recursos de formación que pretenden adaptarse a las especificidades nacionales, si las hay. Existen otros documentos de antecedentes teóricos complementarios relativos a los derechos digitales y la compensación colectiva, que se encuentran accesibles previa solicitud o en línea, tanto en inglés como en muchos otros idiomas europeos.

Acerca de Consumer PRO

Consumer PRO es una iniciativa de la Comisión Europea en el marco del Programa Europeo de Consumidores, que se encuentra implementada por BEUC, la Organización Europea de Consumidores. Su objetivo es desarrollar la capacidad de las organizaciones europeas de consumidores y otros actores en la política de consumo, a través de la educación no formal. El proyecto cubre los Estados miembros de la UE, Islandia y Noruega.

Para obtener más información, escriba a Info@consumer-pro.eu.

1. PROTECCIÓN DE DATOS

1.1. Introducción e historia de la política de consumo de Protección de Datos

La protección de las personas físicas frente al tratamiento de datos personales es un derecho fundamental en la Unión Europea. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE), establecen que toda persona tiene derecho a la protección de los datos personales que le conciernen. Además, el artículo 7 de la Carta de los Derechos Fundamentales establece que toda persona tiene derecho al respeto de su vida privada y familiar, del domicilio y de las comunicaciones.

Por su parte, el Reglamento General de Protección de Datos (RGPD) regula el procesamiento de datos personales en la UE. El mismo requiere que las organizaciones, tanto organismos públicos como empresas, utilicen los datos personales de los consumidores de manera transparente y justa. En tal sentido, el Reglamento refuerza los derechos de las personas consumidoras, y se aplica a todas las organizaciones que procesan datos personales que se encuentren en la UE, con independencia de dónde tenga su sede la organización.

Las normas sobre privacidad electrónica o ePrivacy (actualmente la Directiva sobre privacidad electrónica, que está en revisión) protege la confidencialidad de las comunicaciones electrónicas, así como también contienen protecciones específicas para las personas consumidoras frente las comunicaciones comerciales no solicitadas y enviadas a través de servicios de comunicación electrónica.

1.2. ¿Por qué la protección de datos es importante para las personas consumidoras?

Las tecnologías de la información digital y la aparición de nuevos servicios en línea indudablemente benefician a las personas consumidoras. Sin embargo, lo cierto es que también representan un gran desafío para los derechos fundamentales de privacidad y de protección de datos personales. En efecto, los modelos de negocios que actualmente dominan el mundo digital se basan en rastrear y analizar cada movimiento de los consumidores. Las empresas utilizan la información que recopilan para crear perfiles de usuario, que se comercializan en línea y se utilizan para ofrecer publicidad orientada al comportamiento. Ahora bien, tales perfiles también podrían utilizarse para discriminar a los consumidores e influir en su comportamiento. Por ello, es importante garantizar que las

personas consumidoras puedan mantener el control de sus datos personales y, a su vez, beneficiarse de productos y servicios digitales, sin tener que renunciar a su privacidad.

1.3. Principales retos en materia de política de consumo de Protección de Datos

Es muy difícil para los consumidores poder controlar lo que sucede con sus datos en la práctica. Muchas veces sus derechos no se respetan y, a menudo, se ven obligados a renunciar a su privacidad para poder utilizar productos y servicios digitales.

Las personas consumidoras están bajo constante vigilancia comercial y sus datos personales son explotados por una gran cantidad de empresas, muchas de las cuales ni siquiera conocen. Asimismo, las políticas de privacidad son vagas, largas, complejas y muy difíciles de entender, por lo que el consumidor no tiene más remedio que estar de acuerdo. En efecto, existe una falsa ilusión de control, en tanto en aquellos casos en los que se pide el consentimiento de las personas, esto se convierte en un ejercicio sistemático y sin sentido de "marcar la casilla".

Cabe destacar que el RGPD estaba destinado a abordar muchos de estos problemas. Sin embargo, lo cierto es que, a casi cuatro años de su entrada en vigencia, no ha habido cambios significativos en las prácticas comerciales. El nivel de cumplimiento en ciertas áreas es bajo y, por el momento, la aplicación no es del todo eficiente. Las autoridades de protección de datos tienen dificultades para hacer frente a todas las denuncias que reciben y la nueva estructura de cumplimiento, construida en torno a un mecanismo de cooperación y coherencia para garantizar la interpretación y aplicación coherentes de la ley en toda la UE, se enfrenta a importantes desafíos.

Por otro lado, la reforma de las reglas de ePrivacy, que pretenden complementar el RGPD y proteger aún más la confidencialidad de las comunicaciones, está pendiente desde hace más de cinco años y aún no hay un acuerdo a la vista. (Para obtener más información sobre el Reglamento de privacidad electrónica, consulte la hoja informativa de BEUC).

1.4. Principales derechos y obligaciones de las personas consumidoras

El RGPD exige, tanto a las entidades públicas como a las empresas, que utilicen los datos personales de los consumidores de manera transparente y justa. A tal efecto, el Reglamento establece una serie de principios que regulan el uso de tales datos. Asimismo, reconoce una serie de derechos a las personas consumidoras con el fin de garantizar que puedan tener el control de sus datos. Entre otros, se reconocen los siguientes derechos:

- A ser informado, de forma clara y sencilla, cómo se están utilizando sus datos personales. Se debe incluir la información acerca de qué datos se utilizan, por quién y con qué fines.
- A Acceder a los datos personales que tienen las organizaciones y obtener una copia de los mismos.
- A rectificar los datos personales que sean inexactos.
- A la eliminación de sus datos personales.
- A pedir que dejen de usar sus datos, ya sea de manera temporal o permanente.
- A recibir sus datos en un formato de uso común, de manera que puedan tomarlos u utilizarlos en otro lugar.
- A impugnar las decisiones automatizadas que se basen en sus datos personales que le afecten de manera significativa (por ejemplo, que denieguen un préstamo).
- A ser informado en caso de pérdida o robo de sus datos.
- A presentar reclamaciones ante su autoridad nacional de protección de datos o acudir a los tribunales.

1.5. Leyes y Reglamentos a nivel nacional y de la UE

- Carta de los Derechos Fundamentales de la UE
- Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD)
- Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) - Modificada por Directiva 2009/136/CE
- Directrices, recomendaciones y mejores prácticas del Comité Europeo de Protección de Datos
- Opiniones del Supervisor Europeo de Protección de Datos
- Ejemplo de Código de Conducta: Federación de Marketing Directo

A nivel nacional

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vigente en los artículos referidos en la Disposición adicional decimocuarta y Disposición transitoria cuarta de la Ley Orgánica 3/2018, de 5 de diciembre.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- AEPD: Guía del Reglamento General de Protección de Datos para responsables de tratamiento, con la información y las explicaciones necesarias para preparar y adoptar medidas correspondientes para cumplir con las previsiones del Reglamento UE.
- AEPD: Directrices para la elaboración de contratos entre responsables y encargados de tratamiento, para identificar los puntos clave a tener presente en el momento de establecer la relación entre el responsable y el encargado del tratamiento, así como cuestiones que afectan de forma directa a la gestión de la relación entre ambos.
- AEPD: Guía para el cumplimiento del deber de informar, para orientar las mejores prácticas para informar a los interesados, en virtud del principio de transparencia, acerca de las circunstancias y condiciones del tratamiento de datos a efectuar, así como los derechos que les asisten.
- AEPD: Orientaciones y garantías en los procedimientos de anonimización de datos personales, para garantizar la protección de datos personales en el desarrollo de estudios e investigaciones de interés social, científico y económico, e impulsar su desarrollo y divulgación.
- APED: Guía práctica de análisis de riesgos, hoja de ruta enfocada a la gestión de riesgos potenciales asociados al tratamiento de datos desde su diseño, mediante el establecimiento de medidas de seguridad y control para garantizar los derechos y libertades de las personas.
- AEPD: Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al Reglamento UE
- AEPD: Listado de cumplimiento normativo para facilitar la adaptación al Reglamento UE.

- AEPD: Guía de brechas de seguridad, dirigida a responsables de tratamientos de datos personales, con el objetivo de facilitar la interpretación del Reglamento UE en lo relativo a la obligación de notificar a la autoridad competente y, en su caso, a los afectados.
- Guías de la AEPD

1.6. Jurisprudencia

Para obtener un repositorio de las decisiones de la Autoridad de Protección de Datos y de los Tribunales, así como artículos sobre el RGPD, visite: www.GDPRHub.eu.

En el portal legal oficial de la UE: archivo Eurlex sobre el RGPD. Encontrará una lista de casos del Tribunal de Justicia de la Unión Europea y cuestiones preliminares relacionadas con el RGPD (encuentre la lista de jurisprudencia en "información del documento").

1.7. ¿Qué pueden hacer las personas consumidoras si tienen un problema?

Si un consumidor considera que se han vulnerado sus derechos bajo el RGPD tiene dos opciones:

- Presentar un reclamo ante la autoridad nacional de protección de datos. Puedes encontrar la lista completa aquí.
- Presentar una acción contra una empresa/organización directamente ante los tribunales. De todas maneras, esta opción no impide que el consumidor también presente una reclamación ante las Autoridades Nacionales de Protección de Datos, si así lo desea.

Asimismo, si la persona consumidora considera que las Autoridades de Protección de Datos no han tramitado correctamente su reclamación o, si no está satisfecho con la respuesta obtenida, o no es informado, en un plazo de 3 meses desde el día en que presentó la reclamación, acerca del progreso o el resultado de su reclamo, podrá iniciar una acción directamente ante los tribunales contra las propias autoridades de protección de datos.

Autoridades públicas a nivel nacional:

En España:

A nivel estatal:

- la Agencia Española de Protección de Datos (AEPD)

A nivel autonómico:

- La Autoridad Catalana de Protección de Datos.
- La Agencia Vasca de Protección de Datos.
- El Consejo de Transparencia y Protección de Datos de Andalucía.

Además de las Autoridades Nacionales de Protección de Datos, vale la pena considerar otros organismos públicos, a saber:

A nivel europeo:

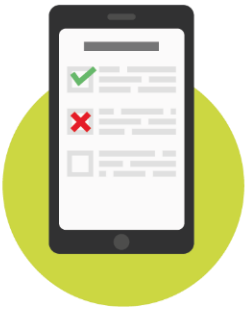
- La Comisión Europea, que está a cargo de garantizar que los Estados miembros implementen correctamente el RGPD. Asimismo, tiene la potestad de "activar" ciertas disposiciones del RGPD a través de actos delegados (por ejemplo, para la creación de "iconos de privacidad" estandarizados).
- El Comité Europeo de Protección de Datos (CEPD), que reúne a todas las Autoridades Nacionales de Protección de Datos. Su tarea principal es asegurar la coherencia en la aplicación e interpretación del RGPD.
- El Supervisor Europeo de Protección de Datos (SEPD), que supervisa el respeto de los datos personales de las personas por parte de las instituciones de la UE y las asesora en materia de protección de datos.

Resolución Alternativa de Conflictos (RAC)

Se pueden establecer, a través de códigos de conducta adoptados por entidades de la industria (artículo 40 del RGPD), procedimientos extrajudiciales y de resolución de conflictos relativos al procesamiento de datos personales entre los controladores y los interesados,, sin perjuicio del derecho a presentar reclamos ante la Autoridad de Protección de Datos y de buscar remedios judiciales.

1.8. Otros recursos: hojas informativas, publicaciones, enlaces

- Sitio web de la Comisión Europea con información sobre RGPD
- Biblioteca de la Comisión Europea sobre el RGPD - Infografías, fichas informativas y otros materiales dirigidos a ciudadanos y empresas
- Hoja informativa de BEUC: ¿Qué implica para usted la ley de protección de datos de la UE?
- Informe de BEUC: Un largo y sinuoso camino: un caso de aplicación de la protección de datos transfronteriza desde la perspectiva del consumidor
- AccessNow – Guía del usuario sobre protección de datos en la UE: Sus derechos y cómo ejercerlos
- Agencia de Derechos Fundamentales – Manual Europeo de Protección de Datos
- Guías publicadas por las Autoridades de Protección de Datos a nivel nacional
- Hojas informativas publicadas por el Supervisor Europeo de Protección de Datos (SEPD)
- La historia del RGPD y un glosario (SEPD)



2. PLATAFORMAS

2.1. Introducción e historia de la política del consumidor relativa a las Plataformas

Las personas consumidoras compran cada vez más servicios y productos en línea, particularmente a través de plataformas.

En los primeros años del comercio electrónico, tales compras se realizaban principalmente a través de los sitios web de empresas que también tenían establecimientos físicos en las calles principales.

Sin embargo, lo cierto es que, en la actualidad, el comportamiento de compra de los consumidores está cambiando radicalmente. En efecto, las personas requieren, cada vez más, de productos y servicios a través de mercados en línea. Además, estos son enviados a consumidores europeos directamente desde fuera de la UE.

Así, las compras no solo se realizan únicamente a través de plataformas de comercio electrónico como Amazon Marketplace, AliExpress, wish.com o eBay, sino también a través de las redes sociales, como Instagram.

Por ejemplo, en 2017 aproximadamente 100 millones de ventas fueron despachadas desde China a Alemania. Esto representa 40 millones más que en 2016. Asimismo, se ha informado un gran aumento de estas actividades en otros países europeos.

Además, debe destacarse que han aumentado las estafas relativas a tiendas web creadas en la UE por vendedores que se hacen pasar por empresas europeas, pero que en realidad están haciendo pedidos a plataformas de China y vendiendo estos productos a los consumidores a un precio más alto que, por ejemplo, en wish.com. Esto se ha observado en Dinamarca y en Francia[1].

Por su parte, debe destacarse que existen, además, serias preocupaciones porque muchos de estos productos no cumplen con las leyes europeas y los estándares técnicos que existen para proteger los derechos de los consumidores, la seguridad, la salud y el medio ambiente[2]. Si bien los fabricantes y distribuidores ubicados en la UE pueden ser considerados responsables de la seguridad y el cumplimiento de los productos, este no suele ser el caso de los productores que no están ubicados en la UE, ya que los intermediarios como, por ejemplo, las plataformas de comercio electrónico niegan su responsabilidad por velar por el cumplimiento de las normas.

[1] http://www.leparisien.fr/economie/consommation/achats-en-ligne-attention-aux-derives-du-dropshipping-16-01-2020-8237226.php

[2] https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html

Sin embargo, la nueva Ley de Servicios Digitales[3] (DSA, por sus siglas en inglés), aprobada recientemente y publicada en el Diario Oficial de la Unión Europea (DOUE) **el 27/10/2022[4]**, busca abordar alguno de estos problemas. Lo mismo se pretende con la propuesta de modificación del Reglamento General de Seguridad de los Productos[5].

2.2. ¿Por qué son importantes las plataformas para las personas consumidoras?

Ir de compras, conectarse con la familia y con amigos, compartir experiencias, ver una película, escuchar música, leer un libro, reservar un viaje, cocinar una nueva receta, planear una salida nocturna, moverse por la ciudad, pedir ayuda a los vecinos y buscar información en la web; son solo algunos ejemplos de actividades que millones de personas realizan todos los días. Para todas y cada una de tales actividades, existe una o múltiples plataformas online que facilitan estos servicios. No hay duda de que las personas consumidoras han abrazado el auge de la economía de las plataformas. Sin embargo, lo cierto es que esto trae tanto beneficios como desafíos para la protección del consumidor.

2.3. Los principales retos relativos a las plataformas

En primer lugar, cabe resaltar que cuando se adoptó la Directiva de comercio electrónico (en 2000), las plataformas como Google, Amazon o Booking.com estaban recién en sus inicios. Por su parte, muchos otros intermediarios ni siquiera existían, por ejemplo, Facebook y Shopify se lanzaron en 2004; Etsy se fundó en 2005; Airbnb en 2008; Instagram, Wish y AliExpress en 2010.

De esta manera, se observa que, en los últimos 20 años, los modelos comerciales de tales empresas -y de otras- y las dinámicas del poder de mercado han cambiado.

En efecto, el mercado digital europeo ha experimentado lo que puede denominarse como "datificación" (la transferencia de información a datos, siendo esta la base de los modelos de negocios digitales), así como también una multiplicación de plataformas, una proliferación de la economía colaborativa[6] y una diversificación de los proveedores de servicios en términos de funciones, integración vertical y tamaño.

---

[3] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_es#cules-son-los-prximos-pasos

[4] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.L_.2022.277.01.0001.01.SPA&toc=OJ%3AL%3A2022%3A277%3ATOC

[5] https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52021PC0346

[6] http://www.beuc.eu/publications/beuc-x-2016-030_gbe_collaborative_economy_beuc_position.pdf

A pesar de ello, lo cierto es que cada empresa tiene que seguir las reglas, por cuanto la protección de las personas consumidoras no depende, ni debe depender, del tamaño de la empresa. Al fin y al cabo, las starts-up o las Pymes de hoy podrían convertirse en el Alibaba del mañana.

Ahora bien, muchas plataformas se han reinventado. En efecto, algunas ya no se limitan a su función inicial de información o de intermediarios de confianza (como podrían ser, por ejemplo, plataformas de comparación o clasificación como Yelp), sino que permiten que las transacciones se concluyan en la propia plataforma. Estos modelos de negocios hacen que la plataforma entre en la categoría de "mercado en línea"[7], en donde se enfocan actualmente las organizaciones de protección al consumidor.

La protección del consumidor no depende, ni debe depender, del tamaño de la empresa. Al fin y al cabo, las *starts-up* o las Pymes de hoy podrían convertirse en el "Alibaba" del mañana.

Este tipo de plataformas es definido en la Directiva Ómnibus[8] como "un servicio que emplea programas ("software"), incluidos un sitio web, parte de un sitio web o una aplicación, operado por el comerciante o por cuenta de este, que permite a los consumidores celebrar contratos a distancia con otros comerciantes o consumidores". Dicho esto, cabe aclarar que, a menudo, el papel de la plataforma no se limita a permitir la celebración de un contrato entre vendedores y compradores, sino que también incluye otras prestaciones, como servicios de pago o de cumplimiento, procesamiento de devoluciones y gestión de reclamaciones[9].

Por su parte, otras plataformas han adquirido múltiples roles. Así, existen las denominadas "plataformas híbridas", que pueden combinar diferentes funciones de intermediación o plataformas integradas verticalmente. Es importante destacar que estos últimos no solo actúan como intermediarios, sino que también compiten con los comerciantes, ya sea directamente o a través de empresas afiliadas. Por ejemplo, Amazon es tanto un vendedor, como un mercado en línea, una empresa de computación en la nube, una plataforma para compartir videos, un editor, una empresa de publicidad, un fabricante de dispositivos conectados y una empresa de inteligencia artificial.

Por ello, las organizaciones de consumidores vienen pidiendo que se ajuste el marco legislativo para hacer frente a esta nueva realidad del mercado. La nueva Ley de Servicios Digitales (DSA) fue una iniciativa muy importante en este sentido. La Comisión presentó la

[7] Vzbv study, https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv_gutachten_verbraucherrechtliche_plattformhaftung.pdf, p. 17.

[8] Artículo 2, apartado 1, letra n), de la Directiva sobre prácticas comerciales desleales, modificada por la Directiva 2019/2161, https://eur-lex.europa.eu/eli/dir/2019/2161/oj?locale=es

[9] Vzbv study, https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv_gutachten_verbraucherrechtliche_plattformhaftung.pdf, p. 18.

propuesta de DSA en diciembre de 2020 y ha sido finalmente publicada en el DOUE el pasado 27/10/2022[10].

Desafíos específicos

Desafío #1. Difusión de una amplia gama de contenidos ilegales

Debe resaltarse que los servicios digitales han facilitado, hasta cierto punto, las violaciones generalizadas a las leyes del consumidor. En efecto, existe un flujo de ingresos generado por la venta de publicidad o promoción de productos peligrosos, inseguros e ilegales en línea. A modo de ejemplo[11]:

	La organización de defensa del consumidor "Which?", que se encuentra en el Reino Unido, encontró a la venta luces para árboles de Navidad que podían incendiarse o electrocutar a las personas consumidoras[12].
	El Consejo Danés de Consumidores reveló que los cosméticos que se venden en wish.com no cumplen con la legislación de la UE
	Seis organizaciones miembros de BEUC descubrieron recientemente que dos tercios de 250 productos comprados en mercados en línea no pasaron las pruebas de seguridad, con consecuencias como descargas eléctricas, incendios o asfixia[13].

[10] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.L_.2022.277.01.0001.01.SPA&toc=OJ%3AL%3A2022%3A277%3ATOC

[11] Ver ejemplos en: https://www.beuc.eu/publications/beuc-x-2019-072_new_evidence_from_beuc_member_organisations_regarding_dangerous_products_available_online.pdf

[12] https://www.which.co.uk/news/2019/12/these-christmas-tree-lights-bought-online-at-ebay-wish-and-aliexpress-could-catch-fire-or-electrocute-you/

[13] https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html

Desafío #2. Existe confusión entre las actividades que realizan los mercados en línea y otro tipo de actividades de las plataformas *online*

Cabe resaltar que el debate para reformar la Directiva de comercio electrónico se centra, en cierta medida, en cuestiones relacionadas con el discurso de odio, contenido terrorista, material protegido por derechos de autor, la libertad de expresión o las consideraciones del mercado único. Si bien son temas importantes, lo cierto es que la UE no debería perder de vista los problemas específicos relacionados con la protección de los consumidores. En efecto, resulta necesario garantizar su protección frente a la compra de productos o servicios a través de mercados en línea[14].

Así, debe distinguirse entre la venta de productos ilegales y otro tipo de actividades como, por ejemplo, publicar comentarios en las redes sociales. Mientras el último supuesto está relacionado con la libertad de expresión, el primero tiene más que ver con una cuestión de seguridad del producto y de protección del consumidor.

Desafío #3. La Directiva de comercio electrónico "no será aplicable a los servicios procedentes de prestadores establecidos en un tercer país"[15].

Debe resaltarse que algunos proveedores establecidos en terceros países se aprovechan de los límites en la aplicación territorial de la Directiva, creando un campo de juego injusto y desigual.

Desafío #4. El modo en que la Directiva de comercio electrónico regula a los proveedores de alojamiento es utilizado por algunas plataformas, incluidos los mercados en línea (aunque no son los únicos), para protegerse de cualquier tipo de responsabilidad o para no tomar medidas significativas por temor a ser considerados responsables.

Desafío #5. Existen en la legislación actual algunas lagunas regulatorias en relación con mercados en línea. Se presta poca atención a su enriquecimiento a partir de contenido ilegal. Parte de este problema viene a abordarse con la Ley de Servicios Digitales (DSA).

Desafío #6.

Las nuevas normas pueden ser un obstáculo para que los Estados miembros aborden correctamente sus objetivos de interés público.

[14] Definido Ómnibus como "*un servicio que emplea programas ("software"), incluidos un sitio web, parte de un sitio web o una aplicación, operado por el comerciante o por cuenta de este, que permite a los consumidores celebrar contratos a distancia con otros comerciantes o consumidores*". Sin embargo, lo cierto es que, a menudo, el papel de las plataformas no se limita a permitir la celebración de un contrato entre vendedores y compradores, sino que también incluye servicios de pago, de cumplimiento, procesamiento de devoluciones y gestión de reclamaciones, entre otros.

[15] Directiva de Comercio Electrónico, considerando 58.

Por ejemplo, en el asunto C-390/18[16], el TJUE dictaminó que Airbnb debe ser considerado un servicio de la sociedad de la información (art. 2.a) de conformidad con la Directiva de comercio electrónico. Así, se sostuvo que, dado que Francia no había notificado a la Comisión la existencia de una ley que exigía a empresas como Airbnb la obtención de una licencia profesional de agente inmobiliario no podía imponer tal obligación a dicha empresa, ya que infringiría el artículo 3.4 b) de la Directiva de comercio electrónico.

A partir de ese caso se demostró que la Directiva de comercio electrónico genera problemas para que los Estados miembros adopten leyes y políticas para proteger a los consumidores, en tanto pone el mercado interior en primer lugar. Ahora bien, es importante aclarar que esta decisión judicial no implica que los gobiernos no puedan imponer este tipo de medidas a empresas como Airbnb. El TJUE fue claro respeto de que la obligación de notificación de la Directiva de comercio electrónico *"no tiene por objeto (...) evitar que un Estado miembro adopte medidas pertenecientes al ámbito de las competencias de este último que puedan afectar a esa libre prestación de servicios, sino prevenir que un Estado miembro interfiera en la competencia que por principio corresponde al Estado miembro de establecimiento del prestador del servicio de la sociedad de la información de que se trate».*

Desafío #7. Falta de supervisión y cumplimiento adecuados

Cabe destacar que los mercados digitales evolucionan a gran velocidad y que las autoridades competentes no parecen estar a la altura, en tanto carecen de la experiencia o los recursos necesarios para monitorear y abordar los problemas que plantean.

2.4. Resumen de los principales derechos y obligaciones de las personas consumidoras

La **Directiva de comercio electrónico** ha sido una de las piedras angulares de Internet durante mucho tiempo. La misma estableció el principio del "país de origen", pero con algunas excepciones importantes (en particular, en relación con los contratos de consumo). Asimismo, dispuso la obligación de brindar información clave a los destinatarios de los servicios (por ejemplo, los consumidores), así como también exenciones de responsabilidad y limitaciones para los proveedores de servicios de intermediación en línea. Se pueden resaltar, además, las siguientes disposiciones:

- **Artículos 1 – 3: Disposiciones generales**
- **Artículo 4 – 15: Principios**
    - Sección 1: Régimen de establecimiento y de información
    - Sección 2: Comunicaciones comerciales
    - Sección 3: Contratos por vía electrónica
    - Sección 4: Responsabilidad de los prestadores de servicios intermediarios

[16] http://curia.europa.eu/juris/documents.jsf?num=C-390/18

- **Artículos 16 – 20: Implementación**
- **Artículos 21 – 24: Disposiciones finales**

¿Dónde se encuentran las disposiciones más importantes de la Directiva de comercio electrónico?

- **Objetivo principal:** mercado interior y libre circulación de los servicios de la sociedad de la información entre los Estados miembros (artículo 1).
- **Establece otros objetivos, entre los que se pueden mencionar** "la seguridad jurídica y la confianza de los consumidores" (Considerando 7), garantizar un alto nivel de protección de los objetivos de interés general y, en especial, la protección de los menores y la dignidad humana, la protección del consumidor y de la salud pública (Considerando 10)
- **Ámbito de aplicación:** sin perjuicio de la protección del consumidor (artículo 1)
- **Definiciones** (Artículo 2)
- **Información básica** a los consumidores y otros destinatarios (artículos 5, 6, 10)
- **Derechos a efectuar pedidos por vía electrónica** (Artículo 11)
- **Principios de responsabilidad del intermediario** (artículos 12-15)**. Los más importantes son:**
    - Los proveedores de alojamiento no son responsables del contenido de terceros siempre que, al saberlo, eliminen o deshabiliten rápidamente el acceso a contenido ilegal (artículo 14)
    - Prohibición de que los Estados miembros impongan a los prestadores una obligación general de supervisar los datos que transmitan o almacenen o de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas (artículo 15)
- **Códigos de conducta** (artículo 16)
- **Solución extrajudicial de litigios** (artículo 17)
- **Acciones judiciales para** *"poner término a cualquier presunta infracción y evitar que se produzcan nuevos perjuicios contra los intereses afectados*" (artículo 18)
- **Cooperación de los Estados miembros** (artículo 19)
- **Sanciones** (Artículo 20)

Ahora bien, cabe recordar que, desde que se adoptó la Directiva de comercio electrónico en el 2000, los servicios digitales han evolucionado y planteado nuevos desafíos. Por ejemplo, el principio de “puerto seguro” otorga un espacio libre para que algunas plataformas no sean consideradas responsables. Asimismo, ciertos proveedores de servicios digitales no asumen una responsabilidad significativa, ni brindan una compensación adecuada a las personas consumidoras en caso de daño. Del mismo modo, se ha retrasado la adopción de medidas

reglamentarias. Sin embargo, algunos de estos problemas son abordados en la nueva Ley de Servicios Digitales (DSA).

Para más información se pueden ver otros dos documentos desarrollados por Consumer PRO sobre los derechos generales del consumidor y las acciones colectivas.

2.5. La nueva Ley de Servicios Digitales

La nueva Ley de Servicios Digitales (DSA), publicada en el DOUE el pasado 27/10/2022[17], regula las obligaciones de los servicios que actúan como intermediarios en lo relativo a la función de conectar a las personas consumidoras con bienes, servicios y contenidos.

Busca proteger mejor a los consumidores y sus derechos fundamentales en línea, establecer un marco eficiente de transparencia y de rendición de cuentas para las plataformas en línea y, por lo tanto, fomentar mercados digitales más justos y abiertos.

A diferencia de la Directiva de comercio electrónico, la DSA es un Reglamento, por lo que armonizará las normas en toda la UE y será directamente aplicable. Las nuevas normas deberían garantizar el mismo nivel de protección a todos los ciudadanos de la UE.

¿A quién se aplica?

- Servicios de intermediación en línea, que ofrecen infraestructuras de red; proveedores de acceso a internet, registradores de nombres de dominio, que a su vez incluyen:
- Servicios de alojamiento de datos (como podrían ser Google Cloud, Amazon Web Services), tales como servicios en nube y de alojamiento web, que a su vez incluyen:
- Plataformas online (como podrían ser Twitter, Amazon, Instagram), que reúnen a vendedores y personas consumidoras, tales como mercados online, tiendas de aplicaciones, plataformas de economía colaborativa y plataformas de redes sociales.
- Motores de búsqueda (como podría ser Google)
- Plataformas en línea de muy gran tamaño y motores de búsqueda de muy gran tamaño (VLOPs/VLOSEs, por sus siglas en inglés, ≥ 45 millones de usuarios de la UE o 10% de la población de la UE)

[17] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.L_.2022.277.01.0001.01.SPA&toc=OJ%3AL%3A2022%3A277%3ATOC

¿Cuáles son las nuevas reglas?

- Los intermediarios en línea deberán tener un papel más activo para abordar el contenido ilegal (productos y servicios incluidos). Así, deberán tomar medidas para contrarrestar el contenido ilegal en línea (incluidos los productos y la desinformación) como, por ejemplo, establecer un mecanismo:
    - para que los usuarios puedan “marcar” dicho contenido;
    - para que las plataformas cooperen con los denominados "alertadores fiables" (entidades que hayan demostrado experiencia y competencia especiales, que contarán con un canal privilegiado o preferente de denuncia para luchar contra la oferta de bienes, servicios o contenidos ilícitos en línea);
    - para retirar mercancías ilegales o inseguras.
- Se establecen obligaciones adicionales de transparencia y diligencia debida para que las plataformas online, por ejemplo:
    - Nuevas garantías para los usuarios, incluida la posibilidad de impugnar las decisiones de moderación de contenido de las plataformas;
    - Medidas de transparencia adicionales, incluidos los algoritmos utilizados para las recomendaciones y la publicidad dirigida.
- Obligación de "Conozca a su cliente comercial" (KYBC, por sus siglas en inglés) para mejorar la trazabilidad de los usuarios comerciales en los mercados en línea, destinada a identificar mejor a los vendedores de productos ilegales.
- Prohibición de patrones oscuros: Se exige a los proveedores de plataformas online que no diseñen, organicen ni exploten sus interfaces en línea de manera que induzcan a error, manipulen o distorsionen de cualquier modo la capacidad de los usuarios de sus servicios de tomar decisiones libres e informadas.
- Restricciones a la publicidad en línea:
    - Se prohíbe la publicidad dirigida a menores basada en la elaboración de perfiles; y se prohíbe la publicidad personalizada basada en la elaboración de perfiles utilizando categorías especiales de datos personales, como la orientación sexual o las creencias religiosas.
    - Los usuarios deben poder comprender y tomar decisiones fundadas sobre los anuncios que ven. Deben estar informados de forma clara de si son destinatarios de anuncios y de la razón de ello, y de quién ha pagado el anuncio.
- Obligaciones adicionales para plataformas en línea y motores de búsqueda de muy gran tamaño (VLOPs/VLOSEs), por ejemplo, para evitar el abuso de sus sistemas, en particular:
    - abordando los riesgos sistémicos (como la desinformación);
    - evaluar y mitigar los riesgos sociales derivados del diseño y el uso de sus servicios;

    - la supervisión de las medidas adoptadas a través de auditorías independientes;
- Marco de aplicación de dos niveles:
    - a nivel nacional: Una nueva estructura de supervisión (a través de los Coordinadores de Servicios Digitales) para abordar la complejidad del espacio en línea en el que los Estados miembros tendrán el papel principal, con el apoyo de una nueva Junta Europea de Servicios Digitales;
    - a nivel de la UE: En el caso de plataformas en línea de muy gran tamaño, la Comisión tendría una función reforzada de supervisión y ejecución.
- Se refuerzan los medios de reparación para las personas consumidoras.

Exención de responsabilidad limitada para "mercados"

La DSA mantiene los principios de exención de responsabilidad de los intermediarios de la Directiva de comercio electrónico, aunque con algunas aclaraciones y pequeñas mejoras:

Cuando se preste un servicio de la sociedad de la información consistente en almacenar información facilitada por un destinatario del servicio, el prestador de servicios no podrá ser considerado responsable de los datos almacenados a petición del destinatario, a condición de que el prestador de servicios:

- no tenga conocimiento efectivo de una actividad ilícita o de un contenido ilícito y, en lo que se refiere a una acción por daños y perjuicios, no tenga conocimiento de hechos o circunstancias por los que la actividad o el contenido revele su carácter ilícito, o de que;
- en cuanto tenga conocimiento de estos puntos, actúe con prontitud para retirar el contenido ilícito o inhabilitar el acceso al mismo.

Excepción a la exención:

- La exención de responsabilidad no debe aplicarse cuando el destinatario del servicio actúe bajo la autoridad o el control del prestador de un servicio de alojamiento de datos. Por ejemplo, cuando el prestador de una plataforma en línea que permite a las personas consumidoras celebrar contratos a distancia con comerciantes determine el precio de los bienes o servicios ofertados por el comerciante.
- Las plataformas en línea que permiten a los consumidores celebrar contratos a distancia con comerciantes, no deben poder acogerse a la exención de responsabilidad aplicable a los prestadores de servicios de alojamiento de datos en la medida en que dichas plataformas presenten la información pertinente relativa a las transacciones en cuestión de manera que induzca a los consumidores a creer que la información ha sido facilitada por las propias plataformas en línea. Podría ser el caso, por ejemplo, de una plataforma que no muestre claramente la identidad del comerciante; de una plataforma en línea que no revele dicha identidad o los datos de

contacto hasta después de la formalización del contrato celebrado entre un comerciante y un consumidor, o de esas plataformas en línea cuando comercialicen el producto o servicio en su propio nombre en lugar de utilizar el nombre del comerciante que lo suministrará. Se deberán evaluar todas las circunstancias pertinentes.

- Los tribunales o la autoridad administrativa correspondiente, de conformidad con los sistemas jurídicos de los Estados miembros, podrá exigir al prestador de servicios que ponga fin a una infracción o que la impida.

¿Cómo se podrá perseguir el resarcimiento?

- Las plataformas en línea deberán establecer sistemas internos de tramitación de reclamaciones, que sean fácilmente accesibles y produzcan resultados rápidos y justos. Los destinatarios del servicio deben poder impugnar de manera fácil y efectiva ciertas decisiones de las plataformas en línea que les afecten negativamente como, por ejemplo, cuando se elimine (o no) contenido o cuando se suspenda su cuenta.
- Además, debe contemplarse la vía de resolución extrajudicial de litigios: mecanismos certificados para la solución de controversias entre proveedores y consumidores. Advertencia: decisiones no vinculantes.
- A su vez, existe la posibilidad de recurso judicial, de conformidad con la legislación del Estado miembro.
- Se prevé el derecho a presentar una denuncia ante su Coordinador de Servicios Digitales.
- Derecho a indemnización: sin perjuicio de la legislación de consumo de la UE, los consumidores podrán solicitar una indemnización a los proveedores por cualquier daño o pérdida sufrida debido al incumplimiento de las obligaciones de DSA. Debe seguirse la legislación nacional aplicable sobre cómo reclamar una indemnización.
- Representación: Sin perjuicio de la Directiva relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores o de cualquier otra representación conforme a la legislación nacional, las personas consumidoras tendrán derecho a otorgar mandato a una ONG (incluidas las organizaciones de consumidores). Sus reclamaciones deberán tener prioridad y deben decidirse sin demoras indebidas.
- Se añade la DSA al anexo de la Directiva de Acciones de Representación.

Aplicación del Reglamento

- Cumplimiento a nivel nacional: Se mantiene el principio del país de origen, es decir que será el regulador del Estado Miembro del país en el que el prestador está establecido el que deba asegurarse que sus servicios son conformes con su legislación.

nacional. Los Estados Miembros serán responsables de las plataformas más pequeñas, quienes deberán designar a los coordinadores de servicios digitales, que supervisarán la conformidad de los servicios establecidos en su territorio con las nuevas normas y participarán en los mecanismos de cooperación de la UE.

- Cumplimiento a nivel de la UE: La Comisión Europea será la responsable principal de las plataformas y motores de búsqueda de muy gran tamaño (≥ 45 millones de usuarios de la UE). Asimismo, tendrá poderes exclusivos para designar y hacer cumplir las obligaciones especiales de VLOP/VLOSE. Se prevé que las solicitudes de acción pueden ser realizadas por los Coordinadores de Servicios Digitales.

Leyes y reglamentos a nivel de la UE

REGLAMENTO / DIRECTIVA	FECHA DE APLICACIÓN	REVISIÓN / EVALUACIÓN: TIPO DE MEDIDA	FECHA DE VENCIMIENTO	COMENTARIO
Directiva de Comercio Electrónico	17/01/2002 (transposición)	Informe de reexamen CE (Art. 21)	Antes del 17/07/2003, y luego, cada dos años.	No se conoce ninguna evaluación formal desde 2012. La investigación sectorial de la Comisión de 2017 puede ser interesante desde la perspectiva de la competencia.
Ley de Servicios Digitales	Aplicable a toda la UE el 17/02/2024. Los VLOP/VLOSE tendrán cuatro meses para cumplir una vez designados.	Art. 91 informes de revisión de la CE	Publicada en el DOUE el pasado 27/10/2022	Los VLOP/VLOSE tendrán cuatro meses para cumplir una vez designados por la Comisión, a menos que dicha fecha sea anterior a la aplicación general de la DSA. La DSA fue presentada en diciembre del 2020 junto con la nueva Ley de Mercados Digitales (DMA)[18], que establece reglas específicas dirigidas a las plataformas que actúan como guardianes de acceso de productos y servicios digitales.
Regulación de Plataformas para Negocios	12/07/2020	CE elaborar orientaciones de las obligaciones de transparencia (Art. 5)	Publicada el 8/12/2020	

[18] Publicada en el DOUE el 12/10/2022: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.SPA&toc=OJ%3AL%3A2022%3A265%3ATOC

(Regulación P2B)		La CE fomentará la elaboración de códigos de conducta (Art. 17)	Sin fecha	Un análisis de su funcionamiento será parte de la revisión.
		CE informe de revisión (Art. 18)	13/01/2022 y cada 3 años	
Directiva Ómnibus	28 de noviembre de 2021 (transposición) 28 de mayo de 2022 (aplicación)	Art. 7 – Transposición	Art. 6 – Presentación de informes por parte de la CE y revisión El primer informe de la CE debe ser publicado a más tardar el 28 de mayo de 2024.	

2.6. Jurisprudencia

- **Re: Directiva Ómnibus**: aún no hay jurisprudencia, ya que solo comenzó a aplicarse a partir del 28 de mayo de 2022. Puede consultar el documento de antecedentes teóricos de la Ley General del Consumidor para conocer la jurisprudencia de otros instrumentos del derecho del consumidor.
- **Re: Directiva de Comercio Electrónico**: vea el listado de jurisprudencia aquí

2.7. ¿Qué pueden hacer las personas consumidoras si tienen un problema?

- Ir directamente al vendedor/plataforma (este paso no es obligatorio).
- Resolución alternativa de disputas (RAD) posible (este paso no es obligatorio).
- Autoridades competentes de los Estados miembros: varía según el país y el tema de un país a otro y de un tema a otro.

A Nivel Nacional[19]:

[19]Normativa aplicable:

- Ley 11/2022 de 28 de junio, General de las telecomunicaciones.
- Ley 34/2002 de 11 de Julio de servicios de la sociedad de la información y de comercio electrónico.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información
- Real Decreto Legislativo 1/2007 de 16 de noviembre que aprueba el Texto Refundido de la Ley General para la Defensa de Consumidores y Usuarios y otras leyes.
- Ley 7/1996 de 15 de enero de Ordenación del Comercio Minorista.
- Condiciones Generales de la Contratación. (véase Disposición Final 5º de la Ley 34/2002 de 11 de Julio)
- Ley 22/2007 de 11 de Julio sobre comercialización a distancia de servicios financieros destinados a los consumidores.

En primer lugar, se puede reclamar ante la propia compañía. Esto podrá hacerse a través de distintas vías:

- Interponiendo una reclamación directamente a la entidad a través de los medios de los que esta disponga (dirección del establecimiento, número de teléfono, número de fax y/o dirección de correo electrónico del mismo),
- A través de la Oficina Municipal de Información al Consumidor (OMIC) de su municipio, que se encargará de gestionar la reclamación, actuando como intermediario, o
- A través de la plataforma europea de resolución de litigios en línea (RLL) de la Comisión Europea para intentar llegar a una solución. En caso contrario, las partes pueden acordar que la disputa se resuelva a través de un organismo homologado para la resolución de conflictos.
- A través de su asociación de consumidores.

La propia entidad deberá informar al consumidor sobre los mecanismos de reclamación y, en su caso, si está adherido a algún sistema alternativo de resolución de conflictos.

Luego, si la entidad no atiende su reclamación de forma satisfactoria en el plazo de un mes, podrá:

- Acudir a un sistema alternativo de resolución de conflictos, si la entidad está adherida a alguno. Esta información deberá facilitarse de forma previa al contrato, así como la forma de acceder al mismo.
- Poner los hechos en conocimiento de la autoridad administrativa competente (Dirección General de Industria, Secretaría de Estado de Telecomunicaciones, Agencia Estatal de Seguridad Aérea, Agencia Española de Protección de Datos, Dirección General de Seguros y Fondo de Pensiones, Banco de España, etc.). Podrá acudir al Sistema Arbitral de Consumo, para obtener un laudo (resolución) de obligado cumplimiento, siempre que la empresa acepte la resolver el conflicto a través de este mecanismo.
- Si la entidad tuviese su domicilio en un Estado de la Unión distinto al del consumidor, tras la primera reclamación el consumidor podrá acudir al Centro Europeo del Consumidor, donde le ayudarán a gestionar su reclamación, con la colaboración con el Centro Europeo del Consumidor del Estado donde se encuentre la entidad; facilitando toda la información en el idioma del consumidor y asesorando sobre los mecanismos existentes para reclamar.

Procedimiento Judicial. Si ninguna de las vías anteriores prospera, el consumidor podrá acudir a los tribunales de justicia. Si la reclamación no supera los 2.000 euros no será necesario

- Ley 6/2020 de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Ley de Ordenación del Comercio Minorista.
- Real Decreto 231/2008, de 15 de febrero, por el que se regula el Sistema Arbitral de Consumo

contar con abogado ni procurador, ni se tendrán que abonar tasas judiciales. Únicamente debe presentarse el modelo de demanda de juicio verbal de menor cuantía, junto con la documentación pertinente, en el juzgado competente. Este modelo puede descargarse en esta página web, en el apartado Formularios; y en la del Consejo General del Poder Judicial, o solicitarse en el propio juzgado.

En caso de reclamación transfronteriza (las partes tienen su domicilio en distintos Estados de la Unión), si esta no supera los 5.000 euros, podrá interponerse la pertinente demanda sin necesidad de abogado ni procurador.

Autoridades y Entidades nacionales de Ciberseguridad

- Policía Nacional - Brigada de Investigación Tecnológica (BIT)
- Guardia Civil - Grupo de Delitos Telemáticos (GDT)
- Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)
- Instituto Nacional de Ciberseguridad (INCIBE) y el CERT de Seguridad e Industria (CERTSI)
- Centro Criptológico Nacional (CCN-CERT)

Autoridades nacionales de protección de datos:

- Agencia Española de Protección de Datos (AEPD)

2.8. Otros recursos: hojas informativas, publicaciones, enlaces

- Presentación de la Comisión Europea sobre los instrumentos y objetivos perseguidos por la Directiva de Comercio Electrónico (ver aquí)
- Documento de posicionamiento de BEUC: "Garantizar la protección del consumidor en la economía de plataformas" (ver aquí)
- Documento de posicionamiento de BEUC: "Economía colaborativa" (ver aquí)
- Documento de posicionamiento de BEUC: "Hacer que la Ley de Servicios Digitales funcione para los consumidores" (ver aquí)
- Documento de posicionamiento de BEUC: "La propuesta de Ley de Servicios Digitales (ver aquí)
- Hoja informativa de BEUC: Propuesta de Ley de Servicios Digitales: una mejor protección para los consumidores (ver aquí)
- Informe del Parlamento Europeo sobre la propuesta de Ley de Servicios Digitales (ver aquí)
- Comisión Europea – Documento de preguntas y respuestas sobre la Ley de Servicios Digitales (ver aquí)

3. INTERNET DE LAS COSAS (IOT, POR SUS SIGLAS EN INGLÉS)

3.1. Introducción e historia

En los últimos años los dispositivos conectados se han vuelto omnipresentes en la vida de muchas personas consumidoras. Si bien antiguamente necesitábamos estar frente a una computadora para poder acceder a Internet, en la actualidad contamos con teléfonos inteligentes que ya se encuentran conectados a la red. Al mismo tiempo, una gran cantidad de los dispositivos que nos rodean cotidianamente están equipados con sensores y se encuentran conectados a Internet. Se pueden mencionar como ejemplo desde cafeteras y cámaras de seguridad hasta automóviles y dispositivos médicos. El auge de los dispositivos conectados se conoce comúnmente como "internet de las cosas" o “IoT”, por sus siglas en inglés.

3.2. ¿Por qué el IOT es importante para las personas consumidoras?

Como se mencionó previamente, los dispositivos conectados están cada vez más presentes en la vida de muchos consumidores y están cambiando la forma en que conducimos nuestras vidas. Si bien la digitalización de los dispositivos ofrece muchos beneficios, también conlleva importantes riesgos y desafíos. Por ejemplo, ¿qué sucede cuando el proveedor de servicios de su sistema doméstico inteligente decide cerrar sus servidores? ¿Quién es responsable si su televisor inteligente se ve comprometido o inutilizado debido a la falta de actualizaciones de software? ¿Y cuál es el impacto sobre nuestra privacidad?

Por lo tanto, es importante que la UE desarrolle políticas claras, con visión de futuro y un marco legal que garantice que los derechos de los consumidores se mantengan en este entorno conectado.

3.3. Los principales desafíos que presenta el IOT

Como se dijo, la conexión a Internet de una gran cantidad de dispositivos plantea tanto oportunidades como riesgos para las personas consumidoras. El mundo interconectado promete mayores comodidades, experiencias diversas y mejoras significativas en la calidad de vida. Asimismo, la información agregada a estos dispositivos también podría generar nuevos conocimientos en áreas como la medicina, la inteligencia artificial y la planificación urbana.

Por ejemplo, una casa inteligente, que se encuentre repleta de dispositivos y sensores conectados, puede aprender los hábitos y las preferencias de su propietario, y adaptar su funcionalidad en consecuencia. Al mismo tiempo, debe resaltarse que los dispositivos pueden comunicarse entre sí de modo que, por ejemplo, si un reloj inteligente detecta un ritmo cardíaco bajo, remita un mensaje urgente al hospital más cercano. Además, la capacidad de monitorear de forma remota, a través de Internet, a determinados dispositivos puede ayudar a las personas que necesitan asistencia a conservar su independencia, por ejemplo, al desbloquear las puertas de forma remota. Por su parte, en otros sectores, como la industria y la salud, el IoT tendrá efectos potencialmente transformadores, tanto en términos de eficiencia, como de acumulación de información.

Sin embargo, debe resaltarse que los dispositivos conectados también presentan múltiples desafíos desde la perspectiva del consumidor. En efecto, el IoT abarca una gran gama de áreas y temas políticos: privacidad y protección de datos, ciberseguridad, obsolescencia de productos, sostenibilidad y consumo de energía, competencia, seguridad, derechos del consumidor, etc.

Por ejemplo, los dispositivos conectados normalmente recopilan una gran cantidad de datos sobre sus usuarios y su entorno. Tal recopilación plantea una serie de preocupaciones en relación con la protección de datos y la privacidad. A medida que cada vez más aspectos de nuestras vidas se integren en una red más amplia de sensores y dispositivos, los riesgos potenciales, el alcance de las filtraciones de datos y los ataques cibernéticos también crecen. En efecto, cada nuevo dispositivo que conectamos a Internet representa otro potencial ataque y, a menudo, la cadena de dispositivos es tan fuerte como su eslabón más débil. Asimismo, el surgimiento e implementación de la inteligencia artificial en las tecnologías IoT también plantea desafíos relacionados con la equidad y la responsabilidad, entre otros. Además, otros desafíos que se presentan o exacerban a través de IoT incluyen: la limitación artificial de los ciclos de vida del producto, los efectos de bloqueo y la responsabilidad del producto.

Por su parte, se resalta que los dispositivos en red tienen un mayor consumo de energía. Una gran parte de este consumo surge de su capacidad de respuesta continua (modo inactivo). Friedli et al. (2016) proyectó que las pérdidas globales en posición de espera aumentarán de 7,5 TWh en 2015 a 47 TWh en 2025, según el consumo de los dispositivos que estén permanentemente conectados a la red eléctrica.[20]

3.4. Resumen de los principales derechos y obligaciones de las personas consumidoras

Cabe resaltar que, en lo relativo a los dispositivos conectados, se aplican los mismos derechos del consumidor que para el resto de los productos no conectados. Por ejemplo, las normas sobre garantías (Directiva de contenidos digitales, Directiva de contratos de compraventa de bienes), sobre información al consumidor (Directiva de derechos del consumidor). En su caso, y para obtener más información sobre la Directiva de contratos de compraventa de bienes y

[20] https://nachhaltigwirtschaften.at/resources/iea_pdf/reports/iea_4e_edna_energy_efficiency_of_the_internet_of_things_technical_report.pdf

la Directiva de Derechos del Consumidor, puede consultar el documento de antecedentes teóricos complementario sobre la Ley General del Consumidor. Asimismo, las reglas de la legislación sobre seguridad de los productos (recientemente se llegó a un acuerdo a Nivel UE sobre el nuevo Reglamento General de Seguridad de los Productos, que pretende modernizar esta legislación[21]) también se aplican, hasta cierto punto[22], a los dispositivos IoT.

A pesar de ello, debe resaltarse que, debido a la propia conectividad de estos dispositivos, se aplican obligaciones específicas:

1) En primer lugar, los dispositivos que recopilan datos personales sobre los consumidores deben asegurarse de que procesan tales datos de acuerdo con el RGPD. Estas reglas incluyen (pero no se limitan) los siguientes principios: de minimización de datos, limitación de propósito y protección de datos por diseño, y la obligación de obtener el consentimiento del usuario, según los fines del procesamiento de datos[23].
2) En segundo lugar, cabe considerar que, de conformidad con la Directiva de equipos de radio, a partir de 2024, los fabricantes de dispositivos conectados deberán asegurarse de que presenten un cierto nivel de seguridad. Estas medidas garantizarán que tales dispositivos (i) no dañen la red, provocando una degradación inaceptable del servicio; (ii) incorporen medidas de seguridad para garantizar que los datos personales, la privacidad del usuario y del suscriptor estén protegidos, y (iii) admitan ciertas funciones que garanticen la protección contra fraudes como el ransomware.
3) De acuerdo con la Directiva de contenidos digitales, los dispositivos conectados deben recibir actualizaciones, incluidas las de seguridad, durante el período de tiempo que las personas consumidoras puedan razonablemente esperar. La extensión de esta obligación está ligada al período de garantía legal, pero también puede ir más allá.

Período de garantía a nivel nacional[24]:

[21] https://www.consilium.europa.eu/es/press/press-releases/2022/11/29/council-and-european-parliament-agree-on-new-product-safety-rules/

[22] Estas reglas establecen que todos los dispositivos deben ser seguros. Sin embargo, no existe acuerdo respecto de si el concepto de "seguridad" también debe incluir "protección". La posición que se acordó es que dicha legislación se aplica a los dispositivos conectados si la vulnerabilidad detectada genera un problema de seguridad (por ejemplo, si un hacker informático se aprovecha de la vulnerabilidad de una alarma contra incendios para apagarla. Si luego hay un incendio, los ocupantes del hogar estarían en peligro físico).

[23] Para más información sobre la protección de datos y el RGPD, ver capítulo 1.

[24] Normativa aplicable:

- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
- Ley 34/1988, de 11 de noviembre, General de Publicidad.
- Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista.
- Real Decreto 231/2008, de 15 de febrero, por el que se regula el Sistema Arbitral de Consumo.
- Ley 3/1991, de 10 de enero, de Competencia Desleal
- Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales,

Para los bienes adquiridos **antes del 1 de enero de 2022**, el plazo de garantía, de dos años desde que el producto fue entregado, es aquel durante el cual el vendedor está obligado a atender las deficiencias que pueda presentar el producto comprado. Fuera de dicho plazo no ha lugar a atender dichas reclamaciones. A falta de prueba en contrario, se presumirá que la fecha de entrega será la que conste en la factura o tique de compra. En el caso de artículos de segunda mano, el plazo también será de dos años, pero el contrato que en su caso se formalice podrá limitar dicha garantía a sólo un año.

El plazo para comunicar los desperfectos es de dos meses desde que se tuviera conocimiento de ello. De incumplirse este plazo, el garante no podrá rehusar su responsabilidad, pero tampoco estará obligado a atender los daños y perjuicios que la demora en dicho plazo pudiera haber causado.

A partir del día **1 de enero de 2022,** la garantía legal se seguirá aplicando a la falta de conformidad de los bienes y se amplía a los contenidos o servicios digitales. En el primer caso, el plazo de garantía será de tres años desde la entrega del producto; en el caso de contenidos o servicios digitales el plazo será de dos años, sin perjuicio de la obligación del empresario de suministrar y comunicar al consumidor las actualizaciones, incluidas las relativas a la seguridad, que sean necesarias para mantener la conformidad. En relación con los bienes de segunda mano, las partes podrán pactar un plazo inferior al general, pero no podrá ser inferior a un año.

En el caso de contratos de suministro continuo de contenidos o servicios digitales o de bienes con elementos digitales, el plazo de garantía será el plazo durante el cual deben suministrarse. Si este fuese inferior a tres años, el periodo de garantía será de tres años desde el momento de la entrega.

Con relación a la aplicación de nuestro derecho, lo importante es acreditar que la falta de conformidad se produjo dentro de los plazos indicados, con independencia de que lo comuniquemos transcurrido el plazo (sin demoras injustificadas ya que en ese caso el consumidor podría tener que acarrear con los daños producidos por su falta de diligencia) o si la reclamación se demora y se resuelve fuera de plazo. El plazo para demandar por falta de conformidad es de cinco años desde que esta se manifieste.

Ha de tenerse en cuenta que el periodo de garantía quedará en suspenso desde el momento en que el consumidor entregue el bien hasta su entrega ya conforme.

Por su parte, el plazo de garantía de la reparación o puesta en conformidad será de un año desde la entrega del bien o suministro puesto en conformidad. Se presumirá que se trata de la misma falta de conformidad cuando se reproduzcan los mismos defectos que los inicialmente manifestados.

desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores.

4) En cuarto lugar, en virtud de la Ley de Ciberseguridad, cuando existan esquemas de certificación y se apliquen al dispositivo conectado en cuestión, el fabricante de este deberá informar al consumidor sobre el período durante el cual se ofrecerá soporte de seguridad a los usuarios finales, en particular en lo que respecta a la disponibilidad de actualización relacionada con la ciberseguridad
5) Las personas consumidoras deben tener una expectativa clara respecto a que el acceso a los servicios de Internet se brinde de manera neutral y no discriminatoria, de acuerdo con el Reglamento de Internet Abierta. Los proveedores de servicios de Internet deben tratar todo el tráfico por igual, sin discriminación, restricción o interferencia ("neutralidad de la red"). En efecto, mantener un acceso a Internet abierta y neutral resulta esencial, si queremos ejercer nuestras libertades fundamentales y derechos democráticos para participar en las sociedades en línea actuales. Asimismo, es una condición previa para beneficiarse del Internet de las Cosas. Las personas consumidoras necesitan una Internet neutral y sin restricciones, para usar sus dispositivos conectados con el fin de acceder a noticias, contenido cultural o para comprar sin restricciones.
6) En lo que respecta a las normas sobre responsabilidad por productos defectuosos, cabe señalar que la Directiva pertinente se redactó en 1985. Es decir, mucho antes de que se pudiera considerar el uso de dispositivos conectados y mucho menos prever los desafíos del futuro. Por ello, dicha directiva no es suficiente para hacer frente a los desafíos del internet de las cosas y para garantizar una compensación a las personas consumidoras si algo va mal. Recientemente se ha revisado esta directiva. En abril de 2020, BEUC hizo varias recomendaciones para garantizar que las normas de responsabilidad de los productos de la UE sigan siendo adecuadas para los consumidores en la era digital y para IoT[25]. En septiembre del 2022 la Comisión Europea presentó dos propuestas para adaptar las normas de responsabilidad a la era digital, la economía circular y el impacto de las cadenas de valor mundiales, que actualmente se encuentran en debate en el Consejo de la UE y el Parlamento Europeo[26].

3.5. Leyes y Reglamentos a nivel UE

- Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE Texto pertinente a efectos del EEE
- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 («Reglamento sobre la Ciberseguridad»)

[25] BEUC, *Product liability 2.0 - How to make EU rules fit for consumers in the digital age*, abril 2020, www.beuc.eu/publications/product-liability-20-how-make-eu-rules-fit-consumers-digital-age/html

[26] https://ec.europa.eu/commission/presscorner/detail/es/ip_22_5807

- Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos
- Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales
- Reglamento de Internet Abierto (Reglamento (UE) 2015/2120), del 25 de noviembre del 2015.
- Reglamento (UE) 2015/2120 de 25 de noviembre de 2015 por el que se establecen medidas en relación con el acceso a una internet abierta y se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (UE) no 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión.
- Informe final de la Comisión Europea sobre la internet de las cosas de consumo.

*Otras leyes relevantes que se trataron en otros módulos como el RGPD y los derechos del consumidor no se mencionan aquí, pero, como se explicó, también se aplican en el contexto del IoT. Por ejemplo, si un dispositivo conectado procesa datos personales, deberá cumplir con el RGPD.

3.6. Jurisprudencia

En lo que se refiere a la 'neutralidad de la red' (ver Punto 5 del Capítulo 3.4), el Tribunal de Justicia de la UE se pronunció recientemente en los asuntos C-854/19, C-5/20 y C-34/20, y sostuvo que las ofertas que aplican una 'tarifa cero'[27] para determinadas aplicaciones, y por ende, las limitaciones que se derivan de la activación de tales opciones (sobre el ancho de banda, la conexión o el uso en roaming), violan el artículo 3 (3) del Reglamento de Internet Abierto y, por lo tanto, son ilegales según la legislación de la UE. De esta manera, los proveedores de servicios deben revisar sus prácticas comerciales, de acuerdo con esta interpretación, para asegurarse que respetan las normas de la UE sobre neutralidad de la red. El Tribunal podría aplicar un razonamiento similar a los proveedores de servicios que ofrecen una 'tarifa cero' para las aplicaciones asociadas con los dispositivos conectados (por ejemplo, en el contexto de una campaña de marketing, un proveedor de servicios de Internet ofrece una tarifa ventajosa, es decir, una tarifa cero, a la aplicación utilizada para controlar una cámara inteligente).

3.7. ¿Qué pueden hacer las personas consumidoras si tienen un problema?

Como se ha visto, se aplican varias leyes a los dispositivos conectados, por lo que, dependiendo cuál sea aplicable, las personas consumidoras tendrán diferentes opciones:

[27] La 'tarifa cero' es una práctica comercial según la cual un proveedor de servicios de Internet aplica una 'tarifa cero' (o una tarifa más ventajosa) a todo o parte del tráfico de datos asociado a una aplicación o categoría de aplicaciones específicas, ofrecidas por socios de ese proveedor de servicios de Internet.

- Si se trata de un problema relacionado con datos personales (ver Punto 1 del Capítulo 3.4), se aplica el RGPD[28].
- De conformidad con la Directiva de Equipos de Radio, si hay un problema con la seguridad de los dispositivos (ver Punto 2 del Capítulo 3.4), los consumidores podrán, a partir de 2024, notificar a sus autoridades nacionales de vigilancia del mercado (a menudo la autoridad de telecomunicaciones), quienes iniciarán una investigación sobre ese dispositivo específico. La decisión de la autoridad de vigilancia del mercado puede llegar a ordenar la retirada de ese producto del mercado.
- Si un dispositivo no proveyó, según las expectativas de los consumidores, con la provisión de actualizaciones de seguridad (ver Punto 3 del Capítulo 3.4), las personas consumidoras tendrán derecho a rescindir el contrato, recibir una reducción proporcional en el precio o exigir que el dispositivo sea puesto en conformidad con las normas (ver la Directiva de Contenidos Digitales)
- En virtud de la Ley de Ciberseguridad, si la provisión de actualizaciones de seguridad es menor que la anunciada por el fabricante (ver Punto 4 del Capítulo 3.4), los consumidores podrán presentar una queja ante un organismo nacional. Si no están satisfechos con la decisión tomada, tendrán derecho a un recurso judicial efectivo.
- Si no se respeta la neutralidad de la red (ver Punto 5 del Capítulo 3.4), los consumidores podrán reclamar ante la autoridad reguladora de telecomunicaciones, quien tendrá que actuar en consecuencia.

3.8. Otros recursos: hojas informativas, publicaciones, enlaces

- Documento de trabajo del personal de la Comisión Europea - Avance del Internet de las cosas en Europa
- Investigación sectorial de la Comisión Europea sobre el Internet de las cosas (IoT) de consumo
- Documento de posicionamiento de BEUC: Proteger a los consumidores europeos en el mundo de los dispositivos conectados
- Hoja informativa de BEUC: Garantizar productos de consumo ciberseguros
- AK EUROPA - Expectativas de los consumidores sobre el Internet de las Cosas

[28] Ver nota al pie anterior.