OECD publishing

LAS PERSONAS PRIMERO EN LA TRANSFORMACIÓN DIGITAL

DOCUMENTO DE REFERENCIA PARA LA CONFERENCIA MINISTERIAL DEL CDEP

OECD DIGITAL ECONOMY PAPERS
Noviembre de 2022 **No. 339**

OCDE
MEJORES POLÍTICAS PARA UNA VIDA MEJOR

Prólogo

Este documento analiza la forma en que la transformación digital nos afecta como individuos, ya sea en condición de ciudadanos, consumidores o trabajadores. Esboza el panorama de políticas públicas y describe los esfuerzos internacionales de múltiples partes interesadas y repletos de matices que se necesitan para alcanzar un equilibrio entre los diferentes derechos, intereses y valores en juego.

Este documento proporciona información de referencia para sustentar los debates sobre el Tema 3 de la Conferencia ministerial del Comité de Política de la Economía Digital: *Las personas primero*, 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 «Derechos en la era digital - construyendo evidencias sólidas (*workshop*)», «Creando un entorno en línea más seguro (*workshop*)» y «Empoderando a los consumidores en el entorno digital».

Este documento ha sido redactado por Nora Beauvais, Giuseppe Bianco, Kosuke Kizawa, Nicholas McSpedden-Brown y Lisa Robinson, bajo la supervisión de Audrey Plonk, jefa de la División de Políticas de Economía Digital de la OCDE. Ha contado con las aportaciones de Brigitte Acoca, Gallia Daor, Clarisse Girot, Molly Lesher, Adam Mollerup, Vincenzo Spiezia, Verena Weber y Jeremy West, así como de Angela Gosmann, Sebastian Ordelheide y Misha Pinkhasov, que han prestado apoyo editorial. Tanto la Conferencia ministerial como los trabajos conexos han contado con el generoso respaldo del Gobierno de España.

Este documento 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)13/FINAL

Índice

Gráficos

Recuadros

Resumen ejecutivo

La transformación digital ofrece numerosas oportunidades sociales y económicas a las personas, ya sea en su condición de ciudadanos, consumidores o trabajadores. Las tecnologías digitales han transformado la vida de miles de millones de personas, ofreciéndoles nuevos espacios y herramientas para comunicarse, trabajar, consumir, participar en la economía y el debate público, y ejercer sus derechos y disfrutar de sus libertades. La creación de un entorno en línea seguro y que dé mayor poder a los usuarios es fundamental a la hora de dar prioridad a las personas en el proceso de transformación digital.

Las tecnologías digitales ofrecen a los consumidores productos y servicios a medida, facilidad de acceso a plataformas de mercadeo en línea, mayor variedad de opciones y precios competitivos, y hogares conectados. No obstante, también exponen a las personas al riesgo de ser víctimas de estafas y fraudes en línea, comprar productos inseguros o ser engañadas, explotadas o discriminadas.

A los trabajadores, estas tecnologías les permiten acceder a nuevas y más flexibles oportunidades laborales, al trabajo mediado por plataformas y a distintas herramientas prácticas. Sin embargo, es cierto que por otro lado estos pueden verse expuestos a condiciones de trabajo difíciles, una gestión descentralizada o a sesgos algorítmicos.

Para las personas en general, las tecnologías digitales abren numerosas posibilidades de establecer relaciones, relajarse, formarse o interactuar con la administración. Sin embargo, las personas pueden toparse en línea con contenidos ilegales y perjudiciales, ver violada su intimidad, sufrir discriminación o algún tipo de desigualdad o salir perjudicadas por fallos de seguridad.

El panorama de políticas públicas del sector digital requiere esfuerzos internacionales en los que participen las múltiples partes interesadas y que reflejen una gran variedad de matices de modo que sea posible lograr un equilibrio entre todos los derechos, intereses y valores en juego. Los responsables de la formulación de estas políticas y las autoridades encargadas de velar por el cumplimiento de la ley cada vez se enfocan más en la protección, el empoderamiento, la seguridad y la salvaguarda de los derechos, pero necesitan herramientas que respalden sus esfuerzos. Tanto para los unos como para los otros, las normas no vinculantes (*soft law*) resultan esenciales a la hora de complementar su respectiva tarea de regular y de velar por el cumplimiento de la ley, y estas pueden consistir en compromisos voluntarios, normas éticas, enfoques de diseño, medidas técnicas y campañas de educación y concienciación. Las políticas públicas y las leyes deben reflejar las interdependencias del entorno digital y basarse en datos empíricos para subsanar las deficiencias de las políticas y proponer respuestas adecuadas.

«Las personas primero» es más que un eslogan o una mera aspiración: refleja los objetivos fundamentales de la era digital.

Las personas primero en la transformación digital: Documento de referencia para la Conferencia ministerial del CDEP

Las tecnologías digitales se entrelazan con la vida de las personas...

La transformación digital ofrece diversos beneficios sociales para ciudadanos, consumidores y trabajadores. Los avances tecnológicos y los nuevos modelos de negocio han reestructurado la vida cotidiana de miles de millones de personas, creando nuevas esferas públicas y nuevos mercados de bienes y servicios. Actividades como chatear, compartir contenidos, comprar en línea, utilizar objetos conectados y pagar con dispositivos inteligentes ofrecen nuevas posibilidades para que las personas se comuniquen, trabajen, consuman, se formen, creen, participen en la democracia y la economía, y ejerzan y gocen de sus derechos en la era digital.

¿Qué significa esto en la práctica? Tomemos el caso de la familia de Antonio, un maestro de escuela de 45 años que tiene dos hijos. Él y su pareja, Yoko, pueden comunicarse en línea con familiares y amigos de todo el mundo siempre que quieren. En su chat familiar comparten noticias, memes y vídeos de gatos, además de fotos de sus hijos y de las vacaciones. En opinión de Antonio, esto ayuda a mantener la familia unida, sobre todo porque sus padres viven muy lejos. Yoko, una entusiasta del medioambiente, también recurre a menudo a Internet para aprender cosas nuevas y disfruta debatiendo cuestiones medioambientales en las redes sociales, donde comparte artículos e ideas en distintas comunidades en línea. Hace no mucho, a través de uno de estos grupos, dio con antiguos amigos del instituto, con los que había perdido el contacto.

Antonio no es un ávido usuario de las redes sociales y no siempre entiende el atractivo de los videoblogs, tuits o *streams*. Sin embargo, los teléfonos inteligentes le facilitan la tarea de controlar lo que hacen sus hijos, Tom, de 14 años, y Ana, de 11, que sí utilizan las redes sociales, a pesar de que en un principio Antonio y Yoko eran reticentes a que Ana tuviera una cuenta siendo tan pequeña. Los niños parecen pasar horas pegados a sus pantallas, según Antonio, demasiadas. Tom pasa gran parte de su tiempo jugando a videojuegos con amigos que ha hecho en línea, algunos de los cuales no conoce en persona. También le encanta dibujar cómics en su tableta. En cuanto a Ana, ve dibujos animados o chatea con sus amigos en las redes sociales; o ambas cosas a la vez. Antonio afirma que sus hijos han progresado mucho

en francés gracias a una nueva aplicación interactiva. ¡Tienen acceso a infinidad de recursos educativos, conocimientos e información! Durante el confinamiento, como muchos profesores, Antonio utilizó plataformas de aprendizaje electrónico, que le servían para conocer mejor las necesidades de aprendizaje de sus alumnos. Uno de ellos no tenía acceso a Internet en casa, y Antonio, sus compañeros y algunos alumnos recaudaron dinero para que el niño pudiera disponer de una tableta con conexión de datos.

La transformación digital también ha aportado a la familia oportunidades de empleo flexible. El hermano de Yoko, Ken, conducía para un servicio de transporte compartido y ganar así un dinero extra mientras estudiaba en la universidad. Esto permitió a Ken, que es padre soltero, elegir cuándo y dónde trabajar en función de sus horarios de clase. Después de la universidad, Ken siguió trabajando como conductor de vez en cuando para tener más ingresos. Ken conducía para múltiples plataformas y, aunque desconocía la tecnología que había detrás, podía pedir que sus valoraciones en una plataforma se transfirieran a otra («portabilidad de datos de reputación»), lo que implicaba que no se sentía constreñido a quedarse en una única plataforma por miedo a perder su alta valoración.

Ken es una de las muchas personas que podrían haber tenido dificultades para llegar a fin de mes, pero que han encontrado una oportunidad de obtener ingresos a través del trabajo mediado por plataformas, que se define como «cualquier actividad productiva realizada por personas para producir bienes o prestar servicios llevada a cabo a través de o en una plataforma digital» (OCDE, 2022[1]). Puede tratarse del trabajo principal de un trabajador o de un trabajo secundario ocasional para complementar los ingresos (por ejemplo, en el caso de estudiantes, o personas que han perdido recientemente su empleo o que acaban de jubilarse).

...pero las personas pueden ser vulnerable a sus inconvenientes.

No obstante, la situación distaba mucho de ser perfecta. Era responsabilidad de Ken mantener su coche y asegurarse de que tenía la formación necesaria para su licencia. Cuando llegó el COVID-19, empezó a preocuparse por su salud porque tenía contacto con mucha gente y, si enfermaba, no podría trabajar y, en consecuencia, no cobraría. A Ken también le resultaba difícil prever con qué ingresos podía contar. Nunca sabía cuánto iba a ganar, y a veces un pasajero rechazaba o discutía un pago, con lo que perdía dinero. En una ocasión, una plataforma desactivó su cuenta sin previo aviso y sin que Ken supiera la razón. Las plataformas no contaban con un mecanismo sencillo de resolución de conflictos y Ken sentía que no estaba en una situación de poder como para plantear este tipo de cuestiones.

Tras estar varios días de baja por enfermedad al contagiarse del COVID-19, Ken vio cómo su posición en la clasificación disminuía ligeramente. Los sistemas algorítmicos que impulsan el trabajo mediado por plataformas pueden ser propensos a la discriminación y los prejuicios. Se han registrado otros casos similares: en 2020, un algoritmo de clasificación de reputación utilizado por una plataforma de entrega de comida a domicilio en Italia penalizó a los trabajadores ausentes por motivos irrelevantes o legítimos (por ejemplo, huelgas o bajas por enfermedad). Por lo tanto, se consideró que había ingrido la legislación italiana (Tribunal de Bolonia, 2020[2]).

Las tecnologías digitales empoderan a los ciudadanos...

Las tecnologías y los datos digitales transforman la relación de los ciudadanos con el gobierno, dotándoles de nuevos medios que los empoderan para participar en la democracia y la sociedad civil. El gobierno digital favorece la apertura y la participación pública para que los ciudadanos se involucren en el diseño, el desarrollo, la aplicación y el seguimiento de las políticas y los servicios públicos. En consonancia con esto, los países están adoptando un

enfoque «*mobile-first*» en relación con el gobierno digital. Las tecnologías digitales también están transformando el funcionamiento de los procesos e instituciones democráticos, creando nuevas oportunidades (por ejemplo, el voto y el recuento por medios electrónicos), al tiempo que plantean desafíos en términos de privacidad, igualdad y seguridad. Para solucionar estos problemas, los gobiernos suelen trabajar con socios del sector privado en medidas dirigidas a fomentar la confianza.

Para Antonio y Yoko, la firma y el DNI electrónicos suponen un ahorro de tiempo considerable. Su hijo Tom utiliza las tecnologías digitales para cultivar su identidad cívica y participar en cuestiones políticas. Él y muchos de sus amigos forman parte de un grupo juvenil en línea de acción medioambiental. Esta es una de las muchas maneras en que la transformación digital facilita la participación cívica de los niños, amplifica sus voces y les permite defender sus derechos e intereses, individual y colectivamente. Al mismo tiempo, la concentración de información sobre las actividades de los ciudadanos en un sistema centralizado puede dar lugar a otro tipo de riesgos como la intrusión injustificada (ICO, 2021[3]).

... y posibilitan la oferta de servicios comerciales a medida...

Antonio se sirve del comercio en línea para poner a la venta en una plataforma de mercadeo en línea las mesas de madera que él mismo restaura. También realiza la mayor parte de sus compras por Internet, siguiendo la tendencia al alza (acelerada por la pandemia del COVID-19) de los consumidores de los países de la OCDE a comprar por Internet: el 64% en 2020, frente a un 36% en 2010. Tras introducir determinadas palabras clave en motores de búsqueda ajustados algorítmicamente en su *smartphone*, compara decenas de ofertas de una amplia gama de productos, a menudo en plataformas de mercadeo en línea, donde lee detalladas reseñas de consumidores. Las herramientas digitales de comparación, los anuncios personalizados y las recomendaciones le ayudan a determinar lo que necesita. A veces recomienda ciertos productos a su hermana menor, María, que está en silla de ruedas, y a la que este sistema le permite comprar y recibir productos de forma totalmente independiente con solo mover un dedo. Realizan estas transacciones fácilmente, utilizando la banca y los pagos digitales. Antonio recuerda haberse sentido afortunado de tener fácil acceso al mercado en línea global durante el confinamiento por el COVID-19, una temporada en la que compró aún más en línea, ya que era consciente de que algunas personas carecían de esta posibilidad.

Cuando Yoko llega a casa después del trabajo, habla con su asistente digital, dotado de inteligencia artificial (IA), que enciende la calefacción y las luces conectadas a Internet, transmite música por toda la casa, le informa del tiempo que hará mañana y puede incluso hacer una reserva en un restaurante para cenar. Con los datos que recoge y gracias a las continuas actualizaciones a distancia, aprendió a adaptar el consumo energético del hogar a las necesidades específicas de la familia. También les sugiere ofertas personalizadas, al igual que otra aplicación basada en los datos de sus transacciones.

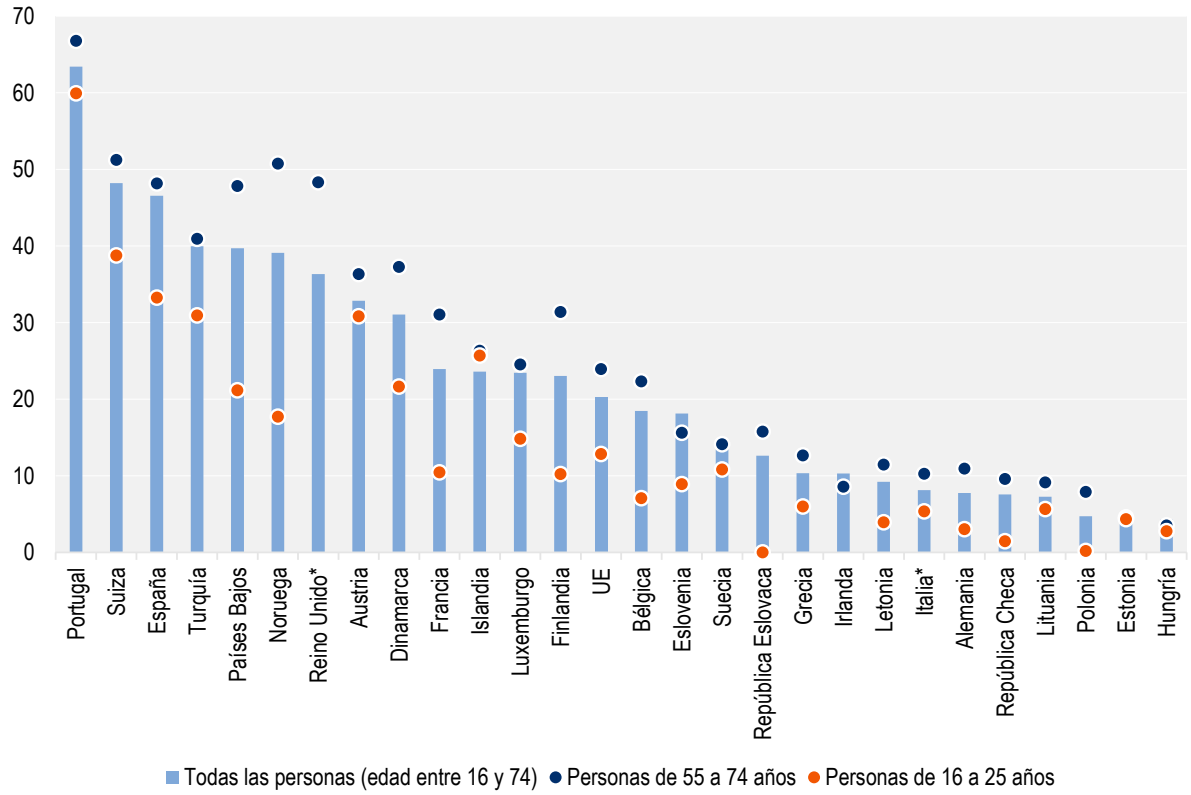
...pero son muchas las preocupaciones sobre las prácticas comerciales en línea.

Sin embargo, no todas sus experiencias con el comercio electrónico y los productos de consumo digital han sido positivas, ya que la familia también ha tenido malas experiencias en línea. Durante la crisis del COVID-19, Antonio compró un desinfectante de manos a un minorista en línea que parecía auténtico pero el pedido nunca llegó: resultó ser un sitio web falso que utilizaba reseñas generadas mediante IA y logotipos robados para parecer legítimo. Yoko encargó unas mascarillas que resultaron ser defectuosas y que podrían haber herido a los niños. También le llegó información sobre iniciativas benéficas para ayudar a las víctimas del virus, que resultaron ser falsas, y se enteró de los riesgos derivados del *phishing* y del fraude financiero en línea. Estas experiencias llevaron a Antonio y a Yoko a ser más cautelosos a la

hora de comprar en línea y compartir su información financiera y personal. Las estadísticas de la OCDE muestran que el 22,5% de los usuarios de Internet no compran en línea por motivos de seguridad en el pago y preocupaciones en cuanto a la privacidad (Gráfico 1) (OCDE, s.f.[4]).

Gráfico 1. Porcentaje de usuarios de Internet que no compran en línea por motivos de seguridad en el pago

% de usuarios de Internet que no han hecho compras en línea en los últimos 3 meses



Nota: Los usuarios de Internet que no han encargado bienes o servicios por Internet en los últimos 3 meses incluyen a los que nunca han hecho compras en línea. Los datos más recientes se refieren a un periodo de recuerdo de 3 meses antes de ser encuestados, aunque algunos países utilizan periodos diferentes y los periodos de recuerdo pueden variar con el tiempo. En 2021, Eurostat modificó el periodo de recuerdo, que pasó de ser el de los 12 meses anteriores a la encuesta, al de los 3 meses anteriores. Para obtener más información sobre las definiciones, la calidad de los datos, las rupturas de las series, etc., visite la(s) fuente(s) de datos subyacentes.
Fuente: *OECD Going Digital Toolkit*, basado en la Base de datos completa de estadísticas sobre sociedad y economía digital de Eurostat

El comercio electrónico plantea una amplia gama de preocupaciones a las personas. Una encuesta de la OCDE realizada en 2021 en 13 países mostró que el 50% de los consumidores en línea se enfrentaron a, al menos, un problema relacionado con el comercio electrónico en los 12 meses anteriores a la encuesta. Considerando solo su problema más grave, alrededor del 25% estaba relacionado con la crisis del COVID-19 (en relación con la cual las estafas eran frecuentes) y el coste total para los consumidores en los países de la OCDE se estimó en más de 22.000 millones de USD en 2020 (OCDE, 2022[5]). Los datos preliminares de un barrido de seguridad de productos en línea realizado por la OCDE en

2021 en 21 jurisdicciones sugieren que las tasas medias de incumplimiento de las prohibiciones/retiradas de productos, los requisitos de etiquetado y las normas de seguridad no han mejorado desde el barrido realizado en 2015 para los productos de consumo de siete categorías (juguetes/juegos, productos eléctricos para el hogar, productos no eléctricos para el hogar, productos deportivos/recreativos, ropa, productos infantiles, tecnología portátil) (OCDE, de próxima publicación[6]; OCDE, 2016[7]).

Ciertas prácticas empresariales podrían socavar aún más la confianza...

Yoko se inscribió recientemente a un servicio en línea en que los niños aprenden a tocar instrumentos musicales. No estaba del todo satisfecha, pero le costó cancelarlo debido a una combinación de información oculta, preguntas engañosas, múltiples pasos de cancelación y un lenguaje emotivo que la acaba convenciendo para quedarse. Tras un breve periodo de prueba, se le facturó por defecto la suscripción de todo un año. Yoko había sido víctima de varios «patrones comerciales oscuros» (en adelante, simplemente «patrones oscuros»), es decir, prácticas comerciales que emplean elementos de la arquitectura de elección digital, en particular en las interfaces de usuario en línea, que subvierten o perjudican la autonomía, la toma de decisiones o la elección del consumidor. Al igual que muchos consumidores, Yoko desconocía lo habituales que son estas prácticas, aunque había oído hablar de la acción emprendida por la Comisión Federal de Comercio de EE. UU. (FTC, por sus siglas en inglés) contra un negocio en línea por la renovación automática de las suscripciones de los consumidores sin su consentimiento, que desembocó en el reembolso de 9,7 millones de USD a los consumidores afectados por la práctica en 2021 (FTC, 2021[8]).

En 2022, la OCDE descubrió que es frecuente encontrar patrones oscuros en sitios web de comercio electrónico, aplicaciones (incluidas las de las principales plataformas y mercados en línea), así como en los avisos de consentimiento de *cookies*, motores de búsqueda y juegos (OCDE, 2022[9]). Un estudio identificó al menos un patrón oscuro en el 95% de 240 aplicaciones populares (Di Geronimo et al., 2020[10]). A menudo estos patrones engañan, coaccionan o manipulan a los consumidores, y es probable que causen un perjuicio directo o indirecto al consumidor, si bien esto puede ser difícil o imposible de medir. Hay pruebas de su eficacia a la hora de influir en la toma de decisiones de los consumidores y de los posibles perjuicios en términos de pérdidas económicas, daños a la intimidad, perjuicios psicológicos, debilitamiento o distorsión de la competencia y pérdida de confianza de los consumidores. Algunos consumidores, como los de menor nivel educativo, los de bajos ingresos o los niños, podrían verse perjudicados de forma desproporcionada.

Consciente de la experiencia de Yoko, a Antonio le preocupa que sus hijos puedan ser víctimas de estos patrones oscuros. Se ha fijado en que cada vez es más común que Tom utilice su paga para comprar elementos aleatorios en videojuegos (cajas de recompensa), que parecen utilizar el mismo diseño engañoso y las mismas técnicas de marketing agresivas de las que fue víctima Yoko. Alrededor del 60% de los principales juegos de Google Play y Apple Store contienen cajas de recompensa (Zendle et al., 2020[11]) y el 44% de los jóvenes de entre 11 y 16 años del Reino Unido que las conocían habían gastado

dinero en ellas alguna vez (Gambling Commission, 2019[12]). También es preocupante que los niños parecen no identificar la publicidad y los anuncios en los juegos y las redes sociales (OCDE, 2021[13]).

...lo que hace que la gente desconfíe de la interacción en línea en general.

De vez en cuando, Antonio piensa en la huella de datos que deja la constante presencia en línea de su familia. Reconoce que no sabe realmente para qué se utilizan, en última instancia, esos datos, sobre todo porque ningún miembro de la familia lee nunca los avisos de consentimiento de *cookies*, las condiciones de servicio o las políticas de privacidad, considerando que son demasiado largos y a menudo sintiendo que deben aceptarlos de todos modos. El hecho de que los niños sean menos conscientes del valor que sus datos pueden tener para las empresas podría, de hecho, ponerlos en mayor riesgo de que se vulneren sus derechos de privacidad.

En ocasiones, a Antonio le preocupa si el hecho de tener tantos datos personales expuestos a la elaboración de perfiles algorítmicos por parte de las empresas podría hacerlos más vulnerables a la explotación o la discriminación, aunque no está seguro de que sus temores sean fundados. ¿Y si las empresas pudieran determinar sus estados emocionales individuales, sus prejuicios o sus problemas de salud en momentos clave y dirigirse a ellos con anuncios manipuladores o con la intención de hacerles pagar más que a los demás? ¿Podrían los algoritmos que aprenden con datos históricos replicar o exacerbar la marginación que experimenta su hermana, María, como persona con discapacidad? Antonio también ha escuchado que los algoritmos y la IA pueden tener un impacto desproporcionado en las personas por motivos raciales o étnicos y otras características protegidas.

Las interacciones sociales en línea también pueden suponer un peligro...

La transformación digital ha permitido una difusión más rápida, barata y amplia de los contenidos perjudiciales. En el colegio, hace apenas unas semanas, el hijo de Antonio y Yoko, Tom, asistió a un curso de prevención del ciberacoso. Aprendió que las tecnologías digitales facilitan la propagación y amplificación del ciberacoso, y que este suele estar asociado a altos niveles de estrés, dificultades sociales, depresión, ansiedad, autolesiones y suicidio. Otros tipos de contenidos perjudiciales, como la propaganda y la desinformación, pueden suponer una amenaza para la democracia, con implicaciones de enorme alcance. La familia de Antonio aún recuerda el escándalo que se produjo cuando una empresa de consultoría política recabó y vendió los datos de 50 millones de usuarios de una red social sin su consentimiento con el objetivo de influir en los votantes (ICO, 2018[14]). Los términos «cámaras de eco» y «burbujas de filtrado» se han adoptado para describir las comunidades en línea de personas con ideas afines, en los que la exposición a puntos de vista diferentes es muy limitada. En ocasiones, estas comunidades, potenciadas por el uso de algoritmos, pueden contribuir a la proliferación de información falsa y engañosa, al aislamiento intelectual, a la exacerbación de los prejuicios y a la polarización de determinadas posturas ideológicas. Esta tendencia es extensible a los contenidos ilegales. Por ejemplo, Yoko recuerda haber escuchado a menudo en las noticias que algunos autores de atentados terroristas se habían radicalizado en línea o habían transmitido el ataque en directo.

A pesar de que sabía que no le estaba permitido, Ana, la hija de 11 años de Antonio y Yoko, instaló en su teléfono una aplicación de redes sociales que utilizaban todos sus compañeros de clase. El verano pasado, recibió una invitación a través de esa aplicación de un desconocido para chatear. Como tenían amigos en común, ella aceptó y empezaron a chatear, pero de repente él le envió varias fotos violentas y pornográficas. También empezó a pedirle que le enviara fotos de ella. Ana lo bloqueó de inmediato, pero estaba demasiado asustada y conmocionada para contarle a sus padres lo que había pasado. No obstante, ellos se dieron cuenta de que algo iba mal porque se la veía muy angustiada.

Los delitos de explotación y abuso sexual infantil (CSEA, por sus siglas en inglés) perpetrados en línea están aumentando a un ritmo espeluznante. Las víctimas son predominantemente niñas, aunque también los niños se ven afectados, y tienen, en su mayoría, entre 3 y 13 años, aunque las imágenes a menudo muestran a bebés de entre 0 y 2 años. También se ha observado un aumento de la «sextorsión», en la que los depredadores exigen favores sexuales, dinero u otras cosas a un niño bajo la amenaza de compartir su contenido autogenerado (WeProtect Global Alliance, 2021[15]).

...pero las medidas de protección conllevan sus propios riesgos.

A raíz de lo ocurrido, Yoko investigó y descubrió que las tecnologías digitales y los algoritmos existentes y emergentes pueden detectar y tomar medidas correctivas contra los contenidos y las prácticas abusivas o ilegales. Algunos ejemplos son las herramientas para detectar y eliminar contenidos terroristas y extremistas violentos en línea utilizando bases de datos o herramientas compartidas entre empresas, o que identifican automáticamente las prácticas comerciales perjudiciales en línea. Sin embargo, la investigación de Yoko también le enseñó que la detección algorítmica de contenidos mediante el uso de la IA puede tener sus propias limitaciones y problemas, dado que tales herramientas pueden ser inexactas, estar sesgadas, ser discriminatorias por diseño, y podrían facilitar la censura y la vigilancia masiva por parte de las empresas (FTC, 2022[16]) o incluso de los gobiernos.

Las tecnologías de vigilancia masiva pueden comprometer la libertad de expresión y la privacidad, pero también la seguridad física y, en última instancia, el derecho a la vida. De hecho, en algunos países, el uso de tecnologías de vigilancia se ha relacionado con detenciones, intimidaciones y asesinatos de periodistas y activistas de derechos humanos. También pueden provocar miedo y llevar a la gente (incluidos periodistas, defensores y activistas) a autocensurarse, amenazando así la libertad de expresión y la capacidad de la gente para acceder a la información. Las tecnologías de vigilancia pueden agravar aún más el impacto físico y psicológico de la violencia de género y de pareja.

Yoko leyó en las noticias que la Comisión Federal de Comercio de EE. UU. había tomados medidas contra una empresa dedicada a la venta de aplicaciones de *stalkerware*, que pueden instalarse subrepticiamente en los dispositivos y utilizarse para controlar las fotos, los mensajes de texto, los historiales web, las ubicaciones GPS y otra información personal sin que el propietario del dispositivo lo sepa (FTC, 2021[17]).

Las políticas deben priorizar a las personas

Antonio, Yoko, Tom, Ana, Ken y María son personajes ficticios, pero los desafíos descritos son una realidad para millones de personas en todo el mundo. Dada la gran cantidad de ventajas y riesgos que conlleva el entorno digital, es esencial que, a la hora de formular las políticas digitales, se priorice el bienestar económico, la seguridad psicológica y física, y el bienestar de las personas. Esto no supone defender un enfoque puramente proteccionista, sino uno que responda a la doble prioridad de la protección y la capacitación, y que maximice las ventajas al tiempo que mitiga los riesgos. Si bien es

necesario adoptar más medidas en este sentido, cabe destacar que la OCDE lleva mucho tiempo a la vanguardia de estas cuestiones (Recuadro 1).

Recuadro 1. Labor de la OCDE para contribuir a que se priorice a las personas en la transformación digital

Privacidad

- Directrices de la OCDE sobre privacidad
- Recomendación sobre la cooperación transfronteriza en la aplicación de las leyes de protección de la intimidad

Niños en la esfera digital

- Recomendación de la OCDE sobre protección de los niños en la esfera digital
- Directrices para los proveedores de servicios digitales

Informes de transparencia

- Informes de análisis comparativo 2020 2021 y 2022
- Marco para la presentación voluntaria de informes de transparencia (VTRF, por sus siglas en inglés)

Consumidores

- Directrices de la OCDE para la protección de los consumidores de prácticas comerciales transfronterizas fraudulentas y engañosas
- Recomendación sobre protección al consumidor en el comercio electrónico
- Recomendación sobre seguridad de los productos de consumo

Políticas que exigen un esfuerzo multilateral y repleto de matices

Salvaguardar el bienestar de las personas en su papel de ciudadanos, trabajadores y consumidores, y garantizar la protección y el respeto de sus derechos, requiere enfoques políticos coordinados y basados en datos empíricos.

Los desafíos que plantea la lucha contra los efectos perjudiciales de los contenidos falsos y/o engañosos —como la información errónea, la desinformación, la propaganda, el engaño contextual y la sátira—, que circulan amplia y rápidamente en línea, ilustran esta complejidad. Esto hace que el equilibrio con la libertad de expresión y el acceso a una información fiable sobre determinados desafíos globales, como el cambio climático, pueda resultar complicado en la era digital. Cuando los gobiernos o las empresas se extralimitan en sus esfuerzos por eliminar contenidos perjudiciales o engañosos, corren el riesgo de restringir indebidamente la libertad de expresión. El derecho a la libertad de expresión y a una prensa libre e independiente son indispensables para el buen funcionamiento de las sociedades democráticas (OCDE, 2022[18]). No obstante, hay que buscar cuidadosamente el justo equilibrio entre la libertad de expresión y otros derechos, como el de la salud y la intimidad.

La privacidad y la protección de datos suelen estar en el centro de los debates sobre la búsqueda de un equilibrio entre los derechos e intereses en conflicto. ¿Cómo pueden los consumidores aprovechar las ventajas de la publicidad y los contenidos personalizados sin comprometer la protección de sus datos? El cifrado de extremo a extremo suele considerarse esencial para proteger la privacidad, pero en la lucha contra la CSEA, por ejemplo, puede considerarse que proporciona a los delincuentes un terreno en el que actuar con impunidad. Resolver este dilema requiere la colaboración de los responsables de la formulación de políticas, la sociedad civil, los expertos en tecnología y privacidad, las fuerzas del orden y los especialistas en protección de la infancia.

También puede ser necesario reflexionar de forma más crítica sobre cómo defendemos ciertos derechos. Por ejemplo, cada vez se cuestiona más la idea todavía generalizada de que los datos anonimizados o «desidentificados» no tienen implicaciones para la privacidad. La desidentificación puede evitar que se conozca la identidad de un individuo y proteger su privacidad, pero no protege contra la atribución de

rasgos o características de grupos a los que este pueda pertenecer. Esto plantea cuestiones relativas a los derechos colectivos de los grupos (como los pueblos indígenas), incluida su capacidad de autodeterminación y de afirmar la soberanía sobre sus datos para hacer frente a la discriminación sistemática (OCDE, 2022[19]). Se ha argumentado que ha de haber más transparencia en este sentido y que las personas deben tener un mayor conocimiento respecto a lo que se hace con sus datos personales una vez estos se han desidentificado, además de disponer de la información necesaria para evaluar si ese uso se adecúa a sus valores (FNIGC, s.f.[20]). Las soluciones de transparencia son, en su mayoría, insuficientes por sí solas, y sus ventajas para los individuos tienen, a menudo, un alcance limitado, dado el tiempo y la complejidad que implica el seguimiento de cómo se ha utilizado su información personal a través de diferentes tecnologías.

Es importante que los responsables de la formulación de políticas se aseguren de evitar consecuencias perjudiciales no deseadas, por ejemplo, crear nuevos problemas sociales al regular los existentes. Las respuestas legales al *sexting* son un buen ejemplo de esta cuestión. Los menores que practican *sexting* pueden autogenerar material que se clasifica legalmente como «CSEA», y muchos niños han sido objeto de una respuesta de la justicia penal, llegando incluso a ser procesados o inscritos en un registro obligatorio de delitos sexuales contra menores, lo que puede acarrearles repercusiones negativas de por vida. La Recomendación de la OCDE sobre protección de los niños en la esfera digital trata de solucionar esta cuestión, recomendando que las medidas para proteger a los niños en la esfera digital sean proporcionadas, no excesivamente punitivas y si procede sean, ante todo, de carácter educativo y terapéutico (OCDE, 2021[21]).

La protección y el empoderamiento de los consumidores, la seguridad y los derechos: elementos centrales que han de inspirar la elaboración de políticas y la aplicación de la ley

Lo cierto es que ya existen leyes para combatir muchos de estos riesgos emergentes. Un gran número de jurisdicciones cuentan con leyes de privacidad y protección de datos que reflejan normas internacionales comunes, como las Directrices sobre privacidad de la OCDE, que establecen una serie de principios básicos para proteger la privacidad. En muchas jurisdicciones, las leyes de consumo, que reflejan los principios clave de la Recomendación de la OCDE de 2016 sobre la protección al consumidor en el comercio electrónico (OCDE, 2016[22]) y la Recomendación de la OCDE de 2020 sobre seguridad de los productos de consumo (OCDE, 2020[23]), establecen disposiciones que prohíben las prácticas comerciales engañosas, fraudulentas, injustas y otras prácticas abusivas, así como la comercialización de productos inseguros (OCDE, de próxima publicación[24]; OCDE, 2022[9]). Muchas legislaciones brindan una protección especial a determinados consumidores vulnerables, como los niños (OCDE, de próxima publicación[24]). En consecuencia, las autoridades de protección de los consumidores y de protección de datos pueden dar respuesta (y, de hecho, lo hacen) a muchas de estas preocupaciones. Asimismo, numerosos países siguen la Recomendación de la OCDE sobre los Principios de alto nivel para la protección del consumidor financiero (OCDE, 2012[25])para establecer o mejorar sus marcos de protección en este ámbito y abordar el impacto, las oportunidades y los riesgos de la digitalización.

Sin embargo, existe un consenso sobre la necesidad de una aplicación más exhaustiva de la normativa vigente y sobre el hecho de que, en muchos casos, esta resulta insuficiente. Esto se debe, en parte, a que el entorno digital es muy diferente del físico, dado que se caracteriza por la ubicuidad, una gran rapidez y amplitud y la ausencia de fronteras. Además, los datos y los contenidos pueden replicarse sin coste alguno o a bajo coste y compartirse o utilizarse en algoritmos.

Hasta hace poco, muchos ámbitos del entorno digital dependían de la autorregulación de entidades privadas que a menudo se amparaban en exenciones de responsabilidad. En los foros internacionales de alto nivel y entre los responsables de la formulación de políticas se plantea cada vez más la cuestión de

cómo proteger el bienestar económico, la privacidad, la seguridad y el bienestar social de todos en la transformación digital, aplicando o proponiendo nuevas normativas.

Los responsables de la formulación de políticas subrayan el papel de las empresas y plataformas en línea a la hora de ofrecer soluciones a los daños ocasionados en línea. Esto se reconoce tanto en la OCDE, como a nivel del G7 y el G20.[1] A menudo, estos llamamientos insisten en la responsabilidad compartida y en que es necesario adoptar un enfoque que contemple la participación de las múltiples partes interesadas. Por ejemplo, la Recomendación de la OCDE sobre protección al consumidor en el comercio electrónico hace hincapié en la responsabilidad compartida que recae sobre las empresas a la hora de promover el bienestar de los consumidores y aumentar su confianza, pidiéndoles que presten la debida atención a los intereses de los consumidores (OCDE, 2016[22]).

Al mismo tiempo, los responsables políticos proponen imponer obligaciones a las empresas en línea — en particular a las plataformas, incluidas las de mercadeo en línea— para proteger a los consumidores y prohibir las prácticas abusivas. Varias leyes recientes o propuestas de ley persiguen prohibir los patrones oscuros, limitar la publicidad dirigida o imponer obligaciones a las plataformas de mercadeo en línea para atajar la venta de productos inseguros. Algunas propuestas legislativas tratan de abordar las prácticas abusivas o los productos de consumo dañinos que incorporan IA, como la prohibición de las técnicas subliminales o las que explotan las vulnerabilidades para alterar el comportamiento (OCDE, 2022[9]);[2] mientras que otras medidas buscan capacitar a los consumidores para que tomen decisiones en línea más informadas, entre otras cosas, mediante una difusión más eficaz de la información (OCDE, 2022[26]).

Se ha prestado especial atención a las normas de transparencia y rendición de cuentas de las plataformas en línea, especialmente de las más grandes. Cada vez son más las jurisdicciones que imponen requisitos de transparencia a las plataformas en línea, incluidos los relativos a las políticas y acciones de moderación de contenidos, y las sanciones por incumplimiento. Los requisitos incluyen informes sobre los métodos de identificación (por ejemplo, revisión humana, tecnologías automatizadas, notificaciones de seguridad) y los métodos de actuación (por ejemplo, eliminación o bloqueo de contenidos, etiquetas de advertencia, suspensión o eliminación de la cuenta), así como sobre los mecanismos de reclamación, resolución de conflictos y evaluación de riesgos. Muchas de estas medidas se integran en leyes que pretenden abordar la seguridad en línea con carácter más general.[3] Estas últimas se centran con demasiada frecuencia en las actividades de las plataformas en línea y establecen requisitos para facilitar la denuncia de contenidos ilícitos o perjudiciales, de modo que estos sean eliminados, e imponen sanciones en caso de que no se respeten esos requisitos. Lo mismo ocurre con el uso de datos personales. Una investigación de la Comisión Australiana de la Competencia y del Consumidor constató que en las plataformas digitales existía falta de transparencia y que los consumidores no contaban con opciones informadas sobre la recopilación y el uso de los datos, así como la necesidad de reforzar la protección en la legislación sobre privacidad (ACCC, 2019[27]).

Dos cuestiones destacadas son la violencia de género y combatir los perjuicios que sufren los menores de modo que muchas propuestas prevén medidas específicas contra la violencia de género o de pareja,[4] o la desprotección de los niños. Entre las medidas de protección de los menores está la propuesta de Reglamento de la UE por el que se establecen normas para prevenir y combatir el abuso sexual de los menores (Comisión Europea, 2022[28]) o que exigen que se aplique la privacidad por diseño adecuada a la edad de los niños.

También se está prestando especial atención a los intereses de los trabajadores en línea. Según la OCDE, los gobiernos deben garantizar que todos los trabajadores tengan acceso a los derechos y medidas de protección pertinentes, independientemente de su situación laboral o tipo de contrato, y deben garantizar la igualdad de condiciones impidiendo que algunas empresas obtengan una ventaja competitiva injusta (OCDE, 2019[29]). La propuesta de Directiva de la UE relativa a la mejora de las condiciones laborales en el trabajo en plataformas digitales establece protecciones que pasan por considerar a la plataforma como empleador (en lugar de considerar a los trabajadores como autónomos). Esto proporcionará a los

trabajadores beneficios como permisos retribuidos, derechos de pensión y requisitos de salario mínimo (Comisión Europea, 2022[30]). Los responsables de la formulación de políticas y los reguladores de la privacidad están prestando atención a la portabilidad de los datos, que puede ayudar a los trabajadores autónomos a mantener sus datos de reputación en todas las plataformas.

Estas cuestiones se examinan cada vez más en el contexto de los derechos. ¿Cambia la transformación digital las expectativas de cómo los gobiernos defienden y protegen los derechos? ¿Complican las tecnologías digitales el equilibrio de los derechos en conflicto? Mientras que algunos países se centran en derechos individuales específicos, como la protección de los datos personales o el acceso a Internet (Conseil d'État, 2016[31]) otros consideran la cuestión de forma más global, llevando a cabo iniciativas amplias para proteger los derechos en la era digital y garantizar una transformación digital centrada en el ser humano. En 2021, el gobierno español adoptó la Carta de Derechos Digitales (Gobierno de España, 2021[32]); en 2022, la Comisión Europea propuso una Declaración de principios y derechos digitales para consagrarlos en la transformación digital (Comisión Europea, 2022[33]); y Corea pretende aprobar una Carta de Derechos Digitales en 2023 (Ministry of Science and ICT, Republic of Korea, 2022[34]).

Algunas jurisdicciones están explorando nuevos derechos en ámbitos específicos, como la transparencia algorítmica y la rendición de cuentas en la toma de decisiones de la IA, mientras que otras priorizan la protección de los derechos en línea y fuera de línea de la misma manera. En cuanto a los menores, se puede afirmar que, a nivel internacional, la cuestión de la defensa de sus derechos en línea está bastante avanzada. En 2018, el Consejo de Europa elaboró unas Directrices para respetar, proteger y cumplir los derechos del niño en el entorno digital (Consejo de Europa, 2018[35]); y en 2021, el Comité de los Derechos del Niño emitió una Observación General relativa a los derechos de los niños en relación con el entorno digital (CDN, 2021[36]). En cuanto a la responsabilidad de las empresas a la hora de respetar los derechos en el entorno digital, el Proyecto B-Tech de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos ofrece orientación y recursos para aplicar los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos en el espacio tecnológico (ACNUDH, s.f.[37]).

Leyes y políticas interoperables y problemas asociados

Los responsables de la formulación de políticas y los reguladores deben tener en cuenta que el entorno digital se extiende más allá de las fronteras tradicionales y tiene importantes interdependencias. Abundan los ejemplos de respuestas políticas fragmentarias. La responsabilidad de satisfacer las necesidades de los niños en línea suele dejarse en manos de los ministerios que se ocupan del asunto fuera de línea (OCDE, 2020[38]), si bien muchos problemas, como el *sexting* y el ciberacoso, requieren una respuesta coordinada de los ministerios de justicia, sanidad y educación (como mínimo), y la consideración de las repercusiones en el derecho a la intimidad de los niños. Del mismo modo, la fragmentación de las respuestas en cuestiones de transparencia, presentación de informes y rendición de cuentas para hacer frente a los contenidos violentos y extremistas puede resultar gravosa e ineficiente. Las empresas multinacionales podrían tener que emitir varias versiones de los informes de transparencia, los gobiernos podrían replicar individualmente los costes legislativos y las partes interesadas probablemente tendrían que buscar los informes en diferentes lugares. Para solucionar esto, en mayo de 2022, la OCDE lanzó el Marco para la presentación voluntaria de informes de transparencia (OCDE, 2022[39]), un portal web internacional estandarizado que está a disposición de cualquier servicio de intercambio de contenidos en línea, independientemente de su tamaño o modelo de negocio.

A menudo, la misma cuestión afecta a varios ámbitos políticos simultáneamente, lo que hace necesaria la cooperación regulatoria. Los patrones oscuros, las prácticas de personalización abusivas y el sesgo algorítmico pueden afectar negativamente a los consumidores, la privacidad, la competencia, la inteligencia artificial y las políticas antidiscriminatorias. La ubicuidad de los datos en todos los sectores económicos y sociales implica que las leyes de privacidad y protección de datos deban interoperar con las autoridades de los sectores regulados como competencia y consumo (OCDE, 2022[40]), que se ocupan

de cuestiones diferentes. Mientras que las autoridades encargadas de velar por la privacidad podrían evaluar las repercusiones de la concentración económica en la protección de datos, las autoridades de competencia deben abordar si la presencia de información personal o las preocupaciones por la privacidad modifican los análisis de la competitividad. Es importante entender hasta qué punto pueden cooperar las autoridades y cómo pueden interoperar sus ecosistemas regulatorios. Varios países cuentan con foros para mejorar la cooperación entre los reguladores digitales, incluidos los de consumo, privacidad, competencia y comunicaciones.

En lugar de respuestas aisladas y descoordinadas, gobiernos y reguladores han de desarrollar enfoques integrales en consulta con la sociedad civil y las empresas, fomentar las sinergias y la cooperación entre diferentes ámbitos políticos, evitar el solapamiento de esfuerzos y determinar el mejor mecanismo para abordar los problemas. La Recomendación de la OCDE sobre gobernanza regulatoria ágil para aprovechar la innovación insta a los gobiernos a sentar unas bases institucionales que permitan la cooperación y los enfoques conjuntos dentro y entre jurisdicciones (OCDE, 2021[41]). Además, la coherencia de las políticas puede ayudar a los países de la OCDE a alcanzar los Objetivos de Desarrollo Sostenible, que son multidimensionales y abarcan muchas áreas políticas relevantes de cara a poner a las personas al frente de la transformación digital.

La cooperación transfronteriza es vital porque los riesgos en línea, como las prácticas engañosas y fraudulentas, las amenazas a la privacidad y los productos inseguros son problemas de carácter transnacional. No obstante, sigue habiendo importantes desafíos. Los organismos encargados de hacer cumplir la ley a menudo carecen de la autoridad necesaria para cooperar plenamente o pueden enfrentarse a problemas prácticos a la hora de trabajar con sus homólogos extranjeros. En 2021, la OCDE publicó unas orientaciones para la adopción de medidas legislativas con el fin de dotar a las autoridades de consumo de poderes y herramientas para hacer cumplir las leyes de protección de los consumidores a escala nacional y cooperar a nivel transfronterizo (OCDE, 2021[42]). La nueva Recomendación de la OCDE sobre la cooperación regulatoria internacional para hacer frente a los desafíos mundiales ayuda a los gobiernos y a los organismos reguladores a transformar los procesos de gobernanza y de elaboración de normas —que se centran en el ámbito interno— para aprovechar las ventajas de la cooperación internacional (OCDE, 2022[43]).

Esfuerzos regulatorios con una sólida base empírica

Establecer prioridades políticas que maximicen la protección y mejoren las oportunidades requiere contar con datos empíricos sólidos, actualizados y fiables para entender en qué aspectos las políticas funcionan bien y en cuáles no. En lo que respecta a varios desafíos, como los que afrontan la familia de Yoko y Antonio, esa base empírica sigue adoleciendo de importantes lagunas.

Los patrones oscuros constituyen uno de los ámbitos en que hace falta mejorar la base empírica para respaldar las políticas públicas y la aplicación de la ley. Esto incluye la necesidad de comprender los efectos de ciertos patrones oscuros en la toma de decisiones de los consumidores y la magnitud de los daños a los consumidores. A menudo, no es solo que sea necesario hacer más pruebas o mejorar las que ya se hacen, sino que lo óptimo sería realizar diferentes tipos de pruebas. Según la Recomendación de la OCDE de 2016 sobre protección al consumidor en el comercio electrónico, la incorporación de enfoques conductuales es fundamental para reforzar la base empírica en que se sustenta la elaboración de políticas de consumo, incluso mediante investigaciones empíricas como la experimentación.

La base empírica que ha respaldado las políticas públicas en materia de privacidad también ha sido desigual. Las autoridades encargadas de velar por la privacidad recopilan una cantidad considerable de datos que se hacen públicos a través de informes anuales, pero no siempre revisten un formato idóneo que permita la comparación internacional. Una fuente habitual de preocupación son las crecientes brechas entre las leyes de privacidad y protección de datos a nivel mundial, a pesar de la alineación general con los principios de protección de datos de las Directrices de la OCDE sobre privacidad. Estas brechas

pueden deberse a diferencias en la aplicación práctica de los principios o a que normas similares se basan en fundamentos diferentes. Sin embargo, a medida que la tecnología evoluciona, que los datos se vuelven más ubicuos y que más países adoptan leyes de privacidad, se necesitan más pruebas empíricas para identificar estas brechas y evaluar si las soluciones siguen teniendo vigencia.

Asimismo, existen importantes carencias de datos empíricos necesarios para proteger y empoderar a los niños en línea. La elaboración de políticas públicas dirigidas a los menores en el entorno digital tiene a menudo carácter reactivo (se legisla, por ejemplo, ante incidentes de gran repercusión) o se basa en datos parciales en lugar de basarse en datos fiables y representativos. Por ejemplo, aunque es común escuchar que el exceso de «tiempo de pantalla» es perjudicial para la salud y el bienestar de los niños, la base empírica que respalda tales preocupaciones es débil. La preocupación por el tiempo frente a la pantalla también pasa por alto que los menores no son un grupo homogéneo, y que las vulnerabilidades en línea están influidas por sus vulnerabilidades fuera de la red (por ejemplo, el género o el entorno socioeconómico). Además, el tiempo frente a la pantalla no presenta un riesgo uniforme y no siempre es perjudicial, ya que depende de las actividades que los niños realicen en línea. El caso de un adolescente con riesgo de padecer un trastorno alimentario expuesto a imágenes corporales poco realistas en línea es muy diferente al de otro que encuentra una comunidad de apoyo en línea en un tema que le preocupa. Se necesitan estudios exhaustivos, de calidad y a gran escala sobre los efectos del entorno digital en la salud y el bienestar de los menores, que tengan en cuenta la multitud de actividades diferentes que realizan los niños en el entorno digital, así como la evolución de sus capacidades y vulnerabilidades (OCDE, 2022[44]).

La *OECD Going Digital Measurement Roadmap* revisada, que señala que los sistemas estadísticos nacionales deben adaptarse y ampliarse para reflejar la digitalización de las economías y las sociedades, puede ayudar a los responsables de la formulación de políticas a construir su base de datos y a alinear las prioridades de sus países para medir la transformación digital utilizando metodologías y enfoques comunes (OCDE, 2022[45]).

Medidas no vinculantes (soft law) para complementar la regulación y la aplicación de la normativa

Las leyes, los reglamentos y las medidas de aplicación de la ley requieren de acciones complementarias para avanzar en materia de seguridad digital y proteger y empoderar a las personas en el entorno digital. Las iniciativas empresariales podrían contemplar compromisos por parte de las plataformas de mercadeo en línea para reducir el suministro de productos inseguros (OCDE, 2021[46]) o normas éticas para que las empresas promuevan un diseño de interfaz de usuario respetuoso con el consumidor. Esto podría ayudar a las empresas a mejorar su reputación y reforzar la confianza de los usuarios. Asimismo, las acciones voluntarias de las empresas desempeñan un papel importante en la mitigación de los riesgos, por ejemplo en materia de seguridad de la información. Entre ellas se encuentran las acciones y mecanismos para evitar accesos no autorizados, daños o intromisiones; las políticas de seguridad de la información, y la evaluación de riesgos.

Las iniciativas que integran estos aspectos por diseño ofrecen estrategias prometedoras. Algunas son bien conocidas, como la privacidad por diseño y la seguridad por diseño, mediante las que se articulan principios y factores de referencia que deben considerarse en la fase de diseño de un servicio o producto y que se incorporan a su funcionamiento (OCDE, 2020[47]). La seguridad digital por diseño es más reciente, pero está ganando terreno como objetivo político, y en los últimos años han surgido varias propuestas de definición. Algunos gobiernos y organizaciones internacionales de la sociedad civil subrayan que implica situar las consideraciones de seguridad del usuario en el centro del desarrollo de servicios y productos; así, en lugar de aplicar remedios de forma reactiva, la seguridad por diseño minimiza las amenazas anticipando, detectando y evitando los daños antes de que se produzcan (eSafety, s.f.[48]).

Las medidas técnicas también pueden ser útiles para mitigar los riesgos. Un ejemplo de este tipo de herramientas son los rastreadores web basados en IA que permiten a las autoridades de consumo detectar y combatir patrones oscuros o productos inseguros en línea. En 2022, la Comisión Europea puso en marcha una herramienta electrónica de vigilancia para ayudar a las autoridades nacionales a detectar la oferta en línea de productos inseguros sobre los que se alerta en Safety Gate, el sistema de alerta rápida de la UE para productos peligrosos no alimentarios (Comisión Europea, 2022[49]). Otras herramientas permiten a las empresas autoauditar su arquitectura de elección en línea y a los consumidores protegerse de los patrones oscuros, como los complementos del navegador que comunican automáticamente a la empresa las decisiones de privacidad de los consumidores sin necesidad de responder a un aviso de consentimiento de *cookies*.

Las medidas educativas y de concienciación orientan a los ciudadanos y consumidores hacia la información, o les ayudan a evitar los daños en línea o a presentar reclamaciones. La orientación puede ser específica para determinados grupos, como las campañas de consumo centradas en los niños o los consumidores con menos habilidades digitales (OCDE, de próxima publicación[24]). La educación digital en general es clave para proteger y empoderar a las personas en el entorno digital. Muchos países de la OCDE tienen una estrategia de educación digital o integran esta materia en una estrategia global de innovación digital. A menudo, las iniciativas de alfabetización digital se dirigen a los menores, lo cual es esencial, pero también deberían enfocarse hacia públicos más amplios, por ejemplo para mejorar las decisiones financieras de los consumidores (OCDE, 2020[50]), mejorar o reciclar la cualificación de los trabajadores, impartir conocimientos digitales a las personas mayores, o ayudar a los padres, cuidadores y profesores (y a las administraciones locales y autoridades educativas) a comprender mejor las tecnologías de modo que estos puedan orientar a los niños. Es importante que haya un acceso equitativo a los programas de alfabetización digital, especialmente en lo que respecta a los menores. Se observa que las diferencias sociales y culturales crean desajustes en las competencias digitales, lo que puede exacerbar ciertos riesgos. Por ejemplo, un mayor nivel de conocimientos digitales por parte del ciberacosador puede crear el desequilibrio de poder inherente a muchas formas de acoso.

Sin embargo, aunque estas iniciativas y herramientas desempeñan un papel importante, es probable que por sí solas resulten insuficientes y que deban entenderse como un complemento de las medidas regulatorias y de aplicación de la normativa que sean sólidas.

Conclusión: Mantenerse a la vanguardia

Por un lado, la familia de Yoko y Antonio se beneficia de la transformación digital, en su condición de ciudadanos, consumidores y trabajadores. Las experiencias de los consumidores han mejorado, la interacción social y la inclusión se han ampliado, la relación entre los ciudadanos y el gobierno se ha transformado y el potencial de los trabajadores se ha incrementado. Por otro lado, existen importantes riesgos relacionados con las nuevas formas de malas prácticas comerciales en línea; los contenidos perjudiciales e ilegales; las amenazas a la privacidad, la protección de los datos personales y la libertad de expresión; y la discriminación y el sesgo algorítmico.

Los rápidos avances y la amplia aceptación de las nuevas tecnologías sugieren que la magnitud y la naturaleza de la vulnerabilidad en la era digital están cambiando rápidamente. Algunas personas siguen siendo desproporcionadamente vulnerables, especialmente los grupos desfavorecidos, marginados, minoritarios e infrarrepresentados. Pero en el entorno digital actual, la mayoría de los individuos, si no todos, pueden ser vulnerables en diferentes momentos y contextos. En el ámbito del consumo, varios expertos han llamado a que se revise la forma de entender la vulnerabilidad del consumidor para que sea algo universal o sistémico (OCDE, de próxima publicación[24]).

Determinadas tendencias tecnológicas, como la creciente omnipresencia de la IA y la Internet de las cosas, van a mantenerse. Irán acompañadas de tendencias emergentes como las tecnologías inmersivas

(por ejemplo, la realidad aumentada y virtual). Estas novedades requerirán enfoques rápidos e innovadores para garantizar la seguridad y los derechos de las generaciones venideras.

La Conferencia ministerial del CDEP es una oportunidad para que los responsables políticos de alto nivel consideren si es necesario —y cómo— adaptar las medidas y los conceptos; cómo lograr una transformación digital centrada en las personas, y cómo alcanzar los objetivos mutuos. Precisamente en este sentido, los derechos en la era digital adquieren una mayor relevancia: ¿Cómo se aplican nuestros derechos tradicionales al mundo digital? ¿Esta nueva realidad impulsa la necesidad de articular derechos específicos del mundo digital? Al adaptar estas medidas, las políticas públicas deben ir más allá y aspirar a empoderar a todos los miembros de la sociedad, en especial a los más susceptibles de sufrir daños. La OCDE, en calidad de foro de debate, realiza investigaciones y presta asesoramiento sobre políticas públicas en relación con todas estas cuestiones.

Notas

[1] Véanse, por ejemplo: los Principios de alto nivel del G20 sobre empoderamiento y protección de la infancia de 2021; los Principios del G7 sobre seguridad en Internet de 2021; los Principios del G7 para hacer frente a la violencia en línea contra mujeres y niñas y un plan de acción para combatir la explotación y el abuso sexual de los niños de 2021; la iniciativa del Christchurch Call de 2019, y la Declaración de Osaka de los líderes del G20 para prevenir el uso de Internet con fines terroristas y de extremismo violento que puede conducir al terrorismo (VECT, por sus siglas en inglés) de 2019.

[2] Véase, por ejemplo, la Propuesta de Ley de Inteligencia Artificial de la Comisión Europea.

[3] Véanse, por ejemplo: En Australia, la *Online Safety Act* (Ley de Seguridad en Línea); en Canadá la *legislative and regulatory proposal to confront harmful content online* (Propuesta legislativa y reglamentaria para hacer frente a los contenidos perjudiciales en línea); en la Unión Europea, la; en Alemania, la *Netzwerkdurchsetzungsgesetz* (Ley para mejorar la aplicación de la ley en las redes sociales); en Irlanda, la *Online Safety and Media Regulation Bill* (proyecto de Ley de regulación de la seguridad y los medios de comunicación en línea); en Nueva Zelanda, la *Films, Video and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill* [Proyecto de Ley de enmienda de la clasificación de películas, vídeos y publicaciones (clasificación provisional urgente de publicaciones y prevención de daños en línea)]; en el Reino Unido, la *Online Safety Bill* (Proyecto de Ley de seguridad en línea) o, en Estados Unidos, la *Platform Accountability and Consumer Transparency Act, (Ley de responsabilidad de la plataforma y transparencia del consumidor; también conocida como «PACT ACT»).*

[4] Por ejemplo, la propuesta de Directiva de la UE sobre la lucha contra la violencia contra las mujeres y la violencia doméstica regula específicamente la violencia en línea, y la Ley de Seguridad en Línea de Australia contempla disposiciones específicas relacionadas con el abuso basado en la imagen.

Referencias

ACCC (2019), *Digital Platforms Inquiry Final Report*, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf (accessed on 24 October 2022). [27]

ACNUDH (s.f.), *B-Tech Project OHCHR and business and human rights*, https://www.ohchr.org/en/business-and-human-rights/b-tech-project (accessed on 24 October 2022). [37]

CDN (2021), *General Comment no. 25 on Children's Rights in Relation to the Digital Environment*, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation (accessed on 24 October 2022). [36]

Comisión Europea (2022), *Declaration on European Digital Rights and Principles*, https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles (accessed on 24 October 2022). [33]

Comisión Europea (2022), *EU proposes directive to protect the rights of platform workers*, https://ec.europa.eu/eures/public/eu-proposes-directive-protect-rights-platform-workers-2022-03-17_en (accessed on 24 October 2022). [30]

Comisión Europea (2022), *Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472 (accessed on 24 October 2022). [28]

Comisión Europea (2022), *Safety Gate: Motor vehicles and toys top the list of dangerous non-food products this year*, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_1343 (accessed on 24 October 2022). [49]

Conseil d'État (2016), *Fundamental rights in the Digital Age*, https://www.conseil-etat.fr/en/Media/actualites/documents/reprise-_contenus/rapports-et-etudes/fundamental-rights-in-the-digital-age.pdf (accessed on 24 October 2022). [31]

Consejo de Europa (2018), *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*, https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a (accessed on 24 October 2022). [35]

Di Geronimo, L. et al. (2020), *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, Association for Computing Machinery, New York, NY, USA, https://doi.org/10.1145/3313831.3376600. [10]

eSafety (s.f.), *Safety by Design*, https://www.esafety.gov.au/about-us/safety-by-design (accessed on 24 October 2022). [48]

FNIGC (s.f.), *First Nations principles of ownership, control, access, and possession*, https://fnigc.ca/ocap-training/ (accessed on 24 October 2022). [20]

FTC (2022), *FTC Report Warns About Using Artificial Intelligence to Combat Online Problems*, https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems (accessed on 24 October 2022). [16]

FTC (2021), *Age of Learning, Inc. (ABCmouse)*, https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3186-age-learning-inc-abcmouse (accessed on 24 October 2022). [8]

FTC (2021), *FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data*, https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data (accessed on 24 October 2022). [17]

Gambling Commission (2019), *Young People and Gambling 2019*, https://www.gamblingcommission.gov.uk/statistics-and-research/publication/young-people-and-gambling-2019 (accessed on 24 October 2022). [12]

Gobierno de España (2021), *Carta de Derechos Digitales*, https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/Charter%20of%20Digital%20Rights.pdf (accessed on 24 October 2022). [32]

ICO (2021), *The Information Commissioner's position paper on the UK Government's proposal for a trusted digital identity system*, https://ico.org.uk/media/about-the-ico/documents/2619686/ico-digital-identity-position-paper-20210422.pdf (accessed on 24 October 2022). [3]

ICO (2018), *Investigation into the use of data analytics in political campaigns*, https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf (accessed on 24 October 2022). [14]

Ministry of Science and ICT, Republic of Korea (2022), *대한민국 디지털 전략 발표, [Korea Digital Strategy Announcement]*, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&pageIndex=3&bbsSeqNo=94&nttSeqNo=3182193&searchOpt=ALL&searchTxt= (accessed on 24 October 2022). [34]

OCDE (2022), *Companion Document to the OECD Recommendation on Children in the Digital Environment*, OECD Publishing, París, https://doi.org/10.1787/a2ebec7c-en. [44]

OCDE (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, París, https://doi.org/10.1787/44f5e846-en. [9]

OCDE (2022), "Enhancing online disclosure effectiveness", *OECD Digital Economy Papers*, No. 335, OECD Publishing, París, https://doi.org/10.1787/6d7ea79c-en. [26]

OCDE (2022), *Expert Workshop on Data Ethics: Balancing Ethical and Innovative Uses of Data (internal document)*, OCDE, https://one.oecd.org/document/DSTI/CDEP/DGP(2022)1/en/pdf. [19]

OCDE (2022), *Measuring Digital Platform Employment and Work (internal document)*, https://one.oecd.org/document/WISE/CSSP(2022)4/en/pdf. [1]

OCDE (2022), "Measuring Financial Consumer Detriment in E-Commerce", *OECD Digital Economy Papers*, No. 326, OECD Publishing, ParÍs, https://doi.org/10.1787/4055c40e-en. [5]

OCDE (2022), *Mis- and dis-information: What governments can do to reinforce democracy (internal* [18]

document), https://one.oecd.org/document/GOV/PGC(2022)8/REV1/en/pdf.

OCDE (2022), *Recommendation of the Council on International Regulatory Co-operation to Tackle Global Challenges*, OCDE, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0475. [43]

OCDE (2022), *Review of the 2007 OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (internal document)*, https://one.oecd.org/document/DSTI/CDEP/DGP(2022)2/en/pdf. [40]

OCDE (2022), "The OECD Going Digital Measurement Roadmap", *OECD Digital Economy Papers*, No. 328, OECD Publishing, París, https://doi.org/10.1787/bd10100f-en. [45]

OCDE (2022), *VTRF web portal*, https://www.oecd-vtrf-pilot.org/. [39]

OCDE (2021), "Children in the digital environment: Revised typology of risks", *OECD Digital Economy Papers*, No. 302, OECD Publishing, París, https://doi.org/10.1787/9b8f222e-en. [13]

OCDE (2021), *Communiqué on product safety pledges*, OCDE, https://www.oecd.org/digital/consumer/communique-product-safety-pledges.pdf. [46]

OCDE (2021), "Implementation toolkit on legislative actions for consumer protection enforcement co-operation", *OECD Digital Economy Papers*, No. 310, OECD Publishing, París, https://doi.org/10.1787/eddcdc57-en. [42]

OCDE (2021), *Recommendation of the Council for Agile Regulatory Governance to Harness Innovation*, OCDE, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464. [41]

OCDE (2021), *Recommendation of the Council on Children in the Digital Environment*, OCDE, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389. [21]

OCDE (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, París, https://doi.org/10.1787/bb167041-en. [47]

OCDE (2020), "Protecting children online: An overview of recent developments in legal frameworks and policies", *OECD Digital Economy Papers*, No. 295, OECD Publishing, París, https://doi.org/10.1787/9e0e49a9-en. [38]

OCDE (2020), *Recommendation of the Council on Consumer Product Safety*, OCDE, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0459. [23]

OCDE (2020), *Recommendation of the Council on Financial Literacy*, OCDE, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0461. [50]

OCDE (2019), *OECD Employment Outlook 2019: The Future of Work*, OECD Publishing, París, https://doi.org/10.1787/9ee00155-en. [29]

OCDE (2016), "Online Product Safety Sweep Results: Australian Competition and Consumer Commission", *OECD Digital Economy Papers*, No. 262, OECD Publishing, París, https://doi.org/10.1787/5jlnb5q64ktd-en. [7]

OCDE (2016), *Recommendation of the Council on Consumer Protection in E-Commerce*, OCDE, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422. [22]

OCDE (2012), *Recommendation of the Council on High-Level Principles on Financial Consumer* [25]

Protection, OCDE, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0394.

OCDE (de próxima publicación), "Consumer Vulnerability in the Digital Age", *OECD Digital Economy Papers*, OECD Publishing, París. [24]

OCDE (de próxima publicación), "OECD Online Product Safety Sweep: Summary Report", *OECD Digital Economy Papers*, OECD Publishing, París. [6]

OCDE (s.f.), *The OECD Going Digital Toolkit*, https://goingdigital.oecd.org/. [4]

Tribunal de Bolonia (2020), *Labour Section, decision of 31 December 2020*, https://www.ansa.it/emiliaromagna/notizie/2021/01/02/rider-cgilalgoritmo-discrimina-sentenza-tribunale-bologna_cc14c299-2c6b-411b-b677-496549ee3af1.html (accessed on 24 October 2022). [2]

WeProtect Global Alliance (2021), *Global Threat Assessment*, https://www.weprotect.org/global-threat-assessment-21/ (accessed on 24 October 2022). [15]

Zendle, D. et al. (2020), *The prevalence of loot boxes in mobile and desktop games*, Addiction, https://doi.org/10.1111/add.14973. [11]