OECD publishing

CATALIZADORES DIGITALES DE LA ECONOMÍA MUNDIAL

DOCUMENTO DE REFERENCIA PARA LA CONFERENCIA MINISTERIAL DEL CDEP

OECD DIGITAL ECONOMY PAPERS
Noviembre de 2022 **No. 337**

OCDE
MEJORES POLÍTICAS PARA UNA VIDA MEJOR

Prólogo

En este documento se analizan tres catalizadores digitales subyacentes de la economía digital — plataformas en línea, flujos de datos transfronterizos y seguridad digital— y los desafíos y oportunidades que plantean a los responsables de la formulación de políticas. Dado que estos problemas revisten carácter internacional, el informe señala la importancia de buscar una respuesta política global.

El presente documento proporciona información de referencia para sustentar los debates sobre el Tema 1 de la Conferencia ministerial del Comité de Políticas de Economía Digital: *Catalizadores digitales de la economía mundial*, que tendrá lugar los días 14 y 15 de diciembre de 2022 en Gran Canaria, España. Ofrece información relacionada con las sesiones de la conferencia ministerial sobre «Desarrollo de políticas de las plataformas en línea», «Fomentando la confianza en los flujos de datos transfronterizos» y «Reforzando las bases de la seguridad digital en productos y servicios».

Este documento ha sido redactado por Angela Attrey, Thyme Burdon, Francesca Casalini, Simon Lange y Peter Stephens, bajo la supervisión de Audrey Plonk, jefa de la División de Políticas de Economía Digital de la OCDE. Ha contado con las contribuciones de Gallia Daor y Angela Gosmann, y el apoyo editorial de Sebastian Ordelheide y Misha Pinkhasov. Tanto la conferencia ministerial como los trabajos conexos han contado con el generoso respaldo del Gobierno de España.

Este informe fue aprobado y desclasificado mediante procedimiento escrito por el Comité de Políticas de Economía Digital el 26 de octubre de 2022 y preparado para su publicación por la Secretaría de la OCDE.

Nota para las delegaciones:

Este documento también está disponible en O.N.E. con el código de referencia:

DSTI/CDEP(2022)11/FINAL

Índice

GRÁFICOS

Resumen ejecutivo

Una parte cada vez mayor de la actividad económica mundial está impulsada por las tecnologías digitales. Si bien dichas tecnologías —y los nuevos modelos de negocio que estas posibilitan— aportan notables beneficios, los cambios fundamentales que conllevan exigen desarrollar nuevos marcos políticos a escala mundial. A pesar de la saturación que caracteriza el panorama digital, hay tres catalizadores que destacan como prioritarios en las agendas políticas:

- **Las plataformas en línea** permiten las transacciones e interacciones entre múltiples conjuntos distintos de usuarios en todo el mundo. Asimismo, abren mercados y ofrecen oportunidades a los consumidores y las empresas, incluso entre partes desconocidas. No obstante, también plantean problemas de competencia y de protección del consumidor. Ante esto, la fragmentación de las respuestas políticas y normativas genera costes e incertidumbre para las empresas y los consumidores y exige que haya una coordinación transnacional.
- **Los flujos de datos transfronterizos** permiten a las empresas crear y gestionar complejas cadenas de suministro mundiales, compartir datos de investigación y facilitar las comunicaciones. Sin embargo, por otra parte, intensifican las preocupaciones políticas, llevando a los gobiernos a adoptar medidas políticas y normativas que regulan si los datos pueden cruzar las fronteras y de qué manera. Corresponde a los responsables de la formulación de políticas analizar esta evolución y garantizar que la fragmentación y la falta de transparencia y de claridad normativa no obstaculizan las oportunidades económicas ni socavan los objetivos que estas normativas pretenden alcanzar.
- **La seguridad digital** promueve la confianza y el crecimiento de la transformación digital. Sin embargo, el ritmo trepidante de esta transformación digital no ha ido acompañado de avances equivalentes en la seguridad de los servicios en línea y los productos conectados. Los usuarios finales rara vez pueden evaluar adecuadamente los enfoques de seguridad, lo que da lugar a fallos del mercado que socavan la confianza de los consumidores y ponen en riesgo el sistema. Muchos de los desafíos en materia de seguridad digital son internacionales, por lo que las vulnerabilidades y las malas prácticas deben combatirse a nivel mundial para maximizar el impacto de las medidas.

La forma más adecuada de abordar los desafíos asociados a estos catalizadores es a través de la cooperación internacional, procurando equilibrar cuidadosamente los objetivos de las políticas nacionales con los beneficios que pueden derivarse de una economía digital globalizada. La falta de coordinación internacional conlleva el riesgo de instaurar un panorama político fragmentado en el que pocas empresas serán capaces de desenvolverse, y todo ello con un coste considerable para los consumidores.

La OCDE desempeña desde hace tiempo un papel de liderazgo en materia de políticas digitales, en particular a través de sus estándares internacionales y orientaciones políticas. Su experiencia en la medición, el seguimiento y la evaluación de las tecnologías digitales y el impacto social de estas goza de reconocimiento internacional. La OCDE también brinda un modelo de diálogo inclusivo y global entre múltiples partes interesadas. Gracias al apoyo continuo de sus miembros y a través del diálogo con las instituciones internacionales pertinentes y los actores relevantes, la OCDE puede respaldar las

ambiciones de los países de lograr una economía mundial cuyo desarrollo venga estimulado por las tecnologías digitales.

1 Introducción

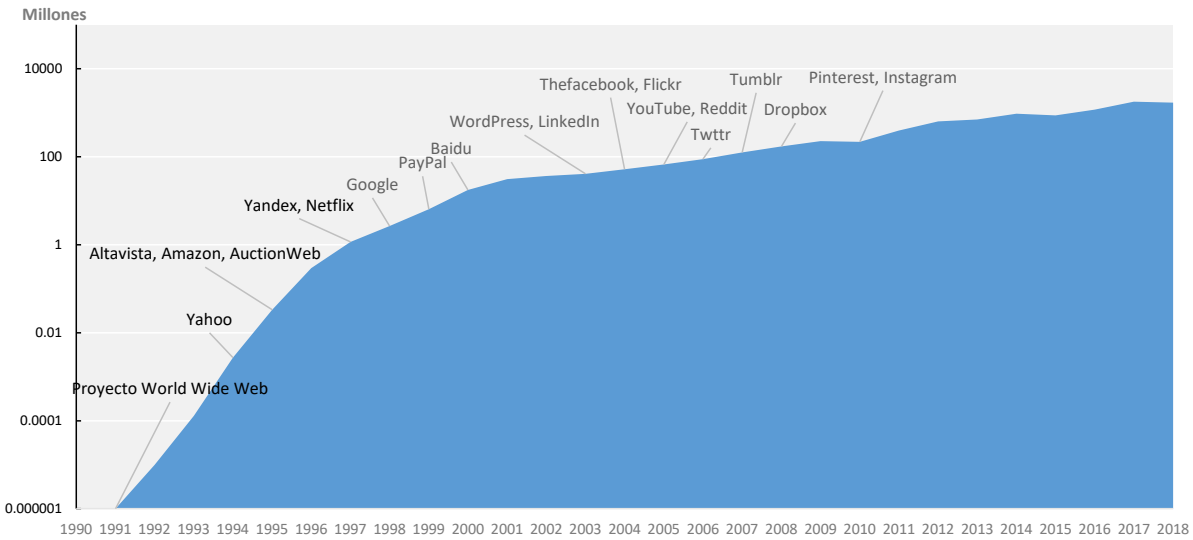
A partir de unos humildes comienzos, se sentaron los cimientos de una economía global

Para los primeros usuarios, la World Wide Web era un lugar extraño y maravilloso lleno de experimentos aparentemente intrascendentes. El primer sitio web se publicó en 1991 y contenía una descripción de la Web y explicaba cómo podía utilizarse. A finales de 1992, solo había diez sitios web en línea, que se dedicaban al software libre, la recopilación aleatoria de información y el humor *nerd*. La primera webcam, que empezó a emitirse a finales de 1993, monitorizaba el nivel de café de la cafetera de un laboratorio de informática de la Universidad de Cambridge.

A partir de estos humildes comienzos, el número de sitios web ha aumentado de forma fulgurante. En 1994 se lanzó *Jerry and David's Guide to the World Wide Web*, que más tarde se rebautizó como Yahoo. Junto con navegadores como Mosaic y Netscape, lanzados en 1993 y 1994, respectivamente, los motores de búsqueda permitieron que distintas partes de la Web fueran accesibles a un público más amplio. Las innovaciones complementarias, como la banda ancha y las tecnologías móviles, propiciaron que más personas se conectaran. La Web pasó de tener un solo sitio en 1991 a más de un millón en 1997. Diez años después, había más de 100 millones (Gráfico 1).

Gráfico 1. Número de sitios web, 1991-2018

Millones, escala logarítmica



Nota: Los sitios web se refieren a nombres de host únicos. El número de sitios web activos (en contraposición a los dominios aparcados o similares) podría ser sustancialmente menor.
Fuente: Netcraft (2022[1]), Web Server Survey, https://news.netcraft.com/archives/category/web-server-survey/; Gray (1996[2]), Web Growth Summary, https://www.mit.edu/people/mkgray/net/web-growth-summary.html

Internet —el sistema mundial de redes informáticas interconectadas— impulsa la innovación (OCDE, 2016[3]). Detrás de algunos de los sitios web que aparecieron entre 1995 y 2005 había empresas jóvenes que estaban creando nuevas aplicaciones y servicios. Algunas de ellas, como Amazon, Baidu, Facebook, Google, Netflix y PayPal, son ahora nombres muy conocidos. La competencia era feroz, como demuestra la conocida como «*browser wars*» (o «guerra de navegadores», esa continua batalla por el mercado que enfrenta a los navegadores de Internet). Las empresas basadas en plataformas, como Amazon, Airbnb y Uber, transformaron sectores enteros, mientras que las empresas tradicionales pasaron a apoyarse en las tecnologías digitales para optimizar sus procesos y crear intrincadas cadenas de suministro mundiales.

Catalizadores digitales de la economía mundial y los desafíos políticos que plantean

Las tecnologías y los servicios digitales basados en Internet son ahora la base de la economía mundial, promoviendo nuevos modelos de negocio, conexiones, transacciones y un acceso sin precedentes a la información, con independencia de la ubicación geográfica. Aunque son muchos los factores relevantes —desde la conectividad hasta las habilidades—, este documento examina tres catalizadores digitales clave de la economía mundial que han pasado a ocupar un lugar destacado en las agendas políticas:

- **Plataformas en línea.** La conexión de usuarios de todo el mundo posibilita una actividad económica global al proporcionar a las empresas acceso a más mercados y a los consumidores, a más contenidos y productos. Sin embargo, aunque el primer ecosistema digital rebosaba de energía emprendedora, cada vez preocupa más que este dinamismo haya decaído y que las plataformas establecidas se hayan atrincherado. Juristas y economistas señalan que el poder de mercado de las empresas digitales parece ir en aumento, al tiempo que crece la preocupación por la protección de los consumidores en línea.
- **Flujos de datos transfronterizos.** La arquitectura de Internet permite que los datos se muevan sin problemas entre dispositivos conectados a la red en cualquier parte del mundo, lo que hace posible la coordinación de las cadenas de valor mundiales y la prestación transfronteriza de servicios. Sin embargo, los gobiernos están adoptando cada vez más medidas normativas y políticas que regulan la transferencia de datos entre jurisdicciones. Los usuarios de Internet tienen la sensación creciente de que son ellos, y no las cafeteras, los que están siendo vigilados en línea. Esto hace que la protección de la privacidad sea una preocupación destacada, junto con la protección de los derechos de propiedad intelectual y otros objetivos políticos.
- **Seguridad digital.** Sin la seguridad digital, las personas y las organizaciones no podrían utilizar con confianza los productos y servicios digitales que impulsan cada vez más la producción y el comercio internacionales. A medida que una parte cada vez mayor de la economía depende de las tecnologías digitales, aumentan los riesgos en materia de seguridad digital: una seguridad deficiente puede provocar daños emocionales, financieros y físicos a una escala sin precedentes. Hasta la fecha, el ritmo fulgurante de la transformación digital no ha ido acompañado de un refuerzo equivalente de los estándares de seguridad.

Un llamamiento a la gobernanza digital mundial

En sus inicios, la World Wide Web era accesible y comprensible para muy pocas personas. Hoy en día, más de la mitad de la humanidad está en línea de alguna forma. A medida que la transformación digital ha ido evolucionando, la mayoría de los países de la OCDE han adoptado estrategias digitales nacionales (Gierten and Lesher, 2022[4]) y han establecido leyes, normativas y otro tipo de disposiciones con el fin de proteger a los consumidores y, al mismo tiempo, propiciar la transformación digital y garantizar que esta beneficie a todos.

Sin embargo, muchos de los desafíos políticos en este ámbito revisten carácter internacional, por lo que la transformación digital requiere una gobernanza más sólida a escala mundial de modo que las personas y las empresas puedan aprovechar plenamente las oportunidades que esta ofrece. En consecuencia, los responsables de la formulación de políticas han de trabajar juntos para encontrar enfoques coherentes que rijan los catalizadores digitales de la economía mundial.

Recuadro 1. Selección de investigaciones en materia de políticas e instrumentos jurídicos de la OCDE en relación con los catalizadores digitales de la economía mundial

Plataformas en línea

- OCDE (de próxima publicación[5]), "Data shaping firms and markets", OECD Digital Economy Papers, OECD Publishing, Paris
- OCDE (2022[6]), "The role of online marketplaces in protecting and empowering consumers: Country and business survey findings", OECD Digital Economy Papers, No. 329, OECD Publishing, Paris, https://doi.org/10.1787/9d8cc586-en
- OCDE (2019[7]), An Introduction to Online Platforms and Their Role in the Digital Transformation, OECD Publishing, Paris, https://doi.org/10.1787/53e5f593-en.
- OCDE (2019[8]), Unpacking E-commerce: Business Models, Trends and Policies, OECD Publishing, Paris, https://doi.org/10.1787/23561431-en
- OCDE (2016[9]), Recommendation of the Council on Consumer Protection in E-Commerce

Flujos de datos transfronterizos

- OCDE (de próxima publicación[10]), "Fostering cross-border data flows with trust", OECD Digital Economy Papers, OECD Publishing, Paris
- OCDE (2021[11]), Recommendation of the Council on Enhancing Access to and Sharing of Data
- OCDE (2013[12]), Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (the *OECD Privacy Guidelines*)

Seguridad digital

- OCDE (de próxima publicación[13]), Recommendation of the Council on Digital Security Risk Management
- OCDE (de próxima publicación[14]), Recommendation of the Council on National Digital Security Strategies
- OCDE (de próxima publicación[15]), Recommendation of the Council on the Digital Security of Products and Services
- OCDE (de próxima publicación[16]), Recommendation of the Council on the Treatment of Digital Security Vulnerabilities
- OCDE (de próxima publicación[17]), Policy Framework on Digital Security
- OCDE (2021[18]), "Understanding the digital security of products: An in-depth analysis", OECD Digital Economy Papers, No. 305, OECD Publishing, Paris, https://doi.org/10.1787/abea0b69-en
- OCDE (2021[19]), "Encouraging vulnerability treatment: Overview for policymakers", OECD Digital Economy Papers, No. 307, OECD Publishing, Paris, https://doi.org/10.1787/0e2615ba-en

2 Plataformas en línea: permiten transacciones e interacciones globales, pero alteran los marcos políticos

Las plataformas en línea son quizás el modelo de negocio digital más arquetípico: un servicio digital que permite la interacción de múltiples conjuntos distintos de usuarios a través de Internet (OCDE, 2019[7]). Las plataformas en línea pueden abrir nuevos mercados y ofrecer oportunidades tanto para los consumidores como para las empresas, permitiendo transacciones e interacciones a escala mundial que de otro modo serían imposibles, entre otras cosas, proporcionando herramientas que garantizan intercambios seguros y de confianza entre partes desconocidas (Burdon, 2021[20]). Las plataformas suelen ofrecer productos y servicios nuevos y de alta calidad a precios bajos, o incluso sin coste monetario (aunque a veces a cambio de la recopilación de datos). Las plataformas en línea han causado un gran impacto en las empresas analógicas establecidas y han propiciado la difusión de información que ayuda a los consumidores a tomar decisiones informadas, como cambiar de producto, servicio o proveedor (OCDE, 2022[21]).

En los albores de la World Wide Web, los modelos de negocio experimentales tuvieron un auge y caída vertiginosos (Furman et al., 2019[22]). Sin embargo, desde mediados de la década de 1990, un pequeño número de plataformas en línea se han hecho un nombre, captando atención, talento, datos e ingresos. Aunque las plataformas en línea difieren en tamaño, usuarios y funcionalidad (OCDE, 2019[7]), las políticas y el interés público se centran en este grupo de gigantes digitales en cuestiones que van desde la privacidad hasta la moderación de contenidos y la intermediación en el mercado laboral. Dado que este grupo acapara la mayor parte de los principales mercados en línea, como el comercio electrónico, las búsquedas, la publicidad en línea y las redes sociales (OCDE, 2022[21]), su efecto sobre la competencia ha suscitado una atención especial.

Las investigaciones económicas más amplias sugieren que la intensidad competitiva en los mercados digitales está disminuyendo. En todos los países de la OCDE, hay menos empresas que entran y salen de los mercados (OCDE, 2021[23]; Bajgar et al., 2019[24]) —un fenómeno aún más pronunciado en aquellos sectores que se caracterizan por el uso intensivo de la tecnología digital (Calvino and Criscuolo, 2019[25]). A pesar de que las empresas digitales de nueva creación atraen importantes inversiones de capital y de riesgo, cada vez es más frecuente que estas acaben siendo adquiridas por operadores más grandes antes de tener la oportunidad de crecer y prosperar (Bajgar, Criscuolo and Timmis, 2021[26]). Las industrias del conjunto de la OCDE están cada vez más concentradas (Bajgar et al., 2019[24]), pero esto es especialmente destacable en los sectores que dependen de determinados elementos como el *software* y los datos (Bajgar, Criscuolo and Timmis, 2021[26]). Estas tendencias son preocupantes porque la competencia resulta esencial para bajar los precios, fomentar la innovación, el crecimiento y el bienestar a largo plazo (OCDE, 2022[21]).

En este contexto, los expertos sostienen que ciertas plataformas digitales gozan de un poder de mercado duradero (OCDE, 2022[27]; OCDE, 2022[21]; OCDE, 2021[28]) y señalan que esto se debe a los siguientes factores:

- **Fuertes efectos de red.** A medida que crece el número de usuarios, el valor del producto para los usuarios aumenta, lo que a su vez atrae a otros usuarios. Esto puede dar lugar a que un mercado se «incline» hacia el monopolio (también conocido como efecto «el ganador se lo lleva todo») (OCDE, 2022[21]).
- **Economías de escala.** Dado que el coste de añadir un usuario adicional suele ser bajo, las plataformas pueden crecer fácilmente y ampliar su cobertura geográfica sin necesidad de hacer una inversión adicional significativa.
- **Recopilación de datos.** Las plataformas en línea pueden recopilar de los usuarios datos detallados de todos los participantes de un mercado, incluidos los consumidores, los anunciantes y otras empresas. Estos datos pueden mejorar la calidad de los productos, reforzar los efectos de red, dirigir los productos a diferentes públicos y orientar la toma de decisiones de los consumidores (OCDE, 2022[29]). La ventaja que otorga la economía de escala, unida a la que confieren los datos de los que disponen las plataformas en línea establecidas, puede suponer una barrera de entrada para otros operadores (OCDE, 2022[27]).
- **Integración vertical, conglomerados y vínculos entre mercados.** Las plataformas en línea suelen ofrecer paquetes de múltiples productos digitales, como sistemas operativos y dispositivos, en una oferta sin fisuras y basada en datos que puede dificultar que los consumidores cambien de proveedor (OCDE, 2022[27]). También pueden aprovechar su posición dominante en un mercado, por ejemplo, utilizando sus datos o paquetes para entrar en otro. Algunas plataformas en línea tienen modelos de negocio integrados verticalmente, lo que puede obligar a los competidores en sentido descendente a depender de ellas para acceder a los clientes y podría dar lugar a denuncias de conductas anticompetitivas (por ejemplo, cuando una plataforma compite en sentido descendente en el mercado en el que opera) (OCDE, 2021[28]).

En respuesta, muchos países han adaptado instrumentos jurídicos tradicionales, han aumentado la capacidad técnica de las autoridades y han establecido entre sus prioridades hacer cumplir las leyes de competencia y protección del consumidor en los mercados digitales. Además, muchas jurisdicciones, a menudo teniendo en cuenta las características estructurales de los mercados digitales que pueden conducir a la concentración, han ido más allá de esas herramientas tradicionales proponiendo o aprobando iniciativas normativas adicionales aplicables a un conjunto limitado de empresas, entre las que suelen estar las plataformas en línea más destacadas (OCDE, 2021[28]). Si bien estas normativas difieren entre sí, en general, todas tienden a abordar las cuestiones siguientes (OCDE, 2021[28]):

- **Problemas relacionados con los datos,** como la obligación de conceder a los competidores acceso a conjuntos de datos importantes y de aplicar medidas de portabilidad e interoperabilidad de los datos.
- **Percepción que se tiene de las plataformas en línea como «*gatekeepers*» (o «guardianes»),** que se combate con medidas relacionadas con la limitación de las prácticas de autopreferenciación de sus propios bienes, servicios y paquetes.
- **Obligaciones de transparencia y de ceñirse a prácticas comerciales justas**, que incluyen códigos de conducta obligatorios y requisitos de transparencia de los algoritmos, las prácticas comerciales y publicitarias y la recopilación de datos. Algunas normas propuestas establecen restricciones en cuanto a la forma en que se pueden conservar, procesar o transferir los datos de los usuarios, sean estos observados o inferidos.
- **Requisitos adicionales para las fusiones**, como la obligación de informar a los reguladores de todas las fusiones y adquisiciones pertinentes.

Aunque las normativas propuestas comparten ciertas características y todas ellas tienen como objetivo promover la competencia en el ámbito línea, las medidas difieren sustancialmente entre unas jurisdicciones y otras. En este sentido, un panorama político y normativo fragmentado para las plataformas conlleva costes tanto para las empresas como para los consumidores, aumenta la incertidumbre y puede suponer un obstáculo para la innovación que incrementa el bienestar social (OCDE, 2021[28]). Asimismo, como las principales plataformas en línea operan a nivel mundial, los efectos de las normativas que se aprueban en una jurisdicción pueden extenderse a otras. Un enfoque global coherente mejoraría la eficacia normativa y garantizaría que los mercados digitales sigan siendo competitivos y de acceso irrestricto y contribuyan al bienestar económico.

Los responsables de la formulación de políticas también se están centrando en cuestiones relacionadas con la protección de los consumidores en todo el mundo. En muchos casos, las plataformas en línea tienen una responsabilidad limitada por la conducta ilegal de sus usuarios, dado que actúan como meros intermediarios que ponen en contacto a comerciantes y consumidores (Burdon, 2021[20]). Sin embargo, la capacidad de las plataformas para controlar su propio ecosistema es una de sus señas de identidad, ya que las experiencias positivas contribuyen a la fidelización de los usuarios, algo fundamental para que la plataforma tenga éxito (OCDE, 2019[7]). Esto se consigue, por lo general, mediante el establecimiento de normas que regulan quién puede unirse a una plataforma y cómo ha de comportarse en ella. Las plataformas pueden supervisar la conducta de los usuarios para asegurarse de que se cumplen las normas y promover su cumplimiento actuando contra los usuarios que las incumplen, por ejemplo, impidiéndoles el acceso.

En la práctica, sin embargo, a pesar de la inversión que realizan en herramientas y procesos de control para detectar los incumplimientos, las plataformas tienen dificultades para regular el comportamiento de sus usuarios. Algunas empresas toman medidas para proteger a los consumidores, pero las estafas, los productos inseguros y falsificados y las calificaciones y reseñas falsas siguen presentes en muchos mercados en línea (OCDE, 2022[6]). Esto ha llevado a los responsables de la formulación de políticas y a las autoridades de defensa de la competencia y de los consumidores a instar a las plataformas a avanzar hacia una mayor autorregulación y modelos alternativos de regulación impulsada por los gobiernos, como los compromisos por la seguridad de los productos (OCDE, 2021[30]).[1] También está llevando a los responsables de la formulación de políticas a plantearse si las plataformas deberían asumir una mayor responsabilidad por las acciones de sus usuarios que redunde en una mayor protección de los consumidores.

3 Flujos de datos transfronterizos: promueven el comercio y la cooperación mundial, pero plantean ciertas inquietudes en materia de políticas públicas

La arquitectura de Internet permite que la información fluya entre y a través de las redes y las fronteras; característica que tanto empresas como consumidores no tardaron en aprovechar para desarrollar nuevos modelos de negocio y acceder a los mercados mundiales. Hoy en día, los flujos de datos sustentan una amplia gama de intercambios internacionales de bienes y servicios. Estos flujos permiten que las empresas creen y gestionen complejas cadenas de suministro mundiales, que las organizaciones compartan datos para la investigación y que los consumidores busquen información sobre bienes y servicios ofrecidos en todo el mundo.

Aunque es probable que la contribución de los flujos de datos transfronterizos al valor añadido mundial sea importante, esta no se conoce bien. No resulta fácil discernir el valor de dicha contribución a partir de las estadísticas comerciales o de las tecnologías de la información y la comunicación (TIC), y todavía no se dispone de pruebas empíricas definitivas al respecto. Dicho esto, se ha atribuido a las TIC el mérito de haber propiciado la fase más reciente de integración mundial, que ha conducido al rápido desarrollo económico de algunos países en desarrollo (Baldwin, 2017[31]).

Al mismo tiempo, el flujo de datos a través de las fronteras acrecienta ciertas inquietudes en materia de políticas públicas, de modo que los gobiernos han tomado medidas para regular si los datos pueden cruzar las fronteras y de qué manera. Entre los fundamentos de estas normativas y políticas públicas se incluyen los siguientes (Casalini and López-Gonzalez, 2019[32]; Aaronson, 2019[33]):

- **Protección de la privacidad.** En el caso de los datos personales, los flujos transfronterizos plantean cuestiones relacionadas con la protección de datos y la privacidad, especialmente cuando los marcos normativos de un país difieren de los de las jurisdicciones receptoras. A algunos gobiernos también les preocupa que los datos personales transferidos al extranjero puedan estar expuestos a la vigilancia de gobiernos extranjeros.
- **Seguridad.** Los gobiernos pueden regular los flujos de datos transfronterizos como forma de proteger la información que consideran sensible desde el punto de vista de la seguridad nacional o para evitar perjuicios a los consumidores nacionales (por ejemplo, fraude con tarjetas de crédito, robo de identidad) y a las empresas (por ejemplo, ataques de *ransomware*).
- **Protección de la propiedad intelectual.** Los gobiernos podrían regular los flujos de datos transfronterizos como una forma de proteger los derechos de propiedad intelectual, incluyendo las marcas, los derechos de autor y los secretos comerciales.

- **Acceso normativo.** Los reguladores nacionales a menudo exigen el acceso a ciertos datos en aras del cumplimiento de la ley. Algunos gobiernos pueden exigir que los datos se almacenen en el país de manera que quede garantizada la posibilidad de acceder a ellos.

Además, a menudo se sostiene que los responsables de la formulación de políticas podrían establecer determinados requisitos para los flujos de datos transfronterizos o exigir a las empresas que almacenen los datos en el territorio nacional como una forma de implementar una política industrial digital (o proteccionismo digital). También se ha acusado a los regímenes autocráticos de impedir los flujos de datos transfronterizos para frenar la libertad de expresión y como un medio de represión política (Fan and Gupta, 2018[34]).

Como reflejo de esta variedad de motivaciones y de las diferencias culturales e históricas que inspiran los distintos enfoques políticos, los gobiernos de todo el mundo optan por diferentes tipos de normativas para regular los flujos de datos transfronterizos. Algunos estipulan amplios principios de responsabilidad con alcance extraterritorial; mientras que otros exigen salvaguardias específicas para las transferencias transfronterizas, como la obligación de que el país de destino esté en la lista blanca de las autoridades nacionales (aunque los criterios varían de un país a otro y no siempre son transparentes) o que entre las entidades que intercambian los datos medie un contrato (en algunos casos, con determinadas cláusulas previamente estipuladas). Otras normativas exigen la previa verificación y aprobación de cualquier transferencia de datos al extranjero. Además de las diferencias de contenido entre las normativas, estas se aplican a distintos tipos de datos y sectores; y las definiciones y los conceptos pueden variar, como por ejemplo a la hora de definir qué se entiende por «información personal».

Las normativas que promueven la confianza en línea favorecen que los datos sean un elemento catalizador de la economía mundial. No obstante las normativas también pueden ser gravosas, especialmente cuando son poco precisas, fragmentarias o poco transparentes. La disparidad que existe en el alcance y la aplicación de las normas entre jurisdicciones enfrenta a las empresas digitales a un panorama normativo mundial complejo e incierto. Por ejemplo, los intentos de establecer una base legal para las transferencias de datos personales entre los EE. UU. y la UE han fracasado en dos ocasiones desde 2015. Las empresas necesitan un entorno normativo estable para tomar decisiones y hacer planes de inversión, y preocupa que este contexto confuso y cambiante pueda frenar las oportunidades económicas. Algunos requisitos pueden ser técnicamente desafiantes, cuando no inviables, y es posible que las pequeñas empresas —incluidas las empresas emergentes de alto crecimiento— tengan más dificultades para asumir los costes de cumplimiento. Esto plantea la posibilidad de una concentración aún mayor de los mercados digitales con la consiguiente disminución del dinamismo empresarial.

Para hacer frente a la fragmentación y mitigar estos desafíos, es fundamental la cooperación internacional en materia de «libre circulación de datos con confianza». Existen fundamentos en los que basarse, como las Directrices de Privacidad de la OCDE, que proporcionan una base para regular la privacidad; la Cooperación Económica Asia-Pacífico, que ha desarrollado su propio sistema de certificación para la transferencia de datos entre las economías participantes; o el Convenio 108 del Consejo Europeo, que establece normas sobre la protección de datos y las transferencias entre las partes. Algunos acuerdos comerciales contienen disposiciones vinculantes para que los datos circulen entre países cuando existen marcos de protección. El fomento de la interoperabilidad de los marcos de protección de la privacidad ha sido un objetivo prioritario de modo que los países con distintas normas de protección de la privacidad puedan seguir intercambiando datos. Por último, las tecnologías que refuerzan la privacidad pueden facilitar el intercambio y el uso de datos personales, también a través de las fronteras, con menores riesgos para la privacidad. Corresponde a los responsables de la formulación de políticas analizar estos avances e identificar los próximos pasos a dar en aras de establecer políticas que resulten adecuadas tanto para los individuos como para las empresas.

4 Seguridad: ¿catalizador fundamental de la transformación digital o su talón de Aquiles?

A medida que más ámbitos de la economía pasan a depender de las tecnologías digitales, aumenta lo que está en juego en materia de seguridad digital. Así, la eficacia en esta materia favorece la confianza y el crecimiento de la transformación digital. Por desgracia, hasta la fecha, el ritmo fulgurante de la transformación digital no ha ido acompañado de una mejora proporcional en la calidad de la seguridad de los dispositivos y servicios. Aunque se han hecho algunos progresos para normalizar las buenas prácticas (por ejemplo, la gestión coordinada de vulnerabilidades, o los requisitos de seguridad de la Internet de las cosas), las organizaciones no aplican estos requisitos básicos a todos los niveles. Los responsables de la formulación de políticas de todo el mundo tienen ahora la oportunidad de abordar estos desafíos —a menudo internacionales— centrándose en los resultados deseados para el usuario final y basándose en las Regulaciones Técnicas Globales y en las mejores prácticas de la industria para reforzar la interoperabilidad.

La Internet de las cosas (IoT, por sus siglas en inglés) —el conjunto de dispositivos y objetos conectados a Internet— encarna un desafío más amplio en materia de seguridad digital. La IoT de los consumidores, también conocida como productos «inteligentes» o «conectados», amplía la superficie de ataque más allá de las tecnologías tradicionales de la información y las comunicaciones (TIC) utilizadas por los consumidores, las empresas y los gobiernos. Los dispositivos inteligentes constituyen una creciente superficie de ataque de productos inseguros que los consumidores adoptan e integran en las redes. En 2019 había 7.700 millones de dispositivos IoT (Statista, 2022[35]), y según una encuesta reciente, el 78,4% de los fabricantes de dispositivos IoT de consumo no incorporan un proceso interno para abordar las vulnerabilidades (IoT Security Foundation, 2021[36]), lo cual es fundamental para la protección continua del producto y su usuario.

Un número relativamente pequeño de actores malintencionados ha sido capaz de capitalizar la transformación digital adoptando modelos de negocio de ciberdelincuencia que pretenden evadir el cumplimiento del Derecho tradicional. El *ransomware* se ha convertido en una amenaza común que afecta a todo tipo de empresas y organizaciones, independientemente de su tamaño y ubicación. En Estados Unidos, en 2021, los operadores de infraestructuras críticas presentaron 649 denuncias ante el FBI, y en 14 de los 16 sectores de infraestructuras críticas hubo al menos un miembro que fue víctima de un ataque de *ransomware* (FBI, 2021[37]). Del mismo modo, los sistemas de información presentan vulnerabilidades relacionadas con la forma en que el *software* se diseña, desarrolla, implementa y actualiza. Los actores maliciosos desarrollan, comercian y utilizan herramientas como los *malware* o programas maliciosos para explotar estas vulnerabilidades mediante ataques que perjudican a las empresas, los gobiernos y las personas, amenazan las actividades esenciales y socavan la confianza en la transformación digital.

Los costes de un ecosistema digital inseguro pueden ser enormes. Las estimaciones sobre el coste potencial mundial de los ciberataques se han elevado a 6 billones de USD al año (lo que equivale al PIB combinado de Francia y Alemania) y aumentan cada año (OCDE, 2021[38]) Los atacantes buscan víctimas

digitalmente dependientes. Según el CyberPeace Institute, en 2021 se produjeron 253 incidentes de este tipo que afectaron al sector sanitario de 32 países, con una media de más de 21 días de impacto operativo y más de 13 millones de registros afectados (CyberPeace Institute, s.f.[39]).

Lo ideal sería que las fuerzas del mercado garantizaran que los productos —incluido el código (por ejemplo, el *software*, los dispositivos IoT, etc.)— y los servicios relacionados (como la nube) fueran suficientemente seguros, y que los desarrolladores reforzaran la seguridad en proporción al riesgo al que se enfrentan los usuarios y lo hicieran a lo largo de todo el ciclo de vida del producto. Sin embargo, los análisis de la OCDE evidencian que las deficiencias del mercado impiden a los actores relevantes evaluar con precisión la seguridad digital de los productos y servicios, y que es poco probable que los incentivos del mercado por sí solos solucionen las deficiencias en la gestión de los riesgos de seguridad digital (OCDE, 2021[38]). El problema es que no está clara la asignación de responsabilidades a la hora de solucionar las vulnerabilidades y mejorar la seguridad, en particular, a causa de la complejidad y opacidad que caracteriza las cadenas de suministro.

A los usuarios finales, en concreto a las pequeñas y medianas empresas y a los consumidores, les suele resultar difícil saber hasta qué punto la seguridad está incorporada por diseño en los productos y servicios que adquieren. Los proveedores, dado que no se ven expuestos a ninguna presión en este sentido, y ello sumado a complejidades como las cadenas de suministro internacionales, a menudo descuidan la seguridad digital considerándola un asunto «de última hora», lo que permite a los actores maliciosos servirse de estos productos para lanzar ataques, incluso de alcance transfronterizo. En términos más generales, existen percepciones erróneas de los riesgos en materia de seguridad digital y un desajuste de los incentivos del mercado. En una encuesta realizada en 2020, el 28% de los consumidores del Reino Unido afirmaron que no buscaban activamente comprar un producto conectado a Internet por temores relacionados con la seguridad (DCMS, 2020[40]).

Muchos de los desafíos a los que se enfrenta la seguridad digital (y la transformación digital en general) son globales. Las cadenas de suministro son complejas e internacionales, lo que plantea importantes desafíos a los legisladores. Mientras tanto, los proveedores de servicios gestionados y en la nube ofrecen servicios transfronterizos, que pueden ser susceptibles de ser atacados por agentes maliciosos desde cualquier lugar. No obstante, los especialistas en materia de seguridad también operan más allá las fronteras, de modo que los marcos legales de «puerto seguro», para que sean eficaces, deben diseñarse sobre la base de principios reconocidos internacionalmente.

5 Conclusión: ¿un sistema de Bretton Woods digital? El papel de la OCDE en la gobernanza digital mundial

Internet se expandió para dar cabida a un crecimiento masivo de usuarios y dispositivos de todo el mundo (OCDE, 2016[3]), dando paso a una era de actividad económica de ámbito igualmente global. La transformación digital permite que los servicios, las tecnologías, las aplicaciones y los dispositivos se extiendan a escala mundial. En un mundo interconectado e interdependiente, los desafíos políticos tienen un alcance intrínsecamente internacional, con efectos que se extienden fácilmente a través de las fronteras.

Sin embargo, los esfuerzos para gestionar los desafíos políticos que plantean las plataformas en línea, los flujos de datos transfronterizos y la seguridad digital se han llevado a cabo, fundamentalmente, a través de políticas de alcance nacional. Así, no solo es menos probable que estas políticas sean eficaces, sino que el panorama fragmentado resultante establece un contexto global desigual que resulta en una protección desigual para los consumidores y las empresas que operan en la economía mundial.

El periodo posterior a la Primera Guerra Mundial se caracterizó por las crisis económicas y el aumento de las tensiones geopolíticas. No obstante, en lugar de optar por la cooperación internacional, los países adoptaron políticas que les beneficiaban a costa de otros, profundizando las divisiones. Al final de la Segunda Guerra Mundial, un selecto grupo de países se reunió en Bretton Woods, en el estado norteamericano de New Hampshire, para crear un sistema de instituciones mundiales, inspirados por el convencimiento de que las ventajas de una economía mundial solo podrían alcanzarse plenamente mediante la cooperación.

Los expertos invocan cada vez más esta ola de multilateralismo de posguerra a la hora de reivindicar marcos de política digital global. Aunque la terminología que emplean es variada, se ha apelado a un «sistema de Bretton Woods para las políticas digitales» (Rockefeller Foundation, 2021[41]; Greenwald, 2020[42]; Clegg, 2021[43]; Tett, 2019[44]), un «Consejo de Estabilidad Digital» (CIGI, 2019[45]) o una «Convención de Ginebra digital» (Microsoft, 2017[46]). Las instituciones políticas se han hecho eco de la necesidad de contar con marcos políticos digitales globales, destacando tres características que estos deberían reunir: (1) el desarrollo de normas y principios internacionales mínimos comunes; (2) una mejor medición y seguimiento de las tecnologías y cuestiones digitales; y (3) la participación inclusiva de las múltiples partes interesadas (Banco Mundial, 2021[47]; Naciones Unidas, 2019[48]; UNCTAD, 2021[49]; Haksar et al., 2021[50]).

La OCDE —cuyos orígenes se sitúan en esa ola de multilateralismo y que cuenta con amplia experiencia en la elaboración de políticas digitales— está en condiciones de responder a estos llamamientos:

- **La OCDE lleva mucho tiempo liderando las cuestiones de política digital, incluido el establecimiento de normas y marcos políticos internacionales**. En 1980 desarrolló las *Directrices sobre protección de la privacidad de la OCDE*, revisadas en 2013, que siguen siendo la norma mínima global en materia de privacidad y protección codificada de datos en los países

de todo el mundo. La OCDE también desarrolló las primeras normas consensuadas internacionalmente en materia de seguridad digital para el crecimiento y la prosperidad (OCDE, de próxima publicación[13]; OCDE, de próxima publicación[14]; OCDE, de próxima publicación[15]; OCDE, de próxima publicación[16]), y principios para el acceso y el intercambio de datos (OCDE, 2021[11]), así como los innovadores *Principios de la OCDE sobre inteligencia artificial* (OCDE, 2019[51]) y la *Recomendación de la OCDE sobre la protección al consumidor en el comercio electrónico* (OCDE, 2016[52]). La aplicación de estas recomendaciones se revisa periódicamente. Además, la OCDE tiene experiencia en áreas políticas a las que afectan especialmente las cuestiones relacionadas con las tecnologías y los datos digitales —como la fiscalidad, la competencia, la protección del consumidor, la privacidad, la gobernanza de datos, la seguridad digital, el comercio y los mercados financieros y laborales— y ha desarrollado el primer marco político integral para el diseño y la implementación de políticas digitales a nivel del gobierno en su conjunto (OCDE, 2020[53]).

- **La OCDE es una institución reconocida por medir, supervisar y evaluar las tecnologías digitales y sus efectos económicos y sociales**. Es la organización que lidera los esfuerzos internacionales para medir los distintos aspectos de la transformación digital, incluyendo el comercio digital (OCDE-OMC-FMI, 2020[54]) y los datos (OCDE, forthcoming[55]) en las estadísticas económicas y a través de la *Hoja de ruta para medir la transformación digital* (OCDE, 2022[56]) En el marco de su labor de seguimiento de los avances de la economía digital, la OCDE ha desarrollado herramientas e indicadores para orientar la formulación de políticas, como el *OECD Going Digital Toolkit* (*Kit de herramientas para la transformación digital de la OCDE*) y el *OECD AI Policy Observatory* (*Observatorio de políticas de IA de la OCDE*). Además, se encarga de examinar y evaluar los efectos de las tecnologías digitales emergentes, como la inteligencia artificial y la cadena de bloques o *blockchain* (OCDE, 2022[57]).
- **La OCDE brinda un modelo de diálogo sobre políticas de economía digital de carácter inclusivo y global entre las múltiples partes interesadas.** En su condición de foro para el intercambio de ideas y buenas prácticas entre más de cien países, la OCDE reúne a responsables de la toma de decisiones y de la formulación de políticas de todo el mundo para compartir conocimientos, identificar las mejores prácticas y desarrollar políticas basadas en datos empíricos para un mundo digital en evolución. Los debates sobre políticas de economía digital en el seno de la OCDE siguen un modelo que prevé la participación de las múltiples partes interesadas y en el que se pone a disposición de la experiencia y los conocimientos de las empresas, los sindicatos, la sociedad civil y la comunidad técnica de Internet una plataforma que favorece que la transformación digital prospere e incorpore consideraciones de seguridad. Además, el trabajo de la OCDE sobre la reforma fiscal internacional en la era digital pone de manifiesto su capacidad para convocar a los países a un consenso sobre las complejas y transversales cuestiones que plantea la transformación digital (OCDE, 2022[58]). El *Foro Global de la OCDE sobre competencia* (OCDE, 2022[59]) y el *Foro Global de la OCDE sobre seguridad digital para la prosperidad* (OCDE, 2022[60]) son otros dos ejemplos de compromiso multilateral y multidisciplinar liderado por la OCDE.

Las instituciones y organizaciones políticas internacionales reconocen la necesidad de contar con marcos políticos digitales de carácter global. La OCDE, impulsada por los países y en diálogo con las organizaciones internacionales pertinentes, puede aprovechar su consolidado papel, sus conocimientos institucionales, su gran número de herramientas analíticas y su capacidad demostrada para trabajar con los países y los grupos de actores relevantes para establecer un plan ambicioso de formulación de políticas digitales y para gestionar las cuestiones políticas asociadas a una economía y sociedad globales, interdependientes y de marcado carácter digital.

Referencias

Aaronson, S. (2019), "What Are We Talking about When We Talk about Digital Protectionism?", *World Trade Review*, Vol. 18/4, pp. 541-577, https://doi.org/10.1017/S1474745618000198. [33]

Bajgar, M. et al. (2019), "Industry Concentration in Europe and North America", *OECD Productivity Working Papers*, No. 18, OECD Publishing, Paris, https://doi.org/10.1787/2ff98246-en. [24]

Bajgar, M., C. Criscuolo and J. Timmis (2021), "Intangibles and industry concentration: Supersize me", *OECD Science, Technology and Industry Working Papers*, No. 2021/12, OECD Publishing, Paris, https://doi.org/10.1787/ce813aa5-en. [26]

Baldwin, R. (2017), *The Great Convergence*, Harvard University Press, https://doi.org/10.4159/9780674972667. [31]

Banco Mundial (2021), *World Development Report*, World Bank Publishing, Washington DC, https://www.worldbank.org/en/publication/wdr2021. [47]

Burdon, T. (2021), "The role of online marketplaces in enhancing consumer protection", *OECD Going Digital Toolkit Notes No. 7*, OECD Publishing, Paris, https://doi.org/10.1787/ddca0e2e-en. [20]

Calvino, F. and C. Criscuolo (2019), "Business dynamics and digitalisation", *OECD Science, Technology and Industry Policy Papers*, No. 62, OECD Publishing, Paris, https://doi.org/10.1787/6e0b011a-en. [25]

Casalini, F. and J. López-Gonzalez (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Paper*, No. 220, OECD, Paris, https://doi.org/10.1787/b2023a47-en (accessed on 4 March 2022). [32]

CIGI (2019), *Digital Platforms Require Global Governance Frameworks*, https://www.cigionline.org/articles/digital-platforms-require-global-governance-framework/. [45]

Clegg, N. (2021), *A Bretton Woods for the Digital Age can Save the Open Internet*, https://www.afr.com/technology/a-bretton-woods-for-the-digital-age-can-save-the-open-internet-20211115-p5994h. [43]

CyberPeace Institute (s.f.), *Cyber Incident Tracer #HEALTH*, https://cit.cyberpeaceinstitute.org/explore (accessed on 11 July 2022). [39]

DCMS (2020), *Evidencing the Cost of the UK Government's Proposed Regulatory Interventions for Consumer IoT*, UK Department for Digital, Culture, Media & Sport, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products.pdf (accessed on 11 July 2022). [40]

Fan, Z. and A. Gupta (2018), *The Dangers of Digital Protectionism*, https://hbr.org/2018/08/the-dangers-of-digital-protectionism (accessed on 6 October 2022). [34]

FBI (2021), *Internet Crime Report*, U.S. Federal Bureau of Investigation, Washington, DC, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (accessed on 11 July 2022). [37]

Furman, J. et al. (2019), *Unlocking digital competition: Report from the Digital Comeptition Expert Panel*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf. [22]

Gierten, D. and M. Lesher (2022), "Assessing National Digital Strategies and Their Governance", *OECD Digital Economy Papers*, No. 324, OECD Publishing, Paris, https://doi.org/10.1787/baffceca-en (accessed on 11 July 2022). [4]

Gray, M. (1996), *Web Growth Summary*, https://www.mit.edu/people/mkgray/net/web-growth-summary.html (accessed on 17 October 2022). [2]

Greenwald, M. (2020), *A new era in financial diplomacy: The third evolution of Bretton Woods*, https://www.atlanticcouncil.org/blogs/new-atlanticist/a-new-era-in-financial-diplomacy-the-third-evolution-of-bretton-woods/. [42]

Haksar, V. et al. (2021), *Toward a Global Approach to Data in the Digital Age*, https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2021/10/06/Towards-a-Global-Approach-to-Data-in-the-Digital-Age-466264. [50]

IoT Security Foundation (2021), *The Contemporary Use of Vulnerability Disclosure in IoT (Report 4)*, https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/The-Contemporary-Use-of-Vulnerability-Disclosure-in-IoT-IoTSF-Report-4-November-2021.pdf (accessed on 11 July 2022). [36]

Microsoft (2017), *The need for a Digital Geneva Convention*, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/. [46]

Naciones Unidas (2019), *The Age of Digital Interdependence*, https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf. [48]

Netcraft (2022), *Web Server Survey*, https://news.netcraft.com/archives/category/web-server-survey/ (accessed on 17 October 2022). [1]

OCDE (2022), "Dark Commercial Patterns Online", *OECD Digital Economy Papers,* No. 336, https://doi.org/10.1787/44f5e846-en. [29]

OCDE (2022), *Global Blockchain Policy Centre*, https://www.oecd.org/daf/blockchain/. [57]

OCDE (2022), *International collaboration to end tax avoidance*, https://www.oecd.org/tax/beps/. [58]

OCDE (2022), *OECD Global Forum on Competition*, https://www.oecd.org/competition/globalforum/. [59]

OCDE (2022), *OECD Global Forum on Digital Security for Prosperity*, https://www.oecd.org/digital/global-forum-digital-security/about/. [60]

OCDE (2022), *OECD Handbook on Competition Policy in the Digital Age*, https://www.oecd.org/daf/competition/oecd-handbook-on-competition-policy-in-the-digital-age.pdf. [21]

OCDE (2022), "The Evolving Concept of Market Power in the Digital Economy", *OECD Competition Policy Roundtable Background Note*, https://www.oecd.org/daf/competition/the-evolving-concept-of-market-power-in-the-digital-economy-2022.pdf. [27]

OCDE (2022), "The OECD Going Digital Measurement Roadmap", *OECD Digital Economy Papers*, No. 328, OECD Publishing, Paris, https://doi.org/10.1787/bd10100f-en. [56]

OCDE (2022), "The role of online marketplaces in protecting and empowering consumers: Country and business survey findings", *OECD Digital Economy Papers*, No. 329, OECD Publishing, Paris, https://doi.org/10.1787/9d8cc586-en. [6]

OCDE (2021), *Communique on Product Safety Pledges*, https://one.oecd.org/document/DSTI/CP/CPS(2021)8/FINAL/en/pdf. [30]

OCDE (2021), "Encouraging vulnerability treatment: Overview for policy makers", *OECD Digital Economy Papers*, No. 307, OECD Publishing, Paris. [19]

OCDE (2021), "Ex Ante Regulation and Competition in Digital Markets", *OECD Competition Committee Discussion Paper*, https://www.oecd.org/daf/competition/ex-ante-regulation-and-competition-in-digital-markets-2021.pdf. [28]

OCDE (2021), *Recommendation of the Council on Enhancing Access to and Sharing of Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463 (accessed on 21 April 2022). [11]

OCDE (2021), "Smart Policies for Smart Products: A Policy Maker's Guide to Enhancing the Digital Security of Products", *STI Policy Note*, OECD Publishing, Paris, https://www.oecd.org/digital/smart-policies-for-smart-products.pdf (accessed on 11 July 2022). [38]

OCDE (2021), *Strengthening Economic Resilience Following the COVID-19 Crisis: A Firm and Industry Perspective*, OECD Publishing, Paris, https://doi.org/10.1787/2a7081d8-en. [23]

OCDE (2021), "Understanding the digital security of products: An in-depth analysis", *OECD Digital Economy Papers*, No. 305, OECD Publishing, Paris. [18]

OCDE (2020), "Going Digital integrated policy framework", *OECD Digital Economy Papers*, No. 292, OECD Publishing, Paris, https://doi.org/10.1787/dc930adc-en. [53]

OCDE (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris, https://doi.org/10.1787/53e5f593-en. [7]

OCDE (2019), *Recommendation of the Council on Artificial Intelligence*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [51]

OCDE (2019), *Unpacking E-commerce: Business Models, Trends and Policies*, OECD Publishing, Paris, https://doi.org/10.1787/23561431-en. [8]

OCDE (2016), "Digital Convergence and Beyond: Innovation, Investment and Competition in Communication Policy and Regulation for the 21st Century", *OECD Digital Economy Papers*, No. 251, OECD Publishing, Paris, https://doi.org/10.1787/5jlwvzzj5wvl-en. [3]

OCDE (2016), *Recommendation of the Council on Consumer Protection in E-commerce*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422. [9]

OCDE (2016), *Recommendation of the Council on Consumer Protection in E-commerce*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422. [52]

OCDE (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [12]

OCDE (de próxima publicación), "Data shaping firms and markets", *OECD Digital Economy Papers*, OECD Publishing, Paris. [5]

OCDE (de próxima publicación), "Fostering cross-border data flows with trust", *OECD Digital Economy Papers*, OECD Publishing, Paris. [10]

OCDE (forthcoming), "Measuring the value of data and data flows", *OECD Digital Economy Papers*, OECD Publishing, Paris. [55]

OCDE (de próxima publicación), *Policy Framework on Digital Security*, OECD Publishing, Paris. [17]

OCDE (de próxima publicación), *Recommendation on Digital Security Risk Management*, OECD. [13]

OCDE (de próxima publicación), *Recommendation on National Digital Security Strategies*, OECD. [14]

OCDE (de próxima publicación), *Recommendation on the Digital Security of Products and Services*, OECD. [15]

OCDE (de próxima publicación), *Recommendation on the Treatment of Digital Security Vulnerabilities*, OCDE. [16]

OCDE-OMC-FMI (2020), *Handbook on Measuring Digital Trade*, https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade-Version-1.pdf. [54]

Rockefeller Foundation (2021), *A Bretton Woods for AI: Ensuring Benefits for Everyone*, https://www.rockefellerfoundation.org/blog/a-bretton-woods-for-ai-ensuring-benefits-for-everyone/;. [41]

Statista (2022), *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030*, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed on 11 July 2022). [35]

Tett, G. (2019), *Do we need an IMF to regulate the internet?*, https://www.ft.com/content/4526982e-60a0-11e9-b285-3acd5d43599e (accessed on 20 February 2022). [44]

UNCTAD (2021), *Digital Economy Report 2021*, https://unctad.org/page/digital-economy-report-2021. [49]

Notas

[1] Los compromisos por la seguridad de los productos implican que las plataformas se comprometan a realizar acciones que van más allá de sus obligaciones legales para proteger a los consumidores de los productos inseguros (por ejemplo, la retirada del mercado de productos inseguros en un plazo determinado tras la notificación de una autoridad gubernamental). El Grupo de Trabajo sobre Seguridad en los Productos de Consumo de la OCDE ha publicado recientemente un comunicado instando a los gobiernos a que desarrollen más compromisos de este tipo y a que los mercados incorporen cuatro compromisos para fomentar la coherencia a nivel internacional (OCDE, 2021[30]).