

Bruselas, 10.12.2021  
COM(2021) 819 final

**INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL  
COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES**

**Protección de los derechos fundamentales en la era digital -**

**Informe anual de 2021 sobre la aplicación de la  
Carta de los Derechos Fundamentales de la UE**

## **Protección de los derechos fundamentales en la era digital –**

### **Informe anual de 2021 sobre la aplicación de la Carta de los Derechos Fundamentales de la UE**

## **Índice**

|                                                                                                                                                                        |           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Protección de los derechos fundamentales en la era digital – Informe anual de 2021 sobre la aplicación de la Carta de los Derechos Fundamentales de la UE .....</b> | <b>1</b>  |
| <b>1. Introducción .....</b>                                                                                                                                           | <b>2</b>  |
| <b>2. La ejecución de la nueva estrategia para reforzar la aplicación de la Carta de los Derechos Fundamentales en la UE .....</b>                                     | <b>3</b>  |
| <b>3. Hacer de la Carta la guía de la UE para la era digital.....</b>                                                                                                  | <b>8</b>  |
| <b>4. Abordar los retos que entraña la moderación del contenido en línea .....</b>                                                                                     | <b>9</b>  |
| <b>5. Salvaguardar los derechos fundamentales cuando se utiliza la IA.....</b>                                                                                         | <b>19</b> |
| <b>6. Abordar la brecha digital .....</b>                                                                                                                              | <b>24</b> |
| <b>7. Proteger a las personas que trabajan a través de plataformas .....</b>                                                                                           | <b>29</b> |
| <b>8. Supervisión de la vigilancia digital .....</b>                                                                                                                   | <b>32</b> |
| <b>9. Unir fuerzas para que la era digital sea una oportunidad para los derechos fundamentales .....</b>                                                               | <b>40</b> |

## 1. Introducción

La Carta de los Derechos Fundamentales de la Unión Europea<sup>1</sup> es un instrumento muy eficaz para proteger, promover y seguir reforzando los derechos de las personas en la Unión Europea. Los derechos fundamentales no solo protegen a las personas de injerencias indebidas tales como la censura o la vigilancia masiva, también las capacitan para que aprovechen plenamente sus derechos y oportunidades en la vida. Siempre es posible mejorar las condiciones y la medida en que las personas pueden disfrutar de sus derechos. La Carta puede orientar las actividades en el campo de la política en toda la UE. Cuanto más conozcan los ciudadanos los derechos consagrados en ella y la forma de invocarlos, más eficaces serán.

La pandemia de COVID-19 ha puesto a prueba la protección y las garantías de nuestros derechos y libertades fundamentales. Cualquier restricción de los derechos fundamentales debe ser necesaria y proporcional, tal y como exige la Carta de los Derechos Fundamentales de la UE, Derecho vinculante de la Unión que protege y promueve un amplio abanico de derechos vinculados a la dignidad humana, la libertad, la igualdad y la solidaridad, y todos los órganos jurisdiccionales nacionales aplicarla en los casos en que esté implementado el Derecho de la UE y sea pertinente para la sentencia definitiva.

Desde 2009, la Carta tiene el mismo carácter jurídico que los Tratados, el Derecho primario de la UE en el que se basa la legislación de la Unión. Las instituciones europeas deben cumplirla en todas sus acciones y los Estados miembros de la UE deben cumplirla cuando apliquen el Derecho de la UE.

### **¿Cuándo deben los Estados miembros cumplir la Carta?**

- A menudo, cuando los Estados miembros acuerdan en el Consejo y con el Parlamento Europeo la adopción de nueva legislación de la UE, es necesario hacer efectiva dicha legislación mediante medidas nacionales de aplicación de la misma.
- Cuando los Estados miembros adoptan o modifican leyes sobre una materia en la que el Derecho de la UE impone obligaciones concretas, sus leyes no pueden contravenir el Derecho de la UE, incluida la Carta, ya que dicha acción legislativa constituiría la aplicación del Derecho de la UE.
- Los programas de financiación de la UE están consagrados en la legislación de la Unión. Los Estados miembros deben asegurarse de que este dinero se gaste de conformidad con las normas recogidas en dicha legislación. Cuando aplican programas de financiación, están aplicando el Derecho de la UE.
- Cuando los Estados miembros adoptan o modifican leyes en un ámbito en el que la UE carece de competencia y en el que no existe Derecho de la UE, no lo están aplicando. En tales casos, no están obligados a cumplir la Carta. Sin embargo, muchos de los derechos fundamentales consagrados en la Carta se recogen al mismo tiempo en las constituciones y la jurisprudencia nacionales, así como en el Convenio Europeo de Derechos Humanos, del que son signatarios todos los Estados miembros de la Unión.

<sup>1</sup> [Carta de los Derechos Fundamentales de la Unión Europea](#), DO C 326, de 26.10.2012, p. 391.

Con el fin de mejorar el conocimiento de la Carta por parte de todos, la Comisión Europea publica desde 2010 informes sobre su aplicación. Esta edición es la primera en seguir el nuevo enfoque anunciado en **la estrategia para reforzar la aplicación de la Carta de los Derechos Fundamentales en la UE** (en adelante, «la estrategia para la aplicación de la Carta»)<sup>2</sup>. El informe anual se centrará en un tema concreto regido por el Derecho de la UE y analizará más a fondo las mejores prácticas y los retos existentes en los Estados miembros en dicho ámbito. Esto permite analizar avances sistémicos, ilustrar cómo pueden reforzarse los distintos derechos entre sí y cómo los avances políticos, sociales y económicos pueden afectar a varios derechos al mismo tiempo.

El tema de la edición de 2021 es la **protección de los derechos fundamentales en la era digital**, en consonancia con el enfoque estratégico de la Comisión Europea sobre la transición digital.

### **¿En qué información se basa este informe?**

Para la elaboración del presente informe se han utilizado los siguientes elementos:

- aportaciones de los Estados miembros, a quienes se invitó a proporcionar puntos de vista desde sus respectivas perspectivas nacionales<sup>3</sup>;
- una consulta específica con las organizaciones que agrupan a las organizaciones de la sociedad civil (OSC) europeas dedicadas al ámbito de los derechos fundamentales; así como
- informes de agencias de la UE, en particular los informes anuales de la Agencia de los Derechos Fundamentales de la Unión Europea (FRA)<sup>4</sup>, que contienen un apartado dedicado a los derechos fundamentales y la digitalización.

## **2. La ejecución de la nueva estrategia para reforzar la aplicación de la Carta de los Derechos Fundamentales en la UE**

Dicha estrategia, adoptada por la Comisión en 2020, tiene por objeto garantizar que la Carta se aplique plenamente, haciendo que los derechos fundamentales sean una realidad para todos. La estrategia para la aplicación de la Carta establece el marco para el trabajo conjunto en materia de derechos fundamentales en toda la UE durante los diez próximos años y goza del pleno respaldo de los Estados miembros<sup>5</sup>. La aplicación de los objetivos recogidos en la estrategia para la aplicación de la Carta se rige por las cuatro prioridades que siguen a continuación.

### **2.1 Respaldo y supervisar la aplicación efectiva de la Carta en los Estados miembros**

<sup>2</sup> Comunicación de la Comisión titulada «Estrategia para reforzar la aplicación de la Carta de los Derechos Fundamentales en la UE», [COM\(2020\)711](#).

<sup>3</sup> Los Estados miembros realizaron sus aportaciones en el marco del Grupo de Trabajo del Consejo «Derechos Fundamentales, Derechos de los Ciudadanos y Libre Circulación de Personas» («FREMP»).

<sup>4</sup> <https://fra.europa.eu/en/publication/2021/fundamental-rights-report-2021>.

<sup>5</sup> <https://data.consilium.europa.eu/doc/document/ST-6795-2021-INIT/es/pdf>.

Las administraciones nacionales y locales, los Parlamentos y las autoridades policiales son esenciales para promover y proteger los derechos conferidos por la Carta y crear un entorno propicio para las organizaciones de la sociedad civil y los defensores de los derechos. La Comisión colabora estrechamente con los Estados miembros para ayudarles a aplicar el Derecho y las políticas de la UE de forma eficaz y plenamente conforme con la Carta.

La Comisión también ayuda a los Estados miembros a aplicar **los programas financiados por la UE** de conformidad con la Carta. El Reglamento sobre disposiciones comunes<sup>6</sup> establece las normas que deben observarse para la utilización de varios fondos de la UE<sup>7</sup>. Obliga a los Estados miembros a crear y utilizar mecanismos efectivos para garantizar que los programas financiados por la UE cumplan la Carta, como disposiciones de presentación de informes al comité de seguimiento sobre las denuncias en relación con la Carta o los casos de incumplimiento de la Carta por operaciones apoyadas por los Fondos. La Comisión seguirá brindando asistencia técnica para ayudar a los Estados miembros a garantizar que los programas que reciban ayuda de los fondos de la UE sean diseñados y ejecutados de conformidad con la Carta.

En el marco de un plan de financiación específico, el Programa Ciudadanos, Igualdad, Derechos y Valores (CERV), la Comisión creó nuevas **oportunidades** de obtención de financiación **para las autoridades nacionales, regionales y locales**, para proyectos que promuevan una cultura de valores y refuercen el conocimiento de la Carta<sup>8</sup>. Las ciudades desempeñan un papel importante en el fomento de dicha cultura y en la protección de los derechos fundamentales. Son varias las ciudades que se han unido a una red de «ciudades de derechos humanos» e incorporan los derechos humanos en la formulación de sus políticas<sup>9</sup>. La FRA presentó un informe titulado *Human Rights in the EU: a framework for reinforcing rights locally* [«Los derechos humanos en la UE: un marco para reforzar los derechos a nivel local», documento en inglés] en su Foro de Derechos Fundamentales celebrado en octubre de 2021<sup>10</sup>. Dicho marco incluye herramientas para ayudar a alcaldes, gobiernos y administraciones locales, así como organizaciones de base, a integrar normas sobre derechos humanos en su trabajo. En noviembre de 2021, como seguimiento del Plan de Acción de la UE Antirracismo para 2020-2025<sup>11</sup>, la Comisión puso en marcha un «premio a la(s)

<sup>6</sup> Reglamento (UE) 2021/1060 del Parlamento Europeo y del Consejo, de 24 de junio de 2021, por el que se establecen las disposiciones comunes relativas al Fondo Europeo de Desarrollo Regional, al Fondo Social Europeo Plus, al Fondo de Cohesión, al Fondo de Transición Justa y al Fondo Europeo Marítimo, de Pesca y de Acuicultura, así como las normas financieras para dichos Fondos y para el Fondo de Asilo, Migración e Integración, el Fondo de Seguridad Interior y el Instrumento de Apoyo Financiero a la Gestión de Fronteras y la Política de Visados (DO L 231 de 30.6.2021, p. 159).

<sup>7</sup> Para el período 2021-2027 son los siguientes: el Fondo Europeo de Desarrollo Regional, el Fondo de Cohesión, el Fondo Social Europeo Plus, el Fondo de Transición Justa, el Fondo Europeo Marítimo, de Pesca y de Acuicultura, el Fondo de Asilo y Migración, el Fondo de Seguridad Interior y el Instrumento de Gestión de las Fronteras y Visados.

<sup>8</sup> <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/cerv>. Dentro de la [convocatoria de propuestas de hermanamiento de ciudades y redes de ciudades](#), el programa CERV va a poner 4,2 millones EUR a disposición en 2021. Puede obtenerse más información en el siguiente enlace: [Financiación y licitaciones \(europa.eu\)](#).

<sup>9</sup> <https://humanrightscities.net/>.

<sup>10</sup> <https://fra.europa.eu/en/publication/2021/human-rights-cities-framework>.

<sup>11</sup> Comunicación de la Comisión titulada «Una Unión de la igualdad: Plan de Acción de la UE Antirracismo para 2020-2025», [COM\(2020\) 565 final](#).

Capital(es) Europea(s) de la Inclusión y la Diversidad»<sup>12</sup>. Premiará a las mejores prácticas que puedan ser una fuente de inspiración para otras ciudades y regiones europeas con respecto a la creación de entornos más diversos e inclusivos para sus habitantes.

En la estrategia para la aplicación de la Carta, la Comisión invitaba a los Estados miembros a designar un **centro de referencia de la Carta** para facilitar la cooperación y el intercambio de información sobre su aplicación. Hasta el momento, diecisiete Estados miembros han designado este centro de referencia de la Carta. Su función es fundamental para difundir información y mejores prácticas sobre el conocimiento de la Carta y coordinar las actividades de creación de capacidad en el país. Su trabajo contribuye a la nueva página sobre las mejores prácticas de los Estados miembros en relación con la Carta, lanzada en el Portal Europeo de Justicia en Red en diciembre de 2021<sup>13</sup>.

La Comisión, como guardiana de los Tratados, ha adoptado medidas concretas para garantizar el respeto de los derechos consagrados en la Carta en los casos en los que la legislación nacional o las prácticas relacionadas con la aplicación del Derecho de la UE vulneran dichos derechos, por ejemplo, mediante la incoación de procedimientos de infracción. En particular, la Comisión actuó para garantizar el respeto de:

- la libertad de asociación de las organizaciones no gubernamentales y los derechos relativos a la protección de los datos personales de sus donantes;
- la libertad de cátedra;
- la libertad de expresión y el pluralismo de los medios de comunicación;
- la dignidad humana;
- el derecho al respeto de la vida privada;
- el derecho de todas las personas, también de las personas LGBTIQ, a no ser discriminadas por razón de sexo y orientación sexual.

La Comisión ha seguido de cerca las medidas de emergencia adoptadas en todos los Estados miembros durante la pandemia de COVID-19 y su repercusión, en especial en el Estado de Derecho, los derechos fundamentales y el cumplimiento con otras disposiciones del Derecho de la UE, como queda reflejado en el **Informe sobre el Estado de Derecho en 2021** y sus capítulos por países<sup>14</sup>.

## **2.2 Capacitar a las organizaciones de la sociedad civil, a los defensores de los derechos y a los profesionales de la Justicia**

Las organizaciones de la sociedad civil (OSC) y los organismos nacionales independientes de derechos humanos son socios clave de las instituciones de la UE y los Estados miembros en la promoción y la protección de los derechos fundamentales, la democracia y el Estado de Derecho. Son fundamentales para sensibilizar a las personas acerca de sus derechos y ayudarles a recibir una tutela judicial efectiva. Estas organizaciones deben poder trabajar en un entorno favorable, sin limitaciones normativas indebidas, obstáculos a la financiación o

<sup>12</sup> <https://eudiversity2022.eu/the-award/apply/>.

<sup>13</sup> [https://e-justice.europa.eu/37134/ES/member\\_states\\_best\\_practices\\_on\\_the\\_charter](https://e-justice.europa.eu/37134/ES/member_states_best_practices_on_the_charter).

<sup>14</sup> COM(2021) 700 final, disponible en el siguiente enlace: [https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2021-rule-law-report\\_en](https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2021-rule-law-report_en).

incluso campañas de desprestigio<sup>15</sup>, y también es necesario que puedan desarrollar su capacidad. Algunos Estados miembros todavía no cuentan con **instituciones nacionales de derechos humanos** plenamente operativas, que constituyen importantes vínculos entre el gobierno y la sociedad civil<sup>16</sup>. Se invita a los Estados miembros a crear dichas instituciones y a velar por que dispongan de los medios necesarios para trabajar con total independencia.

La Comisión está **vigilando de cerca la situación de las OSC** e informa sobre los avances relativos al marco para la sociedad civil en su informe anual sobre el Estado de Derecho. El Informe sobre el Estado de Derecho en 2021 indica que las OSC se vieron afectadas por la pandemia de COVID-19, no solo como consecuencia de las limitaciones a la libertad de circulación y asociación, sino también en lo que respecta a la financiación. De acuerdo con este informe, la participación de la sociedad civil en el diseño y la aplicación de las medidas relativas a la COVID-19 ha sido, en términos generales, limitada<sup>17</sup>. El Informe sobre el Estado de Derecho en 2020 identificó medidas que restringían la libertad de expresión de las OSC<sup>18</sup>. De hecho, los datos recopilados por la FRA<sup>19</sup> muestran que muchas OSC consideran que las medidas nacionales para hacer frente a la pandemia repercutieron negativamente en sus actividades a partir de marzo de 2020. Si bien comunicaron un aumento de la demanda, en su mayoría tuvieron dificultades para poder seguir prestando sus servicios. Entre los retos a los que se enfrentaron en la práctica figuran la suspensión de actividades, los efectos psicológicos en los miembros del personal y la reducción de la contribución laboral de los voluntarios.

La Comisión **apoya a los defensores de los derechos humanos y las OSC** con financiación específica, como una convocatoria de propuestas sobre la protección y la promoción de los valores de la UE, que está dirigida íntegramente a OSC pequeñas y de base y desembolsa 51 millones EUR durante el período 2021/22<sup>20</sup>. Se ha publicado una convocatoria específica por valor de 2 millones EUR para promover los litigios y el desarrollo de capacidades relacionados con la aplicación de la Carta<sup>21</sup>.

La Comisión también está promoviendo el desarrollo de capacidades y la **sensibilización sobre la Carta entre los jueces y otros profesionales del ámbito de la justicia**. En diciembre de 2020, la Comisión adoptó una nueva estrategia europea en materia de formación

<sup>15</sup> FRA, *Protecting the civic space* [«La protección del espacio cívico», documento en inglés], 2021, <https://fra.europa.eu/en/publication/2021/civic-space-challenges>.

<sup>16</sup> Véase la estrategia para la aplicación de la Carta, *op. cit.*, apartado 2 «Capacitar a las organizaciones de la sociedad civil, a los defensores de los derechos y a los profesionales de la Justicia». Véase el informe de la FRA *Instituciones nacionales de derechos humanos sólidas y eficaces. Retos, prácticas alentadoras y oportunidades*, disponible en: <https://fra.europa.eu/en/publication/2020/strong-effective-nhris>. Los capítulos por países del Informe sobre el Estado de Derecho 2021 notifican el estado de acreditación de las instituciones de derechos humanos nacionales: [https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2021-rule-law-report/2021-rule-law-report-communication-and-country-chapters\\_es](https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2021-rule-law-report/2021-rule-law-report-communication-and-country-chapters_es).

<sup>17</sup> Informe sobre el Estado de Derecho en 2021, p. 24.

<sup>18</sup> Informe sobre el Estado de Derecho en 2020, p. 16. [EUR-Lex - 52020SC0316/TXT - ES - EUR-Lex \(europa.eu\)](https://eur-lex.europa.eu/lexuris/ui/1/52020SC0316/TXT-ES).

<sup>19</sup> <https://fra.europa.eu/en/news/2021/findings-fra-consultation-covid-19-impact-civil-society>; FRA, *Protecting the civic space*, *op. cit.*, véase el apartado 1.3. La COVID-19 agrava los problemas a los que se enfrenta la sociedad civil, p. 16.

<sup>20</sup> [Programa de trabajo del CERV 2021/22](#).

<sup>21</sup> [Convocatoria de propuestas para promover el desarrollo de capacidades y la sensibilización sobre la Carta de los Derechos Fundamentales de la UE](#).

judicial para 2021-2024<sup>22</sup>, y en marzo de 2021, publicó una convocatoria de propuestas de apoyo a proyectos relacionados con la formación judicial que incluyan los derechos fundamentales como una de sus prioridades clave<sup>23</sup>. Se ejecutaron varios proyectos de formación judicial sobre la Carta, cofinanciados por la Comisión en el marco de su Programa «Justicia» 2014-2020<sup>24</sup>. Los profesionales de la justicia pueden acceder a material formativo judicial sobre derechos fundamentales a través de una plataforma puesta en funcionamiento en diciembre de 2020<sup>25</sup>.

### **2.3 Utilizar plenamente la Carta de los Derechos Fundamentales en la toma de decisiones de la UE**

Las instituciones, organismos, oficinas y agencias de la UE deben cumplir las disposiciones de la Carta en todas sus acciones. La Comisión está impulsando su capacidad interna en materia de cumplimiento de la Carta y está actualizando su caja de herramientas para la mejora de la legislación<sup>26</sup> incluidas las directrices de 2011 sobre la consideración de los derechos fundamentales en las evaluaciones de impacto<sup>27</sup>. También está elaborando formación específica sobre la Carta y una herramienta de aprendizaje electrónico para ayudar a los miembros del personal a evaluar el impacto de las políticas y las propuestas legislativas de la Comisión relativas a los derechos fundamentales. La herramienta de aprendizaje electrónico se pondrá a disposición del público y podría ser un recurso útil, junto con las actualizaciones de la caja de herramientas para la mejora de la legislación y las directrices actualizadas sobre la mejora de la legislación, para otras instituciones de la UE y para los legisladores y responsables políticos de los Estados miembros. La Comisión está dispuesta a apoyar al Parlamento Europeo y al Consejo para garantizar que apliquen eficazmente la Carta en su trabajo.

### **2.4 Reforzar la conciencia de las personas**

Junto con la adopción del presente informe, la Comisión va a poner en marcha una campaña de concienciación sobre la Carta para informar a las personas sobre sus derechos y sobre a quién deben dirigirse si estos se ven vulnerados. Esta campaña se desarrollará en línea, a través de actos para los medios de comunicación y en los medios sociales, con la etiqueta **#RightHereRightNow**. Se centrará en una serie de derechos concretos, como la no discriminación y la igualdad, los derechos del niño, la libertad de expresión y de información, y el derecho a la tutela judicial efectiva y a un juez imparcial. En la campaña de concienciación participarán socios clave como OSC, instituciones y organismos de derechos humanos nacionales, la FRA y otros organismos y agencias de la UE. Se forjarán vínculos con otras campañas de información en materia de derechos y con la Conferencia sobre el Futuro de Europa. La Comisión también ha traducido su página web sobre la Carta que figura

<sup>22</sup> [COM\(2020\) 713 final](#).

<sup>23</sup> Programa «Justicia», convocatoria de propuestas JUST-2021-JTRA, disponible en: <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home>.

<sup>24</sup> Por ejemplo, <https://era-comm.eu/charter-of-fundamental-rights/seminar-materials/>; <http://charterclick.ittig.cnr.it:3000/>; <http://help.elearning.ext.coe.int/>.

<sup>25</sup> [La Plataforma Europea de Formación](#).

<sup>26</sup> [Caja de herramientas para la mejora de la legislación](#) | [Comisión Europea \(europa.eu\)](#).

<sup>27</sup> [Directrices operativas para tener en cuenta los derechos fundamentales en las evaluaciones de impacto de la Comisión Europea](#) | [Comisión Europea \(europa.eu\)](#).

en el sitio web Europa a todas las lenguas oficiales de la UE<sup>28</sup> e hizo pública una nueva versión del Portal Europeo de Justicia en Red, que contiene información sobre la aplicación de la Carta y sobre dónde obtener ayuda<sup>29</sup>.

### **3. Hacer de la Carta la guía de la UE para la era digital**

La Comisión Europea se ha marcado como prioridad configurar la transición digital de un modo que beneficie a todo el mundo y no deje a nadie atrás. Lo que antes se describía como «el mundo fuera de línea» y el «mundo en línea» se está convirtiendo en una misma cosa: Esto plantea una serie de retos para garantizar el respeto de los derechos fundamentales en un entorno digital en rápida evolución.

La tecnología digital permea cada vez más todos los ámbitos de nuestra sociedad y puede utilizarse de formas muy diversas y, a menudo, beneficiosas. Las soluciones digitales impulsan la investigación científica, aumentan la producción industrial, facilitan la transición hacia la sostenibilidad, propician un amplio conjunto de servicios, y son, hoy por hoy, el principal canal de comunicación privado y público. Aumentan las posibilidades de las personas de participar en el discurso democrático y de informarse sobre cualquier tema. En particular, los sistemas de inteligencia artificial pueden servir para fomentar la innovación y la riqueza, y los ciudadanos pueden utilizarlos como herramientas en todas las esferas de la vida, por ejemplo, en la atención sanitaria, para realizar traducciones y para apoyar la toma de decisiones. La automatización digital ayuda a organizar el trabajo de un modo más eficiente y permite lograr unos niveles de coordinación sin precedentes. La recopilación de datos sobre las acciones humanas y sus efectos ayuda a las personas a entender y dar forma al mundo.

Al mismo tiempo, determinados usos de la tecnología corren el peligro de limitar la eficacia de la protección garantizada por los derechos fundamentales. La difusión de contenidos ilícitos como los discursos de odio y la pornografía infantil amenazan el derecho a la dignidad de la víctima, y la difusión de la desinformación amenaza al discurso democrático y nuestro derecho a acceder a la información. Cuando se automatizan los procesos o incluso las decisiones, puede resultar difícil garantizar la transparencia y la rendición de cuentas con respecto a los resultados, por ejemplo, en los casos en que se utilizan programas informáticos complejos para decidir la asignación del trabajo. Cuando falta información o es difícil obtenerla, puede resultar difícil evaluar y abordar las vulneraciones de los derechos fundamentales.

Cuanto más dependa una herramienta automatizada de factores externos como datos, aportaciones de las personas u otros sistemas para producir un resultado, más difícil resultará garantizar que dicha herramienta no vulnere los derechos desde el principio, por ejemplo, cuando determinados prejuicios adquiridos puedan influenciar la toma de decisiones en el ámbito laboral. Cuantos más datos se adquieran sobre las personas, más fácil será vigilarlas y atentar contra su intimidad. Los efectos de la red pueden mermar el poder de las personas frente a las grandes organizaciones, por ejemplo, en los mercados en línea o en las plataformas laborales, donde el poder de negociación o las posibilidades de organización de

<sup>28</sup> [Sus derechos en la UE |. Comisión Europea \(europa.eu\).](https://e-justice.europa.eu/581/ES/fundamental_rights)

<sup>29</sup> [https://e-justice.europa.eu/581/ES/fundamental\\_rights.](https://e-justice.europa.eu/581/ES/fundamental_rights)

las personas son escasos. Al mismo tiempo, las plataformas de medios sociales también se utilizan para difundir odio y contenidos ilícitos, por ejemplo, cuando difunden discursos ilícitos de odio, pornografía infantil o contenidos terroristas. Además, todavía hay trabajo por hacer a la hora de ayudar a que todo el mundo saque partido de las herramientas útiles y modernas en los lugares en los que el acceso a internet, los equipos o los conocimientos acerca de su uso son escasos.

Estos retos se pueden presentar de forma individual o combinada, según el contexto. Pueden reforzarse mutuamente y afectar a varios derechos fundamentales al mismo tiempo, lo que debe tenerse en cuenta a la hora de abordar estos retos. En este informe se presentan algunos de los aspectos más importantes en los que se plantean retos relacionados con los derechos fundamentales a causa del uso de la tecnología digital. Se muestran qué derechos se ven afectados en estos contextos, cómo está evolucionando la situación en los Estados miembros de la UE y cómo estos junto con la Comisión Europea utilizan la Carta para superar los distintos desafíos y salvaguardar y promover los derechos de las personas.

#### **4. Abordar los retos que entraña la moderación del contenido en línea**

Los intermediarios en línea como las plataformas de medios sociales desempeñan un papel importante en la vida de todas las personas y promueven nuevas formas de interacciones entre ellas, las administraciones públicas y las empresas. Su uso ha propiciado un aumento significativo de la información que está a disposición de los ciudadanos y proporciona mayores oportunidades para que estos ejerzan su derecho a la libertad de expresión y accedan a la información, creando asimismo múltiples espacios para el activismo en línea y la reunión de individuos y de la sociedad civil.

##### **Las grandes plataformas – la nueva plaza mayor**

- Algunas plataformas en línea se han vuelto tan importantes para facilitar el intercambio de información que desempeñan un papel fundamental en el debate democrático.
- Teniendo en cuenta que más de la mitad de la población de la UE utiliza los medios sociales, porcentaje que llega a prácticamente el 90 % entre los ciudadanos de 16 a 24 años de edad, los efectos del diseño de estas plataformas y las normas relativas a ellas tienen una amplia repercusión social<sup>30</sup>.
- Las herramientas y los mecanismos que utilizan estas plataformas para moderar sus contenidos y alentar a las personas a dedicar el máximo tiempo posible a la utilización de su servicio desempeñan un papel esencial en la configuración de la información y las opiniones que encuentran las personas en la red.
- No resulta fácil abordar los contenidos ilícitos de estas grandes plataformas, ya que se han convertido en espacios públicos para el intercambio de información sin ser legalmente responsables de las consideraciones de interés público.

<sup>30</sup> [https://ec.europa.eu/eurostat/web/products-datasets/-/isoc\\_sk\\_dskl\\_i](https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_sk_dskl_i).

Al mismo tiempo, el uso de las plataformas en línea está amplificando problemas sociales como la polarización<sup>31</sup> o la difusión de contenidos ilícitos, a menudo con efectos significativamente negativos en los derechos fundamentales, como la protección de los derechos del niño, la protección de los consumidores, la libertad de recibir o comunicar informaciones, y la protección de la propiedad intelectual.

La escala y la velocidad de difusión de contenidos en línea que no son ilícitos en sí mismos, como la desinformación y las teorías conspirativas, pueden afectar al discurso democrático, a la confianza en las instituciones y, como se ha visto a raíz de la pandemia de COVID-19, a la salud, la seguridad y la igualdad de trato.

La democracia en la UE se enfrenta a numerosos retos, como el populismo, el aumento de las desigualdades, un debate político cada vez más polarizado y la erosión de la confianza pública en los procesos democráticos causada por la desinformación<sup>32</sup>. La injerencia coordinada en las elecciones por parte de terceros países o intereses privados, la difusión de desinformación y una falta de transparencia y rendición de cuentas en los anuncios políticos dirigidos, están agravando estos fenómenos. También se ha manifestado preocupación con respecto a la inclusión o implicación insuficiente de determinados grupos, como los jóvenes, las personas de edad avanzada o las personas con discapacidad. Las minorías étnicas, entre ellas las comunidades gitanas, las personas LGBTIQ y las mujeres, dudan en mayor o menor medida y en función del contexto a la hora de presentar su candidatura política por miedo a la intimidación, las amenazas, el acoso y el discurso de incitación al odio. En estas circunstancias, las medidas destinadas a proteger los derechos fundamentales contribuyen directamente a la defensa de los valores de la UE de una sociedad sostenible, igualitaria, democrática y participativa en la que prevalecen la tolerancia, la no discriminación y el pluralismo.

La libertad de expresión, también en línea, constituye el núcleo de cualquier democracia. Toda medida legislativa o no legislativa relativa a la moderación de contenidos y la responsabilidad de los intermediarios en línea con respecto a los contenidos relativos a sus servicios debe tener en cuenta que el derecho a la libertad de palabra incluye el derecho a expresar ideas que puedan considerarse críticas, ofensivas, insultantes o controvertidas y que el derecho a la libertad de palabra solo puede limitarse en condiciones muy estrictas, por ejemplo, en relación con la difusión de contenidos supuestamente ilícitos como contenidos con discursos de odio. No obstante, el Tribunal Europeo de Derechos Humanos también ha dejado claro que los Estados están autorizados, e incluso pueden tener el deber positivo de contrarrestar todas las formas de expresión que difundan, inciten, promuevan o justifiquen el odio dirigido a personas o grupos pertenecientes a una etnia o religión determinada<sup>33</sup>.

<sup>31</sup> Véanse ejemplos de riesgos sociales sistémicos emergentes que plantean las plataformas en línea en la evaluación de impacto que acompaña a la propuesta de Reglamento relativo a un mercado único de servicios digitales (Ley de servicios digitales), [SWD\(2020\) 348 final](#), p. 40 («Evaluación de impacto de la Ley de servicios digitales»).

<sup>32</sup> Estudio del Parlamento Europeo solicitado por la Subcomisión de Derechos Humanos titulado *The impact of disinformation on democratic processes and human rights in the world* [«El impacto de la desinformación sobre los procesos democráticos y los derechos humanos en el mundo», documento en inglés], Carme Colomina, Héctor Sánchez Margalef, Richard Youngs, disponible en: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO\\_STU\(2021\)653635\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf).

<sup>33</sup> Sentencia de 6 de julio de 2006, Erbakan / Turquía, apartado 56.

En la mayoría de los casos, la desinformación y la información errónea no son ilícitas, ni siquiera aunque puedan parecer molestas u ofensivas. Si bien la obligación principal del Estado con respecto al discurso protegido por la libertad de expresión es evitar la interferencia y la censura, también tiene la obligación positiva de garantizar un entorno favorable para un debate público inclusivo y pluralista, en particular en relación con los procesos electorales, y para el ejercicio de la libertad de los medios de comunicación. Estas medidas van más allá del ámbito de la moderación de contenidos y guardan relación con acciones educativas e informativas más fundamentales.

Los agentes privados, como las plataformas en línea, definen sus propios términos y modelos de negocio en el ejercicio de sus derechos a la libertad de contratación y de empresa sin seguir instrucciones estatales relativas al tipo de contenidos que estarían obligados a alojar. En este contexto, podrían adoptar medidas que afectan significativamente a los usuarios y a sus derechos. No siempre existe un recurso jurídico disponible contra dichas decisiones privadas que permita equilibrarlas con los derechos e intereses legítimos de las personas y garantizar cierta previsibilidad. Cuando las plataformas en línea suprimen excesivamente los contenidos legales, pueden limitar significativamente la libertad de expresión e información.

#### **4.1 Situación en el ámbito de los Estados miembros**

En la **consulta específica** a efectos de elaborar el presente informe, los agentes de la sociedad civil informaron de problemas en los Estados miembros provocados por determinados contenidos ilícitos en línea, como campañas de desprestigio y ataques contra quienes trabajan para proteger los derechos de los demás. Se informó de que se centraban desproporcionadamente en las mujeres, en especial las mujeres de color y las pertenecientes a grupos vulnerables como los migrantes y los gitanos, así como las personas LGBTIQ. Los menores que utilizan las plataformas en línea están expuestos a contenidos inapropiados, nocivos y violentos, así como a depredadores en línea, lo que también aumenta los riesgos de captación de menores y reclutamiento en entornos extremistas. Se informó de la amplificación de la violencia sexual contra los niños a través de internet, por ejemplo, como consecuencia del aumento de la demanda de pornografía infantil.

Las organizaciones de la sociedad civil también identificaron la desinformación como un problema que afecta a la salud, la seguridad y el discurso democrático en varios Estados Miembros. Existía una preocupación generalizada con respecto a la falta de transparencia (etiquetas, alertas de intercambio, notificaciones de exposición) y a una falta de alfabetización mediática con respecto a los contenidos falsos o engañosos.

Si bien la difusión de contenidos ilícitos y desinformación se consideraba una amenaza, las OSC consultadas también alertaron de los efectos de la libertad de expresión cuando se utilizan políticas de moderación mal calibradas para hacer frente a estas amenazas. Las OSC indicaron que se ha hecho un uso indebido de la protección de los derechos de autor para acallar voces en línea y que se han utilizado leyes de difamación y enaltecimiento del terrorismo para la represión de ciudadanos. La escasa precisión de los sistemas de moderación automatizada de contenidos, en particular cuando se aplican a contenidos en los que la evaluación de su legalidad depende de un alto grado de contextualización, suscitó preocupación con respecto a los efectos injustificados en la libertad de expresión mediante retiradas excesivamente generalizadas de contenidos y el silenciamiento de determinadas declaraciones y opiniones, también de minorías. En opinión de miembros del sector

académico y de participantes en la consulta específica, el uso de algoritmos para adaptar la visualización de contenidos a los usuarios también puede distorsionar el discurso democrático, ya que a menudo está pensado para aumentar los ingresos por publicidad y no tiene como objetivo ofrecer a los ciudadanos información fiable de interés público. Los denunciantes de irregularidades también han hecho afirmaciones similares ante los medios de comunicación con respecto a que los algoritmos utilizados para adaptar el contenido que ven los usuarios están causando daño<sup>34</sup>. Más allá de los efectos del uso de estos sistemas en los derechos fundamentales, los participantes en la consulta específica alegaban que, a menudo, se utilizaban de un modo poco o nada transparente, y con escasa responsabilidad por sus resultados.

Varios Estados miembros han regulado los servicios digitales establecidos en sus territorios. Estas leyes tienen por objeto garantizar que los proveedores de servicios cumplan determinadas normas procesales cuando los usuarios o las autoridades denuncien contenidos ilícitos. En ocasiones, abarcan categorías concretas de contenidos ilícitos, como la vulneración de los derechos de autor o la incitación ilegal al odio. Sin embargo, los requisitos precisos de estas leyes a menudo difieren en varios puntos, como por ejemplo:

- la información necesaria para denunciar contenidos ilícitos;
- la posibilidad de reacción de quienes han publicado los contenidos;
- el plazo de reacción de los proveedores de servicios;
- las posibles medidas obligatorias contra las denuncias abusivas; o
- la posibilidad de remitir los casos controvertidos a un tercero independiente.

Más recientemente, frente a las crecientes preocupaciones sobre la difusión de los discursos de odio y los contenidos terroristas, varios Estados miembros han adoptado, propuesto o previsto la adopción de normas adicionales, centrándose en particular en determinadas categorías de contenidos ilícitos, y en algunos casos aplicables también a proveedores de servicios radicados fuera de su territorio. Sin embargo, como consecuencia de los esfuerzos individuales de los Estados miembros para abordar los contenidos ilícitos en línea y ofrecer diversos tipos de salvaguardias para la libertad de expresión, existe una fragmentación jurídica considerable. Varios Estados miembros<sup>35</sup>, así como el Consejo<sup>36</sup> y el Parlamento Europeo<sup>37</sup> han instado a que estas preocupaciones compartidas se aborden a escala de la UE. Además, varios Estados miembros observaron que la falta de cooperación transfronteriza entre las autoridades nacionales obstaculiza la supervisión efectiva de las plataformas en línea que operan a través de las fronteras<sup>38</sup>.

<sup>34</sup> Véase, por ejemplo, <https://www.theguardian.com/technology/2021/oct/10/frances-haugen-takes-on-facebook-the-making-of-a-modern-us-hero>.

<sup>35</sup> <https://digital-strategy.ec.europa.eu/en/summary-report-open-public-consultation-digital-services-act-package>.

<sup>36</sup> [Conclusiones del Consejo](#), de 9 de junio de 2020, «Conformar el futuro digital de Europa» y [Conclusiones](#) de la reunión especial del Consejo Europeo de los días 1 y 2 de octubre de 2020.

<sup>37</sup> Resolución del Parlamento Europeo de 20 de octubre de 2020 con recomendaciones a la Comisión sobre la Ley de servicios digitales: una mejora del funcionamiento del mercado único [2020/2018(INL)]; Resolución del Parlamento Europeo de 20 de octubre de 2020 con recomendaciones a la Comisión sobre una Ley de servicios digitales: adaptación de las normas de Derecho mercantil y civil a las entidades comerciales que operan en línea [2020/2019(INL)].

<sup>38</sup> Evaluación de impacto de la Ley de servicios digitales, sección 2.3.6. Cooperación limitada entre los Estados miembros y falta de confianza.

## 4.2 La respuesta política de la UE

A raíz de las peticiones manifestadas por los Estados miembros, se han adoptado varias iniciativas sectoriales a escala de la UE para abordar el problema de determinados tipos de contenidos ilícitos tales como los relacionados con el terrorismo, el abuso sexual de menores, la incitación al odio y la violencia, la trata de seres humanos, los productos inseguros y la vulneración de los derechos de autor, garantizando, al mismo tiempo, la protección de los derechos fundamentales.

### *Directiva de servicios de comunicación audiovisual*

La **Directiva de servicios de comunicación audiovisual** revisada se adoptó en 2018. Incluye medidas destinadas a proteger a los menores de contenidos y comunicaciones comerciales audiovisuales que les puedan causar un perjuicio físico, psíquico o moral. Además, los Estados miembros deben garantizar que los servicios de comunicación audiovisual no contengan incitación a la violencia o al odio contra las personas por cualquiera de los motivos mencionados en el artículo 21 de la Carta de los Derechos Fundamentales de la UE. La fecha límite de transposición de esta Directiva era el 19 de septiembre de 2020. En noviembre de 2020, la Comisión incoó procedimientos de infracción (cartas de emplazamiento) contra veintitrés Estados miembros que no habían transpuesto la Directiva y muchos la transpusieron el año siguiente. En septiembre de 2021, la Comisión envió una segunda advertencia (dictámenes motivados) a nueve Estados miembros por no haber notificado la transposición completa. La aplicación de la Directiva de servicios de comunicación audiovisual revisada es esencial no solo para los agentes del mercado, sino también para los ciudadanos (incluidos los espectadores y los menores).

### *La Directiva sobre los derechos de autor en el mercado único digital*

La **Directiva sobre los derechos de autor**<sup>39</sup> se adoptó en abril de 2019 y tiene por objeto garantizar que los titulares de derechos reciban una compensación justa por el uso de su obra. De este modo, logra un equilibrio entre derechos fundamentales contrapuestos como el derecho de propiedad intelectual, la libertad de expresión y de información, la libertad de las ciencias y el derecho a la educación y la diversidad cultural. La Directiva introduce excepciones obligatorias a los derechos de autor que protegen la libertad de expresión de los usuarios que generan y cargan contenidos en servicios de intercambio de contenidos en línea. También exigía a la Comisión la organización de un diálogo entre las partes interesadas para discutir las mejores prácticas para la cooperación entre los prestadores de servicios para compartir contenidos en línea y los titulares de derechos, teniendo especialmente en cuenta la necesidad de encontrar un justo equilibrio entre los derechos fundamentales y el uso de excepciones y limitaciones. Tras este diálogo, en junio de 2021, la Comisión adoptó una guía para apoyar la coherencia en la aplicación del artículo 17 de la Directiva, que establece nuevas normas sobre el uso de contenidos protegidos por parte de los servicios para compartir contenidos en línea<sup>40</sup>. La guía ofrece indicaciones prácticas sobre las disposiciones principales del artículo 17, que ayudan a los operadores del mercado a cumplir mejor las

<sup>39</sup> [Directiva \(UE\) 2019/790 sobre los derechos de autor y derechos afines en el mercado único digital](#) (DO L 130 de 17.5.2019, p. 92).

<sup>40</sup> Comunicación de la Comisión, Orientaciones sobre el artículo 17 de la Directiva 2019/790 sobre los derechos de autor en el mercado único digital, [COM/2021/288 final](#).

leyes nacionales que se basan en la Directiva y toman en consideración las opiniones recabadas de los Estados miembros y las partes interesadas.

### *El código de conducta para la lucha contra la incitación ilegal al odio racial y xenófobo*

En 2016, la Comisión firmó un **código de conducta** voluntario con las principales plataformas en línea para garantizar que las notificaciones relativas a la **incitación ilegal al odio racial y xenófobo** se evalúen rápidamente, no solo con respecto a las condiciones de servicio de las empresas, sino también con respecto a las leyes de los Estados miembros utilizadas para aplicar el Derecho de la UE que penaliza la incitación al odio racista y xenófobo<sup>41</sup>. El cumplimiento de dicho código de conducta se supervisa periódicamente<sup>42</sup>. Arroja buenos resultados y también ha promovido un enfoque colaborativo entre las plataformas en línea, los Estados miembros y la sociedad civil para garantizar una moderación de contenidos de alta calidad cuando se requiere un conocimiento profundo del contexto cultural, lingüístico e histórico del contenido controvertido.

### *Recomendación sobre la seguridad de los periodistas y otros profesionales de los medios de comunicación*

La seguridad se ha convertido en una gran preocupación para los periodistas debido a la incitación al odio en línea y a las amenazas de violencia física, pero también a los riesgos de ciberseguridad y la vigilancia ilegal. El 16 de septiembre de 2021, la Comisión Europea emitió una **Recomendación para la protección, la seguridad y el empoderamiento de los periodistas**<sup>43</sup>. La Recomendación anima a los Estados miembros a promover la cooperación entre las plataformas en línea y las organizaciones con experiencia en la lucha contra las amenazas de las que son objeto los periodistas, por ejemplo, impulsando su papel potencial como alertadores fiables. Los periodistas y otros profesionales de los medios de comunicación no son solo blanco de incitación en línea al odio y de amenazas de violencia física, sino que también pueden ser objeto de vigilancia ilegal, y la recomendación indica que los organismos de ciberseguridad nacionales competentes, previa solicitud, deben ayudar a los periodistas que traten de averiguar si sus dispositivos o cuentas en línea se han visto intervenidas a acceder a los servicios de investigadores forenses en materia de ciberseguridad. Los Estados miembros también deben promover un diálogo regular entre estos organismos de ciberseguridad, los medios de comunicación y la industria, en particular para reforzar la concienciación cibernética y desarrollar las capacidades digitales de los periodistas.

<sup>41</sup> [Decisión Marco 2008/913/JAI del Consejo, de 28 de noviembre de 2008, relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia mediante el Derecho penal](#) (DO L 328 de 6.12.2008, p. 55).

<sup>42</sup> El último ejercicio de seguimiento tuvo lugar en 2021: [El Código de Conducta de la UE para la Lucha contra la Incitación Ilegal al Odio en Internet](#) | Comisión Europea (europa.eu).

<sup>43</sup> Véase la Recomendación de la Comisión sobre la garantía de la protección, la seguridad y el empoderamiento de los periodistas y los otros profesionales de los medios de comunicación en la Unión Europea, de 16.9.2021, [C \(2021\) 6650 final](#).

### *Reglamento sobre la lucha contra la difusión de contenidos terroristas en línea*

La seguridad y el respeto de los derechos fundamentales no son objetivos contradictorios, sino coherentes y complementarios. La seguridad de los entornos físicos y en línea exige luchar contra los contenidos ilícitos en línea. Para garantizar la eliminación de los contenidos terroristas, el Parlamento Europeo y el Consejo adoptaron un **Reglamento sobre la lucha contra la difusión de contenidos terroristas en línea** en 2021<sup>44</sup>, que contiene una serie de salvaguardias para la protección de los derechos fundamentales, en particular la libertad de expresión. Por ejemplo, las autoridades nacionales solo pueden dictar órdenes de retirada de contenidos terroristas, tal y como se define en el Reglamento, y estas órdenes deben justificar por qué el material se considera contenido terrorista. El Reglamento excluye los contenidos difundidos con fines educativos, periodísticos, artísticos o de investigación, así como contenidos difundidos con fines de sensibilización contra actividades terroristas. No es obligatorio que las plataformas en línea utilicen herramientas automatizadas para anticipar la identificación o eliminación de contenidos terroristas, pero si se utilizan recursos técnicos, deben preverse salvaguardias para ofrecer garantías de fiabilidad, en particular, mediante la supervisión y la verificación humanas. A partir de marzo de 2023, los Estados miembros y las plataformas en línea también tendrán que presentar informes anuales sobre las medidas adoptadas para la retirada de contenidos terroristas y el funcionamiento de cualquier herramienta automatizada que haya podido ser empleada.

### *Legislación sobre el tratamiento de los abusos sexuales de menores en línea*

Aunque la acción reguladora para luchar contra los contenidos ilícitos se centra en gran medida en los contenidos disponibles públicamente, como los publicados en los medios sociales o los sitios web, también es necesario abordar el reto de la lucha contra la **pornografía infantil** compartida a través de servicios de comunicaciones interpersonales, incluidas las herramientas de comunicaciones interpersonales de los medios sociales. Una **legislación provisional**<sup>45</sup>, en vigor desde agosto de 2021, vela por que determinados servicios de comunicaciones en línea, como el correo web y los servicios de mensajería, puedan seguir utilizando tecnologías específicas, en la medida que sea estrictamente necesaria, con el fin de detectar pornografía infantil, denunciarla y retirarla, siempre que cumpla una serie de garantías de salvaguardia de la privacidad y la protección de datos personales de conformidad con el Reglamento General de Protección de Datos. Los mecanismos para detectar pornografía infantil en las comunicaciones interpersonales pueden afectar a los derechos fundamentales, en particular al derecho a la confidencialidad de las comunicaciones, la protección de los datos personales o la libertad de expresión. El Reglamento provisional tiene por objeto reducir ese impacto mediante la limitación de las tecnologías en línea utilizadas a las menos intrusivas para la privacidad, de conformidad con el estado actual de la técnica en el sector. El Reglamento también prevé mecanismos de recurso que deben establecerse para garantizar que los particulares puedan presentar

<sup>44</sup> [Reglamento \(UE\) 2021/784 sobre la lucha contra la difusión de contenidos terroristas en línea](#) (DO L 172 de 17.5.2021, p. 79).

<sup>45</sup> [Reglamento \(UE\) 2021/1232 por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea](#) (DO L 274 de 30.7.2021, p. 41).

reclamaciones ante los proveedores si sus contenidos se han retirado erróneamente. La Comisión está preparando también **una propuesta de legislación** para sustituir esta medida provisional y otorgar seguridad jurídica a los proveedores de servicios, así como para garantizar un enfoque uniforme para la detección, retirada y denuncia de pornografía infantil, al mismo tiempo que se establece el equilibrio adecuado entre los derechos del niño y la necesidad de proteger a los niños de los abusos sexuales, y el derecho a la vida privada y a las comunicaciones de todos los usuarios de los servicios en línea.

#### *Estrategia de la UE en la lucha contra la trata de seres humanos 2021-2025*

Combatir el modelo de negocio digital de los tratantes constituye una de las prioridades de la estrategia de la UE en la lucha contra la trata de seres humanos 2021-2025<sup>46</sup>, presentada por la Comisión en abril de 2021. Los proveedores de servicios de internet y las empresas relacionadas forman parte de la solución para apoyar los esfuerzos contra la trata de seres humanos mediante la identificación y la eliminación del material digital asociado con la explotación y el abuso de las víctimas de trata. La Comisión mantendrá un diálogo con las empresas tecnológicas y de internet pertinentes a fin de reducir el uso de las plataformas en línea para la captación y explotación de víctimas. La Comisión también facilitará los posibles diálogos de este tipo que lleven a cabo los Estados miembros a escala nacional.

#### *La propuesta de Reglamento relativo a la Ley de Servicios Digitales*

La propuesta de Reglamento relativo a la **Ley de servicios digitales**<sup>47</sup>, adoptada por la Comisión en diciembre de 2020 y que actualmente está siendo debatida por los colegisladores, define las responsabilidades de los intermediarios en línea. Sin perjuicio de las normas de la UE específicas de cada sector, como las relativas a los derechos de autor o a los contenidos terroristas en línea, ofrece un conjunto de normas horizontales en la UE para una gobernanza equilibrada de la moderación de los contenidos en línea.

La propuesta contempla la protección adecuada de todos los derechos fundamentales, incluidos la libertad de expresión y el derecho a la vida privada de los usuarios, la libertad de empresa de las plataformas y la libertad de contratación y los derechos de propiedad intelectual. También pretende mitigar los riesgos de las personas en situación de vulnerabilidad y los grupos vulnerables con el fin de brindarles protección frente a amenazas, intimidación o conducta discriminatoria y tiene por objeto proteger el derecho a la dignidad humana de todos los usuarios de servicios en línea.

La propuesta de Reglamento aspira alcanzar estos objetivos:

- Manteniendo en gran medida el régimen de responsabilidad de los intermediarios en línea, incluida la prohibición de imponer obligaciones generales de supervisión o investigación. Este enfoque se basa en la actual Directiva sobre el comercio

<sup>46</sup> Comunicación de la Comisión sobre la estrategia de la UE en la lucha contra la trata de seres humanos 2021-2025, [COM\(2021\) 171 final](#).

<sup>47</sup> Propuesta de Reglamento relativo a un mercado único de servicios digitales (Ley de Servicios Digitales) y por el que se modifica la Directiva 2000/31/CE, [COM/2020/825 final](#).

electrónico<sup>48</sup>. Su objetivo es ofrecer: i) la protección proporcionada y apropiada del derecho a la libertad de expresión por medio de la limitación de los incentivos para la retirada de contenidos legales, y el derecho a la libertad de empresa, garantizando la proporcionalidad en los esfuerzos exigidos a los intermediarios en línea y protegiendo a sus usuarios profesionales legítimos; e ii) inquietudes de política pública relacionadas con la difusión de distintos tipos de contenidos ilícitos, mediante la garantía de su rápida retirada por parte de los intermediarios en las condiciones establecidas por ley.

- Estableciendo obligaciones de diligencia debida claras y proporcionadas para los intermediarios en línea, a fin de garantizar que se actúa contra los contenidos ilícitos en línea de manera apropiada y transparente y que los usuarios puedan hacer valer sus derechos. La propuesta también recoge un riguroso conjunto de salvaguardias para los procesos de moderación de contenidos, incluidas las basadas en las condiciones marcadas con carácter privado.
- Imponiendo la obligación a las plataformas en línea de muy gran tamaño —aquellas que por su alcance han adquirido un papel esencial y sistémico a la hora de facilitar el debate público— de evaluar y reducir los riesgos que presentan sus servicios, también en relación con determinados derechos fundamentales: respeto de la vida privada y familiar, libertad de expresión y de información, no discriminación, y los derechos del niño. Las estrategias de reducción de riesgos también han de tener en cuenta los efectos potencialmente negativos de los algoritmos de amplificación de contenidos de las plataformas, como los sistemas de recomendación o publicitarios. Las plataformas en línea de muy gran tamaño también están sujetas a una rendición de cuentas cada vez mayor, lo que brinda a los usuarios más posibilidades de elección en sus interacciones en línea y permite que sus sistemas sean examinados por auditores independientes e investigadores autorizados.

### *Lucha contra la desinformación y regulación de la publicidad política en línea*

La difusión de desinformación, información errónea y mitos conspirativos puede dar lugar a la polarización de los debates y poner en riesgo la salud, la seguridad y el medio ambiente. La desinformación también puede mermar la capacidad de las personas de tomar decisiones con conocimiento de causa, basándose en hechos correctos. En algunos casos, la desinformación constituye un discurso que el Estado puede restringir legítimamente (como la incitación racista y xenófoba a la violencia y el odio). Sin embargo, muy a menudo, está protegida por el derecho a la libertad de expresión, incluso si carece de toda prueba científica o no está basada en hechos reales. En lo que respecta al discurso protegido, los Estados deben evitar la censura. Para ser eficaces, las acciones para limitar el alcance de los mitos de la desinformación y la conspiración deben complementarse con el fomento de un entorno favorable para un debate público inclusivo y pluralista. lo que resulta especialmente pertinente en relación con los procesos electorales.

<sup>48</sup> [Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior](#) (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000, p. 1).

En este contexto, durante el período 2020-2021 la Comisión siguió desarrollando varias acciones destinadas a lograr que el entorno en línea sea más transparente y sus agentes responsables, capacitar a los usuarios, y fomentar un debate democrático abierto. Estas acciones incluyeron: i) apoyo a los verificadores de datos y los investigadores académicos independientes, en particular por conducto del **Observatorio Europeo de los Medios de Comunicación Digitales** (EDMO)<sup>49</sup>, ii) medidas para mejorar la alfabetización mediática y iii) el seguimiento de un **Código autorregulador de Buenas Prácticas en materia de Desinformación**<sup>50</sup>. Basándose en los resultados de estas actividades de seguimiento, la Comisión también ha publicado orientaciones sobre el modo en que los signatarios actuales y nuevos del Código de Buenas Prácticas, incluidas las aplicaciones de mensajería privada, el sector publicitario y otras partes interesadas pertinentes podrían reforzar el alcance y la aplicación del Código, y garantizar un marco de seguimiento más sólido<sup>51</sup>.

Con el fin de fomentar el discurso democrático, el **Plan de Acción para la Democracia Europea**<sup>52</sup> establece medidas destinadas a promover elecciones libres y justas, reforzar la libertad de los medios de comunicación y combatir la desinformación. Esto incluye la propuesta sobre la transparencia y la segmentación de la publicidad política, adoptada en noviembre de 2021<sup>53</sup>, como parte de las medidas destinadas a proteger la integridad electoral y el debate democrático abierto. Estas normas propuestas dispondrán que toda la publicidad política sea etiquetada como tal e incluya información sobre quién la ha pagado y lo que ha costado. Las técnicas de segmentación y amplificación políticas tendrán que explicarse públicamente con un grado de detalle sin precedentes y quedarán prohibidas cuando se utilicen datos personales sensibles sin el consentimiento expreso de la persona interesada. Por último, el **nuevo Plan de Acción de Educación Digital (2021-2027)**<sup>54</sup> propone la elaboración de directrices para el personal docente y educativo para abordar la desinformación y fomentar la alfabetización digital.

### *La propuesta de un nuevo Reglamento relativo a la seguridad general de los productos*

Además, para atender nuevos requisitos sectoriales, la Comisión, como parte de la revisión del marco de la seguridad de los productos de la UE, adoptó y publicó una propuesta de nuevo **Reglamento relativo a la seguridad general de los productos** en junio de 2021<sup>55</sup>. Esta propuesta, basada en la propuesta de la Ley de Servicios Digitales, introducirá requisitos adicionales para los mercados en línea relativos a los productos no seguros como una categoría específica de contenidos ilícitos. La propuesta está siendo debatida en la actualidad por los colegisladores.

<sup>49</sup> EDMO – Unidos contra la desinformación.

<sup>50</sup> [Código de Buenas Prácticas en materia de Desinformación |. Configurar el futuro digital de Europa \(europa.eu\).](#)

<sup>51</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2585](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585).

<sup>52</sup> [Plan de Acción para la Democracia Europea |. Comisión Europea \(europa.eu\).](#)

<sup>53</sup> Propuesta de reglamento sobre la transparencia y la segmentación de la publicidad política, [COM\(2021\) 731 final](#).

<sup>54</sup> [Plan de Acción de Educación Digital \(2021-2027\) |. Educación y formación \(europa.eu\).](#)

<sup>55</sup> Propuesta de Reglamento relativo a la seguridad general de los productos, por el que se modifica el Reglamento (UE) n.º 1025/2012 y se deroga la Directiva 87/357/CEE del Consejo y la Directiva 2001/95/CE del Parlamento Europeo y del Consejo, [COM\(2021\)346 final](#).

## 5. Salvaguardar los derechos fundamentales cuando se utiliza la IA

El uso de tecnologías de inteligencia artificial (IA) puede tener efectos positivos significativos en nuestras sociedades. Puede aumentar la eficiencia de los procesos o impulsar la innovación y la investigación. También puede utilizarse para promover una serie de derechos fundamentales, como los derechos a la libertad de expresión y de información o a la protección de la salud, así como para fomentar cuestiones importantes de interés público como la seguridad pública o la salud pública.

Por otro lado, cuando la IA se utiliza sin las salvaguardias ni los controles de calidad adecuados para automatizar o apoyar procesos de toma de decisiones o para actividades como la vigilancia, también se pueden vulnerar los derechos de los ciudadanos. Estas vulneraciones pueden producirse a gran escala, dependiendo de lo generalizado que esté el uso de un sistema, y puede ser difícil prevenirlas o detectarlas cuando el sistema de IA no es suficientemente transparente o las personas no son conocedoras de su uso. Por ejemplo, el uso de la IA para inferir información acerca de las personas puede afectar a la protección de los datos y a la privacidad. El sesgo en los algoritmos o en los datos de entrenamiento, como el sesgo de género o el sesgo relacionado con el origen étnico o racial, puede conducir a resultados injustos y discriminatorios. Si un sistema para estimar las posibilidades de éxito en el trabajo se entrena mayoritariamente con datos sobre los hombres, es previsible que ofrezca peores resultados cuando se utilice para analizar datos de mujeres, y conduzca, probablemente, a la discriminación. Además, el uso de la IA también puede afectar a los derechos a la dignidad humana, a la buena administración, a la protección de los consumidores, a la seguridad y ayuda social, a la libertad de expresión, a la libertad de reunión, a la educación, al asilo, a la negociación y a la acción colectivas, a unas condiciones de trabajo justas y equitativas, al acceso a la prevención sanitaria, a la diversidad cultural y lingüística, a los derechos a la protección de datos y al respeto de la vida privada, así como a los derechos de grupos vulnerables, como los niños. Si esos sistemas se utilizan en el contexto de la aplicación de la ley o del poder judicial, también pueden afectar a la presunción de inocencia, así como al derecho a un juicio imparcial y una defensa justa. Es más, la inaccesibilidad o la inexistencia de información pertinente sobre los sistemas automatizados impide el cumplimiento efectivo de las obligaciones asociadas a los derechos fundamentales y el acceso de las personas a las vías de recurso legal.

### **¿Qué es la IA y cuáles son las características específicas que pueden conllevar riesgos?**

- IA es un término que designa un conjunto de tecnologías que han experimentado un rápido desarrollo en los últimos años. En el caso de determinados tipos de sistemas de IA, sus funciones siguen unas normas que se generan automáticamente y no son programadas explícitamente por personas. En ocasiones, esto puede generar resultados impresionantes, pero también puede entrañar riesgos. Basándose en la definición de la IA de la Organización de Cooperación y Desarrollo Económicos (OCDE), la propuesta de Ley de Inteligencia Artificial define la IA como un *software* que se desarrolla con aprendizaje automático, basado en la lógica y el conocimiento, y que puede, para un conjunto concreto de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa.

- La opacidad (falta de transparencia) y la complejidad (funcionamiento con numerosos componentes y procesos distintos) de determinados sistemas de IA dificultan la identificación y la prueba de posibles infracciones de la ley, incluidas las disposiciones que garantizan el respeto de los derechos fundamentales, y el rastreo del origen de posibles errores o del mal funcionamiento del sistema.
- Un subconjunto específico de aplicaciones de IA puede experimentar una adaptación constante, incluso durante su utilización, y cambiar y evolucionar de formas imprevistas, que no pueden controlarse fácilmente. Esto lleva a un determinado grado de imprevisibilidad que puede afectar a la seguridad o a los derechos fundamentales.
- El funcionamiento autónomo de los sistemas puede afectar a la seguridad, ya que algunos sistemas de IA requieren poca intervención humana o ninguna para el desempeño de sus tareas.
- La dependencia de los datos de determinados sistemas y los posibles sesgos integrados en los algoritmos pueden provocar o aumentar los sesgos y errores sistémicos. Si estos sistemas no se diseñan, se prueban y se utilizan adecuadamente, pueden agravar los resultados adversos como la discriminación.

### 5.1 Situación y acciones a escala de los Estados miembros

En los últimos años, los Estados miembros de la UE han procurado abordar los retos que entraña el uso de las tecnologías de IA. Muchos han elaborado estrategias nacionales de IA<sup>56</sup>, en las que ponen de relieve la necesidad de garantizar el respeto de los derechos fundamentales. Además, los Estados miembros han elaborado o tienen previsto elaborar guías y normas éticas que ayuden a quienes utilicen herramientas de IA a garantizar la transparencia, la trazabilidad y la solidez, a abordar posibles sesgos y buscar vías eficaces para cumplir sus obligaciones de respetar los derechos fundamentales. En algunos casos, las guías y los conocimientos especializados son elaborados por académicos<sup>57</sup> o grupos de expertos creados para este fin<sup>58</sup>.

Por otra parte, cuando actuaron conjuntamente a nivel de la UE, los Estados miembros subrayaron la necesidad de garantizar que los derechos de la Carta se respeten plenamente y pidieron una revisión de la legislación pertinente en vigor para que sea adecuada para su finalidad con vistas a garantizar que esta se adapte a las nuevas oportunidades y retos que plantea la inteligencia artificial<sup>59</sup>. En octubre de 2020, veintiséis de los veintisiete Estados miembros adoptaron un documento titulado «La Carta de los Derechos Fundamentales en el

<sup>56</sup> En junio de 2021, veinte Estados miembros y Noruega habían publicado sus estrategias nacionales de IA, mientras que siete Estados miembros se encontraban en la fase final de redacción.

[https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence\\_en](https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence_en).

<sup>57</sup> Por ejemplo, académicos de la Universidad de Utrecht elaboraron en abril de 2021 un Código de buena administración digital para las autoridades neerlandesas basado en los derechos fundamentales.

<https://www.rijksoverheid.nl/documenten/rapporten/2021/04/30/code-goed-digitaal-openbaar-bestuur>.

<sup>58</sup> Un ejemplo de ello es la «Comisión de Ética de los Datos» alemana y su experiencia en 2019:

[https://www.bmfv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission\\_node.html](https://www.bmfv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_node.html).

<sup>59</sup> Reunión del Consejo Europeo (19 de octubre de 2017) – [Conclusiones EUCO 14/17](#), p. 8. y [Conclusiones relativas al Plan Coordinado sobre la Inteligencia Artificial](#) (11 de febrero de 2019) 6177/19, 2019.

contexto de la inteligencia artificial y el cambio digital»<sup>60</sup>, en el que pedían que se afrontaran la opacidad, la complejidad y los sesgos, así como el cierto grado de imprevisibilidad y un comportamiento parcialmente autónomo de determinados sistemas de IA, con el fin de garantizar su compatibilidad con los derechos fundamentales y de facilitar la aplicación de las normas jurídicas. Los Estados miembros subrayaron la importancia de involucrar a diversas partes interesadas, también a las de la sociedad civil, para aprovechar su conocimiento especializado.

En el momento de la adopción del presente informe, ningún Estado miembro había adoptado legislación específica para abordar los retos relacionados con los derechos humanos que plantea la utilización de la IA<sup>61</sup>. Más bien, parece que las autoridades de los Estados miembros se basaban en la legislación en vigor. En 2017, un tribunal italiano ordenó al Ministerio de Educación de Italia que diera a conocer un algoritmo de toma de decisiones automatizada que utilizaba para la gestión de la movilidad de los trabajadores basándose en el derecho de acceso a la documentación, que también confiere el derecho a una vía de recurso efectiva<sup>62</sup>. En 2018, el Tribunal de Igualdad y No Discriminación de Finlandia consideró discriminatorio un asunto de calificación crediticia basada en estadísticas relativas al género, el lugar de residencia, la edad y el idioma en lugar de en una evaluación individual<sup>63</sup>. En febrero de 2020, un tribunal neerlandés invalidó la legislación neerlandesa que había establecido un sistema de detección de fraude basado en el derecho fundamental a la vida privada consagrado en el Convenio Europeo de Derechos Humanos<sup>64</sup>. El sistema de indicación del riesgo (SyRi) se utilizaba para analizar los datos recopilados por distintas autoridades públicas para detectar a personas que podrían cometer fraude en la percepción de prestaciones sociales. El tribunal neerlandés concluyó que el uso de SyRi no era suficientemente transparente y que su injerencia en el derecho a la intimidad no era proporcional al objetivo de detección del fraude.

Estos ejemplos muestran que los Estados miembros ya se han enfrentado a los retos que plantea el uso de la IA en relación con los derechos fundamentales. El enfoque propuesto por la Comisión con respecto a los retos relacionados con la IA tiene como objetivo reforzar la protección efectiva de los derechos fundamentales y, al mismo tiempo, fomentar la innovación en la IA.

## **5.2 La propuesta de la Comisión para regular la IA de alto riesgo**

En abril de 2021, la Comisión presentó una propuesta de Reglamento en materia de IA (Ley de Inteligencia Artificial)<sup>65</sup>. Los objetivos principales de la Ley de Inteligencia Artificial

<sup>60</sup> <https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/es/pdf>.

<sup>61</sup> Finlandia comunicó que se está trabajando en la elaboración de un proyecto de propuesta legislativa sobre la toma de decisiones administrativas automatizada para el fin de 2021. Con la inclusión de ejemplos de actuaciones de los Estados miembros (legislación, financiación u otras) en este informe se pretende ilustrar distintos tipos de actuaciones. No se pueden nombrar todas las iniciativas correspondientes a cada tema y la selección se basa, en gran medida, en la información presentada por los Estados miembros en junio de 2021.

<sup>62</sup> T.A.R., Roma, sect. III-bis, 22 marzo 2017, n.º 3769.

<sup>63</sup> [https://www.yvlttk.fi/material/attachments/ytaltk/tapausselosteet/45LI2c6dD/YVTltk-tapausseloste-21.3.2018-luotto-moniperusteinen\\_syrjinta-S-en\\_2.pdf](https://www.yvlttk.fi/material/attachments/ytaltk/tapausselosteet/45LI2c6dD/YVTltk-tapausseloste-21.3.2018-luotto-moniperusteinen_syrjinta-S-en_2.pdf).

<sup>64</sup> <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878>.

<sup>65</sup> Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, [COM/2021/206 final](#).

propuesta son la protección de los derechos fundamentales y la seguridad, así como la creación de un mercado único de sistemas de IA fiables. La propuesta tiene por objeto garantizar que los sistemas de IA de alto riesgo se diseñen y utilicen de conformidad con los derechos fundamentales y que los órganos jurisdiccionales y las autoridades nacionales competentes puedan investigar y abordar con mayor eficacia los posibles incumplimientos de las obligaciones asociadas a los derechos fundamentales.

La propuesta sigue un enfoque basado en el riesgo. Determinados sistemas de IA están directamente prohibidos, como los que se sirven de técnicas subliminales y los utilizados por las autoridades públicas para realizar calificaciones sociales, debido a que contravienen los valores de la UE. También se prohíbe el uso de sistemas de identificación biométrica remota en espacios de acceso público con fines de aplicación de la ley, salvo que se apliquen excepciones y salvaguardias claramente definidas.

Para introducir en el mercado los sistemas de IA de alto riesgo o ponerlos en servicio, estos tendrán que cumplir una serie de requisitos y seguir unos procedimientos de evaluación de la conformidad. Estos requisitos garantizan la documentación y las pruebas adecuadas de los sistemas de IA de alto riesgo, así como la calidad adecuada de los datos, la trazabilidad, la supervisión humana, la solidez, la precisión y la ciberseguridad. Se aplicarán cuando se utilicen sistemas de IA en esferas críticas, como la identificación biométrica, la educación, el empleo, los servicios públicos y privados esenciales, como los créditos, o las prestaciones de asistencia pública, la aplicación de la ley, la migración y el control fronterizo, y el poder judicial. Los sistemas de IA que sean componentes de seguridad de determinados productos (p. ej., maquinaria o productos sanitarios) también estarán cubiertos por los mismos requisitos y tendrán que ser controlados antes de que puedan comercializarse en la UE o ponerse en servicio.

La propuesta garantiza que los usuarios de los sistemas de IA, como las empresas que interactúan con los clientes o las autoridades públicas que toman decisiones, reciban información adecuada de los desarrolladores de los sistemas con el fin de garantizar el uso adecuado de sus aplicaciones y de que puedan cumplir sus obligaciones con arreglo a la legislación en materia de derechos fundamentales.

En caso de que se produzcan vulneraciones de los derechos fundamentales mediante el uso de sistemas de IA, se facilitará la reparación efectiva de las personas afectadas mediante la transparencia y la trazabilidad de estos sistemas, junto con unos controles *ex post* sólidos por parte de las autoridades competentes. Las autoridades de supervisión encargadas de velar por el cumplimiento de los derechos fundamentales, como las autoridades de protección de datos, los organismos de igualdad o los organismos de consumidores, tendrán acceso a toda la documentación relacionada con los sistemas de IA de alto riesgo que entren en su mandato. Podrán cooperar con las autoridades de vigilancia del mercado para probar los sistemas de IA correspondientes, cuando proceda.

En el caso de los sistemas específicos de IA, las obligaciones de transparencia con respecto a las personas afectadas reducirán al mínimo el riesgo de manipulación, en particular cuando se utilicen robots conversacionales (programas informáticos que pueden responder a preguntas en una conversación en línea) o ultrafalsificaciones (imágenes, audios o vídeos generados de forma artificial o manipulados que se asemejen a personas, objetos, lugares u otras entidades o sucesos existentes y que puedan inducir erróneamente a pensar que son auténticos o

veraces). También debe informarse a las personas cuando se utilicen sistemas de reconocimiento de emociones o de categorización biométrica, lo que les ayudará a hacer valer sus derechos con arreglo a la legislación en vigor en materia de protección de datos.

La propuesta se encuentra actualmente en fase de negociación con los colegisladores.

### **5.3 Interacción con la legislación sectorial: el ejemplo de la solvencia y la calificación crediticia**

La propuesta de Ley de Inteligencia Artificial trabajará conjuntamente con otra legislación en el establecimiento de normas sustantivas para el uso de los sistemas de IA en contextos claramente definidos. Por ejemplo, los proveedores de crédito utilizan a menudo técnicas de toma de decisiones automatizadas, incluidos los sistemas de IA, para las evaluaciones de la solvencia o la calificación crediticia. Estos proveedores se basan en distintos datos, muchos de los cuales no son proporcionados por los consumidores o estos los desconocen, algo que suscita preocupación con respecto a la protección de los datos personales, la discriminación directa o indirecta<sup>66</sup> y la protección de los consumidores<sup>67</sup>. La **Directiva sobre créditos al consumo**<sup>68</sup> y la **Directiva sobre créditos hipotecarios**<sup>69</sup> contienen disposiciones relacionadas con las evaluaciones de la solvencia. En junio de 2021, la Comisión adoptó una **nueva propuesta de Directiva sobre créditos al consumo** por la que se deroga y sustituye la Directiva sobre créditos al consumo en vigor. Propone unas normas relacionadas a la concesión de créditos al consumo en función de las cuales los Estados miembros tendrán que garantizar la documentación de los procedimientos y la información utilizados en las evaluaciones de solvencia. Además, las evaluaciones tendrán que basarse en información pertinente y exacta sobre las circunstancias financieras y económicas (p. ej., ingresos y gastos) y no deberán basarse en datos como los de los medios sociales. Los consumidores también tendrán derecho a una explicación sobre cómo se llegó a una decisión relativa a su solvencia, a expresar su punto de vista y a obtener intervención humana, lo que refleja los principios del Reglamento General de Protección de Datos<sup>70</sup> concernientes a la toma de decisiones automatizada. La nueva propuesta incluye también un artículo relacionado con la no discriminación, que establece que las condiciones que deben cumplirse para obtener un crédito no deben discriminar a los consumidores que residan legalmente en la Unión por razón de su nacionalidad o lugar de residencia o por cualquier otro motivo contemplado en el

<sup>66</sup> Informe de la evaluación de impacto que acompaña a la propuesta de Directiva relativa a los contratos de crédito al consumo por la que se deroga y se sustituye a la Directiva 2008/48/CE, COM(2021) 347 final.

<sup>67</sup> Por ejemplo, en abril de 2019, el Defensor del Pueblo para la Protección de los Datos de Finlandia ordenó a la empresa de créditos financieros Svea Ekonomi que corrigiera sus prácticas de evaluación de la solvencia, al considerar que un límite de edad máxima no era un factor aceptable, ya que la edad no describe la solvencia o la voluntad de pagar.

<sup>68</sup> Directiva 2008/48/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2008, relativa a los contratos de crédito al consumo y por la que se deroga la Directiva 87/102/CEE del Consejo (DO L 133 de 22.5.2008, p. 66).

<sup>69</sup> Directiva 2014/17/UE del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, sobre los contratos de crédito celebrados con los consumidores para bienes inmuebles de uso residencial y por la que se modifican las Directivas 2008/48/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 (texto pertinente a efectos del EEE) (DO L 60 de 28.2.2014, p. 34).

<sup>70</sup> Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

artículo 21 de la Carta de los Derechos Fundamentales. La propuesta se encuentra actualmente en fase de negociación con los legisladores.

#### 5.4 Capacidades

Cuando se utilizan sistemas de IA, es necesario que los trabajadores estén debidamente cualificados con el fin de garantizar el respeto de los derechos fundamentales y una supervisión humana apropiada. Las autoridades de supervisión también necesitarán personal con capacidades técnicas específicas para cumplir eficazmente sus mandatos. En septiembre de 2020, la Comisión adoptó un **Plan de Acción de Educación Digital** para 2021-2027<sup>71</sup>, cuyo objetivo consiste en fomentar las capacidades digitales, también en relación con la IA<sup>72</sup>, e incluye la elaboración de orientaciones éticas en el ámbito de la IA y los datos en la educación y la formación. Además, todos los Estados miembros que han adoptado estrategias nacionales de IA han integrado en ellas un componente relacionado con las capacidades, por ejemplo, por medio de reformas de los sistemas educativos para reforzar el pensamiento computacional o de iniciativas para adaptar el aprendizaje permanente y las políticas de reciclaje profesional<sup>73</sup>.

### 6. Abordar la brecha digital

Estar conectado y ser competente digitalmente permite una participación activa en la sociedad. Cada vez son más las actividades esenciales que se están trasladando a internet, desde la búsqueda de empleo, la realización de trabajos mediante teletrabajo y la educación, hasta la interacción con la administración pública o la solicitud de una cita médica. Pero no todo el mundo está conectado. No estar conectado puede afectar a las personas en el ejercicio de sus derechos. Por ejemplo, puede afectar a los derechos de las personas en una sociedad democrática, incluido su derecho a la libertad de expresión y de información, y su derecho a presentar su candidatura en las elecciones municipales, puesto que las campañas políticas cada vez se desarrollan más a través de la red. Al cerrarse las oficinas y pedirse a las personas que se comuniquen en línea con sus administraciones nacionales, la pandemia de COVID-19 ha exacerbado las dificultades que tienen quienes carecen del equipo o los conocimientos digitales necesarios para acceder a los servicios públicos.

Este fenómeno se suele denominar «la brecha digital». Aún hoy, el 46 % de los europeos carecen de competencias digitales básicas<sup>74</sup>. Así lo reconoce el **pilar europeo de derechos sociales**, que incluye las comunicaciones digitales entre los servicios esenciales a los que todo el mundo debería tener acceso y pide medidas de apoyo para quienes lo necesiten<sup>75</sup>. Quienes carecen de un acceso regular a internet, o de las capacidades necesarias para hacer uso de estos servicios, o bien no pueden acceder a un producto o servicio digital debido a una discapacidad física o cognitiva, corren un riesgo cada vez mayor de quedar excluidos y de tener dificultades para hacer valer sus derechos.

<sup>71</sup> [Plan de Acción de Educación Digital \(2021-2027\)](#) | Educación y formación (europa.eu).

<sup>72</sup> [https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan/action-8\\_es](https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan/action-8_es).

<sup>73</sup> [https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence\\_en](https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence_en).

<sup>74</sup> <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020DC0624> y [Estadísticas](#) | Eurostat (europa.eu).

<sup>75</sup> [El pilar europeo de derechos sociales en 20 principios](#) | Comisión Europea (europa.eu), véase el principio 20.

En el caso de los servicios públicos a los que se puede acceder exclusivamente por medios digitales, las personas que no están conectadas pueden verse imposibilitadas o necesitadas de ayuda para ejercer sus derechos. A modo de ejemplo, el *Haut Conseil du Travail*, un órgano consultivo del Ministerio de Asuntos Sociales de Francia, estima que en este país una de cada cinco personas tiene dificultades para cumplimentar procedimientos administrativos en línea, y advierte que la digitalización puede hacer peligrar el principio de igualdad de acceso a los servicios públicos si no se mantienen unos medios de acceso alternativos<sup>76</sup>. Del mismo modo, como cada vez son más las actividades económicas que tienen un componente digital, el ejercicio del derecho de acceso a los servicios de interés económico general está cada vez más condicionado al acceso a internet. Los niños que carecen de un dispositivo conectado en casa tienen dificultades para participar de forma remota en la escuela, lo que afecta a los derechos del niño y al derecho a la educación. Además, cuando los sitios web y las aplicaciones móviles no están adaptados a las necesidades de las personas con discapacidad, su derecho a la integración puede verse mermado.

En vista de los retos que plantea la brecha digital, los Estados miembros y la Comisión están aplicando una serie de medidas para garantizar que nadie se quede atrás. Como se anunció en el **Plan de Acción del Pilar Europeo de Derechos Sociales**<sup>77</sup>, en 2022 la Comisión publicará un informe sobre el acceso a los servicios esenciales, que también abordará el acceso a las comunicaciones digitales, y presentará un resumen de la situación en la EU-27, así como un inventario de las medidas y buenas prácticas nacionales y de la UE en vigor y de las buenas prácticas que apoyan el acceso a las personas necesitadas.

### 6.1 Reducción general de la brecha digital

El hecho de que durante la pandemia muchas actividades se trasladaran al entorno en línea no solo constituye un reto, sino también una oportunidad. Los Estados miembros han elaborado proyectos que serán financiados por la UE para ayudar a la economía a recuperarse de la recesión provocada por la pandemia. Estos proyectos incluyen medidas para abordar la brecha digital y lograr unos derechos digitales inclusivos, así como para abordar la digitalización del trabajo. Cabe citar como ejemplo dos planes nacionales. **Rumanía** tiene previsto invertir en la creación de contenidos educativos y recursos accesibles, como vídeos y clases interactivas, y desarrollar programas accesibles de alfabetización digital dirigidos a alumnos con discapacidad. **Alemania** pretende ayudar a adquirir dispositivos digitales para los profesores de todo el país. Además, creará una plataforma de aprendizaje permanente en línea y se prestará especial atención a la ayuda a las personas menos cualificadas formalmente.

<sup>76</sup> [https://solidarites-sante.gouv.fr/IMG/pdf/pourquoi\\_et\\_comment\\_les\\_travailleurs\\_sociaux\\_se\\_saisissent\\_des\\_outils\\_numeriques.pdf](https://solidarites-sante.gouv.fr/IMG/pdf/pourquoi_et_comment_les_travailleurs_sociaux_se_saisissent_des_outils_numeriques.pdf), p.4.

<sup>77</sup> [El Plan de Acción del Pilar Europeo de Derechos Sociales \(europa.eu\)](#).

En términos más generales, existen varias iniciativas prometedoras en distintos Estados miembros<sup>78</sup>. En febrero de 2021, **Bélgica** puso en marcha un concurso público de proyectos de apoyo a las empresarias afectadas por la pandemia de COVID-19, ofreciendo también orientaciones para la digitalización. El país también está invirtiendo en organizaciones locales que tienen por objeto aumentar las capacidades digitales de los jóvenes en situaciones económicas precarias.

**Portugal** está movilizando a jóvenes voluntarios para que ayuden a educar a los adultos en lo referente a la transición digital, sobre la base de una red nacional de 1 500 centros formativos y una serie de herramientas y recursos gratuitos. Se espera que el programa de inclusión digital llegue a un millón de personas y se ejecutará en colaboración con las autoridades y organizaciones locales<sup>79</sup>.

Con una lógica similar a la iniciativa WiFi4EU<sup>80</sup>, **Italia** subvenciona el acceso a internet para determinadas personas y ha iniciado el proyecto *Piazza Wifi Italia*<sup>81</sup> que permite a más de 400 000 personas conectarse fácilmente y de forma gratuita, a través de una aplicación específica, a una red wifi gratuita repartida por todo el país. En marzo de 2020, el proyecto se amplió para incluir a los centros sanitarios y también a los hospitales.

Es probable que la infraestructura digital siga evolucionando y la UE ha tomado medidas en una serie de ámbitos para mejorar la conectividad. El objetivo principal de la conectividad en la **Década Digital** es que todos los hogares europeos tengan acceso a una cobertura de Internet de alta velocidad para 2025 y conectividad de altísima velocidad para 2030<sup>82</sup>. En marzo de 2021, la Comisión y los Estados miembros acordaron una **caja de herramientas de conectividad** para fomentar el despliegue de redes digitales y facilitar el acceso al espectro 5G. La revisión de la Directiva sobre reducción de costes de la banda ancha, prevista para 2022, tiene por objeto seguir apoyando el despliegue de las redes digitales mediante la reducción de la carga administrativa y del coste y el ritmo de dichos despliegues. Además, la **visión para las zonas rurales**<sup>83</sup> de la Comisión de junio de 2021 busca abordar la brecha urbana / rural posibilitando para ello el acceso a conectividad rápida a internet, 5G (también a través de financiación de la UE<sup>84</sup>) y tecnología digital, y reforzando asimismo las competencias digitales. La conectividad de banda ancha de alta velocidad es un factor clave para la transición digital y la recuperación posterior a la COVID-19. La Comisión se comprometió a reducir las fracturas digitales de la accesibilidad en las zonas rurales y la UE invertirá en infraestructura de red, un estándar para la transmisión de datos inalámbrica, y en

<sup>78</sup> No es posible mencionar todas las iniciativas en este informe y con la siguiente selección se pretende ilustrar los distintos tipos de actuaciones. Se basa en información presentada por los Estados miembros en junio de 2021.

<sup>79</sup> [Resolução do Conselho de Ministros n.º 30/2020 - DRE.](#)

<sup>80</sup> <https://digital-strategy.ec.europa.eu/es/activities/wifi4eu>.

<sup>81</sup> <https://www.wifi.italia.it/it/>.

<sup>82</sup> Comunicación de la Comisión «Brújula Digital 2030: el enfoque de Europa para el Decenio Digital», [COM\(2021\) 118 final](#).

<sup>83</sup> [Visión a largo plazo para las zonas rurales de la UE | Comisión Europea \(europa.eu\)](#).

<sup>84</sup> Habrá financiación disponible del Fondo Europeo de Desarrollo Regional, el Fondo Europeo Agrícola de Desarrollo Rural, el Mecanismo «Conectar Europa» - Sector digital y el Mecanismo Recuperación y Resiliencia para cumplir los objetivos de conectividad de la UE para 2025.

fibra para garantizar que todo el mundo en la UE tenga acceso a infraestructura de conectividad digital eficiente desde el punto de vista energético y que resista al paso del tiempo.

## 6.2 Administración pública

Gracias a la tecnología digital, las personas pueden beneficiarse de un acceso más amplio a la información y los servicios públicos que puede ayudarles a gestionar su vida cotidiana y a ejercer sus derechos, en particular las libertades de establecimiento y prestación de servicios. Desde la **Declaración de Malmö**, firmada durante una cumbre celebrada en Suecia en 2009, los Estados miembros han realizado avances constantes para modernizar las administraciones públicas<sup>85</sup>. La **Declaración de Tallin** de 2017 dio un impulso a la digitalización de los servicios públicos para las personas y los servicios públicos transfronterizos para las empresas<sup>86</sup>. Más recientemente, la **Declaración de Berlín** de 2020 incluía medidas a tomar para la protección de los derechos fundamentales en línea entre los compromisos de los Estados miembros<sup>87</sup> y la **Declaración de Lisboa** de junio de 2021 tiene por objeto garantizar que «nadie se quede atrás». Los esfuerzos realizados por los Estados miembros también incluyen la digitalización de la justicia<sup>88</sup>.

Los Estados miembros están aplicando diferentes enfoques para garantizar el acceso a los servicios públicos, intentando reducir esta brecha digital y satisfaciendo al mismo tiempo las exigencias de esta era digital. Por ejemplo, **Francia** ha optado por mantener varias vías para garantizar el acceso a los servicios públicos con el fin de evitar cualquier obstáculo. Los ciudadanos no están obligados a contactar con la Administración de forma electrónica. Sin embargo, **Dinamarca** ha seguido un camino distinto, estableciendo una estrategia «digital por defecto», y, en 2014, impuso la obligatoriedad del uso de medios electrónicos para todos los contactos con la Administración. Para abordar la brecha digital, el Estado está financiando medidas como ayuda personalizada directa en las bibliotecas<sup>89</sup>, asistencia con la compra de equipos y contribuciones a las suscripciones a internet. En una línea similar, en **los Países Bajos** el Gobierno y las bibliotecas locales han puesto en marcha el «Punto de Información del Gobierno Digital», una iniciativa en la que un empleado de la biblioteca con formación responde a las preguntas y ayuda a las personas con los servicios gubernamentales digitales tradicionales, como las declaraciones de impuestos y los servicios sociales, así como con servicios más novedosos como las aplicaciones relacionadas con el coronavirus.

<sup>85</sup> <https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf>.

<sup>86</sup> <https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration>.

<sup>87</sup> [https://ec.europa.eu/isa2/news/eu-member-states-sign-berlin-declaration-digital-society\\_en](https://ec.europa.eu/isa2/news/eu-member-states-sign-berlin-declaration-digital-society_en).

<sup>88</sup> El Informe sobre el Estado de Derecho en 2021 de la Comisión refleja los avances realizados en este ámbito: [https://ec.europa.eu/info/sites/default/files/communication\\_2021\\_rule\\_of\\_law\\_report\\_en.pdf](https://ec.europa.eu/info/sites/default/files/communication_2021_rule_of_law_report_en.pdf). Véase también la Comunicación de la Comisión sobre la digitalización de la justicia en la UE, [COM \(2020\) 710 final](#), acompañado por [SWD\(2020\) 540](#), de 2 de diciembre de 2020.

<sup>89</sup> Este tipo de apoyo también se ofrece en otros lugares, pero para los fines de ilustrar el enfoque basta con seleccionar unos cuantos ejemplos. El objetivo de este informe no es ofrecer un catálogo exhaustivo de medidas, sino un resumen de las ideas y los enfoques.

### 6.3 Sanidad

La pandemia ha causado un aumento de la prestación de asistencia sanitaria en línea, p. ej., a través de consultas virtuales o por medio de aplicaciones y programas informáticos desarrollados con fines de diagnóstico o terapéuticos. Para algunas personas, como las que residen en zonas rurales o en pequeñas islas, esta tendencia hace que les resulte más fácil recibir atención médica, mientras que para otras representa un nuevo obstáculo. Las medidas destinadas a salvar la brecha digital pueden mejorar la situación de las personas que carecen de acceso o de competencias. Por ejemplo, **Polonia** ha introducido la «Cuenta de Internet del Paciente», una herramienta en línea que da a los pacientes acceso a la información sobre su tratamiento médico pasado, actual o previsto, y les permite gestionar una serie de cuestiones (receta electrónica, consulta de historiales, derivación electrónica, bajas médicas electrónicas, y derechos) sin necesidad de acudir personalmente a un centro de atención sanitaria.

### 6.4 Educación

Varios Estados miembros cuentan con políticas y programas para fomentar el acceso a la tecnología y reforzar las competencias digitales en el contexto de la educación formal. **Grecia**, por ejemplo, ofrece a los alumnos y estudiantes que lo necesitan vales para la compra de equipos como tabletas u ordenadores e imparte programas educativos pertinentes a través de una «Academia de Capacidades Digitales» virtual puesta en marcha de 2020.

En el ámbito de la UE, el **Plan de Acción de Educación Digital**<sup>90</sup> (2021-2027), puesto en marcha en septiembre de 2020, marca una visión estratégica a largo plazo para una transformación digital sostenible e inclusiva en la educación y la formación. Promueve el derecho de acceso a una educación digital de alta calidad para todos y la igualdad de acceso a las infraestructuras, prestando especial atención a alentar la participación de las mujeres y las niñas en las materias CTIM (ciencia, tecnología, ingeniería y matemáticas).

### 6.5 Integración de las personas con discapacidad

El **Código Europeo de Comunicaciones Electrónicas**<sup>91</sup> garantiza el acceso equivalente y la posibilidad elección de los servicios de comunicaciones electrónicas para los usuarios finales con discapacidad, facilitando la participación en la sociedad digital. La **Ley europea de accesibilidad**<sup>92</sup> entrará en vigor en 2025 y ampliará la inclusión de las personas con discapacidad y las personas de edad avanzada en el mundo digital haciendo más accesible un conjunto de productos y servicios clave del sector público y privado. La **Directiva sobre la accesibilidad a la web** de 2016<sup>93</sup> obliga a los Estados miembros a garantizar que los sitios web y las aplicaciones para dispositivos móviles de los organismos del sector público sean accesibles a las personas con discapacidad, como las personas con deficiencia visual, auditiva o motora. De este modo, promueve la libertad de expresión y de información, el derecho a la educación, la libertad profesional y el derecho a trabajar, la no discriminación, la integración

<sup>90</sup> [Plan de Acción de Educación Digital \(2021-2027\) | Educación y formación \(europa.eu\)](#).

<sup>91</sup> [Directiva \(UE\) 2018/1972 por la que se establece el Código Europeo de las Comunicaciones Electrónicas \(versión refundida\)](#) (DO L 321 de 17.12.2018, p. 36).

<sup>92</sup> [Directiva \(UE\) 2019/882 sobre los requisitos de accesibilidad de los productos y servicios](#) (DO L 151 de 7.6.2019, p. 70).

<sup>93</sup> [Directiva \(UE\) 2016/2102 sobre la accesibilidad de los sitios web y aplicaciones móviles de los organismos del sector público](#) (DO L 327 de 2.12.2016, p. 1).

de las personas con discapacidad, el acceso a los servicios de interés económico general, el derecho de acceso a los documentos, el derecho a circular y residir libremente en el territorio de la Unión, la libertad de establecimiento y su libertad para prestar servicios.

La Directiva puede aplicarse de distintas maneras. Por ejemplo, **Eslovenia** modernizó su portal estatal de gobierno electrónico de forma que pueda ser utilizado por las personas ciegas y con deficiencia visual, las personas sordas y con problemas auditivos, las personas con dislexia y los usuarios con dificultades de comprensión. Las descripciones textuales de los procedimientos, por ejemplo, se acompañan de breves vídeos, que también ofrecen interpretaciones en lengua de signos. En **Grecia**, durante la pandemia se adaptaron los libros de texto digitales para que las personas con todas las categorías de discapacidad pudieran acceder a ellos.

## 7. Proteger a las personas que trabajan a través de plataformas

Las plataformas en línea constan de un amplio abanico de mercados, medios sociales, puntos de venta de contenidos creativos, tiendas de aplicaciones, sitios web de comparación de precios, plataformas para la economía colaborativa, así como motores de búsqueda. Todos ellos facilitan la interacción entre los usuarios y las empresas. Han surgido las plataformas de trabajo digitales, un subconjunto específico de las plataformas en línea, como una característica distintiva de la economía digital.

El trabajo en plataformas ha generado nuevas oportunidades económicas para las personas, y les permite, por ejemplo, dedicarse a actividades a tiempo parcial y acceder al mercado laboral en general, pero al mismo tiempo plantea retos en relación con los derechos fundamentales, como la protección de los datos personales, la privacidad, los derechos de los trabajadores a la información y la consulta, el derecho a la negociación y la acción colectivas, y unas condiciones laborales justas y equitativas. De los 28 millones de personas que se calcula que trabajan a través de plataformas de trabajo digitales, puede haber hasta 5,5 millones de personas que son «falsos» autónomos<sup>94</sup>. Aunque sus contratos con las plataformas a través de las que trabajan describen a estas personas como trabajadores autónomos, en realidad están sujetas a control y supervisión, que son características de la condición de «trabajador por cuenta ajena». Los modelos empresariales basados en algoritmos también plantean retos, como la falta de información y consulta con las personas que trabajan a través de plataformas y sus representantes acerca del modo en que se utilizan los algoritmos y en que estos afectan a las condiciones laborales del trabajo en plataformas. Tampoco existen suficientes vías de recurso ni unas responsabilidades claras con respecto al uso de algoritmos.

<sup>94</sup> Véase el *Impact Assessment report accompanying the proposal for a Directive on improving working conditions in platform work* [«Informe de la evaluación de impacto que acompaña a la propuesta de Directiva sobre la mejora de las condiciones de trabajo en las plataformas digitales», documento en inglés] [SWD\(2021\) 396 final](#).

## El trabajo en plataformas

Normalmente, en el trabajo en plataformas intervienen tres partes: la **plataforma**, la **persona que trabaja a través de ella** y el **cliente** (particulares o empresas). En determinados casos también puede intervenir una cuarta parte, por ejemplo, restaurantes con servicio de entrega a domicilio.

Las plataformas de trabajo digitales suelen definirse a sí mismas como intermediarias y describen la relación entre las partes como una relación de trabajo autónomo. Las tareas realizadas en las plataformas de trabajo digitales pueden ser complejas, como la programación informática y el diseño gráfico, o bien sencillas, como el etiquetado de imágenes.

La Presidenta de la Comisión, Ursula von der Leyen, anunció en sus orientaciones políticas la necesidad de mejorar las condiciones de trabajo en las plataformas<sup>95</sup>. La crisis de la COVID-19 y la adopción acelerada de modelos empresariales de plataformas digitales han puesto aún más de relieve esta necesidad. Una resolución reciente del Parlamento Europeo<sup>96</sup> subraya que el trabajo en plataformas ha suscitado preocupación por la precariedad y las malas condiciones de trabajo, la falta o la dificultad de acceso a una protección social adecuada, los ingresos irregulares o impredecibles, y una ausencia de medidas de salud y seguridad en el trabajo. En la resolución se pide una acción firme de la UE para abordar la clasificación errónea del empleo y mejorar la transparencia en el uso de algoritmos, también para los representantes de los trabajadores.

### 7.1 Situación y acciones a escala de los Estados miembros

Para evitar la competencia desleal en detrimento de los trabajadores y una carrera de mínimos en las prácticas de empleo y las normas sociales, la UE ha creado un límite mínimo de derechos laborales aplicable a los trabajadores de todos los Estados miembros. El corpus jurídico de la UE en materia laboral y social ha ido creciendo a lo largo de los años. Además, las respuestas nacionales a los retos que plantea el trabajo en plataformas difieren de un Estado miembro a otro. Algunos han adoptado legislación nacional para mejorar las condiciones laborales o el acceso a la protección social en el trabajo en plataformas. Los tribunales se han pronunciado sobre la cuestión de la clasificación errónea de la situación profesional en un importante número de Estados miembros. En algunos de ellos, los interlocutores sociales y las empresas de plataformas han entablado negociaciones sobre convenios colectivos.

En 2016, **Francia** adoptó una legislación que prevé derechos laborales y sociales para las personas que trabajan a través de plataformas, independientemente del sector de actividad económica, mediante una reforma laboral. La ley se aplica a los trabajadores autónomos tecnológica y económicamente dependientes. Otorga acceso a un régimen de seguro

<sup>95</sup> COM(2021) 762.

<sup>96</sup> Resolución del Parlamento Europeo de 16 de septiembre de 2021 titulada *Fair working conditions, rights and social protection for platform workers – new forms of employment linked to digital development* («condiciones de trabajo justas, derechos y protección social para los trabajadores de plataformas: nuevas formas de empleo vinculadas al desarrollo digital», documento en inglés) [[2019/2186\(INI\)](#)].

voluntario contra accidentes profesionales, obliga a las plataformas a pagar primas de seguros o a ofrecer seguros colectivos a sus trabajadores, y garantiza el derecho a emprender acciones colectivas y a seguir formándose. Además, el tribunal superior para asuntos laborales privados (el Tribunal de Casación) destacó en dos sentencias que debe reconocerse la condición de trabajadores a los trabajadores de plataformas del ámbito de los servicios de alquiler de vehículos con conductor cuando la plataforma pueda elaborar instrucciones y exigir su cumplimiento<sup>97</sup>. Sin embargo, el debate sobre la condición real de las personas que trabajan a través de plataformas sigue abierto, también en otros sectores.

La región **italiana** del Lacio promulgó<sup>98</sup> en 2019 una legislación destinada a mejorar las condiciones laborales y la protección social de todos los trabajadores de plataformas independientemente de su situación profesional. Esta legislación contempla salvaguardias para los accidentes de trabajo, formación adecuada en materia de seguridad y seguro de responsabilidad civil y de accidentes. También prohíbe el pago por tareas. Además, en 2019, Italia adoptó legislación nacional para mejorar las condiciones de trabajo de los repartidores de comida autónomos<sup>99</sup>. Por otra parte, en julio de 2021, la autoridad italiana de protección de datos ordenó a Deliveroo Italia el pago de una multa de 2,5 millones EUR como consecuencia de la falta de transparencia en el uso de algoritmos y la recopilación desproporcionada de datos de los trabajadores. La autoridad detectó infracciones de algunas disposiciones del Reglamento general de protección de datos y de la legislación nacional en materia de privacidad, el estatuto de los trabajadores italianos y la citada legislación relativa a la protección de los trabajadores<sup>100</sup>.

**España** adoptó legislación en mayo de 2021, mediante la que introdujo una presunción en virtud de la cual se considera trabajadores a quienes trabajen a través de plataformas de reparto tanto de comida como de paquetes, invirtiendo la carga de la prueba a las plataformas con respecto a la demostración de que no lo son<sup>101</sup>. Además, esta ley obliga a las plataformas a proporcionar información sobre la gestión algorítmica, incluido el control digitalizado del rendimiento y la asignación automatizada de los encargos, a los sindicatos. Esta ley estipula que todas las empresas (no solo las plataformas de reparto) deben informar a sus trabajadores de los parámetros y las reglas en los que se basan los sistemas automatizados, que pueden afectar a las condiciones de trabajo, el acceso al empleo y el mantenimiento de este.

**Alemania** publicó documentos de orientación sobre el futuro del trabajo, concernientes a la inclusión de los trabajadores autónomos que realizan trabajos en plataformas en los planes de seguros y de pensiones, y a las mejoras de sus seguros de accidentes laborales.

En noviembre de 2020, **Portugal** también publicó un documento de orientación sobre el futuro del trabajo, relativo a la creación de una presunción legal sobre la condición de las personas que trabajan a través de plataformas, formas de aumentar la protección social de los trabajadores autónomos y formas de fomentar la representación colectiva de los trabajadores de plataformas. En 2018, Portugal adoptó legislación relativa al transporte individual y

<sup>97</sup> Take Eat Easy (18 de noviembre de 2018, asunto 17-20.079) y Uber (4 de marzo de 2020, asunto 19-13.316).

<sup>98</sup> Regione Lazio, Legge Regionale 12 aprile 2019, n.º 4, disponible [en línea](#).

<sup>99</sup> L. 2 novembre 2019, n.º 128, Conversione in legge, con modificazioni, del decreto-legge 3 settembre 2019, n.º 101, disponible [en línea](#).

<sup>100</sup> Decisión de la autoridad de protección de datos italiana, disponible [en línea](#).

<sup>101</sup> Real Decreto-ley 9/2021, de 11 de mayo, disponible [en línea](#).

remunerado de pasajeros, estableciendo límites relativos a las horas de trabajo de los conductores<sup>102</sup>.

## **7.2 Un enfoque común de la UE**

A la luz de los enfoques nacionales que se están desarrollando para abordar los distintos retos vinculados al trabajo en plataformas, existe un riesgo de fragmentación entre las distintas iniciativas legislativas nacionales. La Comisión ha identificado varios retos en el trabajo en las plataformas y ha consultado a los interlocutores sociales europeos en dos fases sobre la necesidad de una iniciativa sobre el trabajo en las plataformas y su posible orientación. Los interlocutores sociales europeos coincidieron en los retos que debían abordarse, pero mantuvieron diferencias sobre la necesidad de tomar medidas concretas a nivel de la UE. Además, la Comisión mantuvo intercambios con muchas partes interesadas, mediante reuniones específicas y bilaterales con empresas de plataformas, asociaciones de trabajadores de plataformas, sindicatos, representantes de los Estados miembros, expertos de instituciones académicas y organizaciones internacionales y representantes de la sociedad civil<sup>103</sup>. La Comisión ha propuesto una directiva para mejorar las condiciones de trabajo de los trabajadores de plataformas en la UE, garantizando la correcta determinación de su situación laboral, promoviendo la transparencia, la equidad y la responsabilidad en la gestión algorítmica en el trabajo de las plataformas y mejorando la transparencia en el trabajo de las plataformas, también en el ámbito transfronterizo, fomentando al mismo tiempo condiciones para el crecimiento sostenible de las plataformas de trabajo digitales en la Unión.

## **8. Supervisión de la vigilancia digital**

La protección de datos y la privacidad son derechos fundamentales esenciales en la era digital. También son derechos «instrumentales» que posibilitan y aumentan la protección de otros derechos fundamentales que pueden verse afectados por la vigilancia estatal o privada, como la dignidad humana, la libertad de expresión, la libertad de pensamiento, de conciencia y de religión o la libertad de reunión, el derecho a un juicio justo y a un recurso efectivo o la no discriminación. El Reglamento General de Protección de Datos (RGPD), la Directiva sobre protección de datos en el ámbito penal y la Directiva sobre la privacidad y las comunicaciones electrónicas han situado a Europa a la cabeza en lo que respecta a la protección de los derechos fundamentales en línea. El aumento de la digitalización en todas las esferas de la vida plantea retos relacionados con la protección de los datos y con la vida privada y familiar. Otras leyes, como la Ley de Gobernanza de Datos, sobre la que se ha llegado recientemente a un acuerdo político entre los legisladores, tienen por objeto fomentar el surgimiento de una economía de datos sólida mediante la regulación de los servicios intermediarios de datos, el altruismo de datos y la reutilización de datos públicos protegidos, de acuerdo con el régimen de protección de datos.

<sup>102</sup> Lei n.º 45/2018 Regime jurídico da atividade de transporte individual e remunerado de passageiros em veículos descaracterizados a partir de plataforma eletrónica. Disponible [en línea](#).

<sup>103</sup> Véase el *Impact Assessment report accompanying the proposal for a Directive on improving working conditions in platform work* [«Informe de la evaluación de impacto que acompaña a la propuesta de Directiva sobre la mejora de las condiciones de trabajo en las plataformas digitales», documento en inglés] [SWD\(2021\) 396 final](#).

### **¿Cuál es la relación entre los derechos a la intimidad y a la protección de datos?**

Son derechos fundamentales independientes pero que se solapan, consagrados en el artículo 7 y el artículo 8 de la Carta de los Derechos Fundamentales.

- El respeto a la vida privada y familiar (intimidad) protege el ámbito privado frente a intrusiones ilícitas. Por ejemplo, en este derecho se protegen la confidencialidad de las comunicaciones interpersonales, así como los dispositivos terminales electrónicos contra intrusiones no autorizadas.
- La «protección de los datos» solo es aplicable cuando los datos personales se tratan por medios automatizados o de un modo estructurado manualmente. El derecho no está limitado a la información relativa al ámbito privado de la persona sino que abarca cualquier dato personal de esta, también relativo a su vida profesional. Los principios fundamentales de la protección de los datos son la transparencia, la licitud y la lealtad de las actividades de tratamiento de datos personales. La protección de datos también implica que los datos personales solamente deben tratarse con fines específicos y explícitos, deben ser precisos, limitarse a lo necesario y mantenerse seguros y utilizarse únicamente mientras sean necesarios.

En la práctica, el sólido marco jurídico de la UE se pone constantemente a prueba. Las organizaciones de consumidores y las OSC centradas en los derechos fundamentales se quejan de la falta de aplicación de la ley en los casos de infracción del RGPD<sup>104</sup>. En los últimos años, la UE y los Estados miembros han adoptado una serie de medidas para salvaguardar la seguridad pública y hacer frente a los retos de seguridad que plantea el uso de la tecnología moderna. En este contexto, las organizaciones de la sociedad civil manifiestan su preocupación sobre la proporcionalidad de las políticas de vigilancia y seguridad, por ejemplo, en relación con la vigilancia de las fronteras<sup>105</sup> o en el caso de legislación promulgada o propuesta que permita a las autoridades escanear comunicaciones privadas con fines de seguridad<sup>106</sup>. Las organizaciones sectoriales y de la sociedad civil también han expresado su preocupación por lo que perciben como tentativas de debilitación del cifrado por parte de los Estados miembros<sup>107</sup>.

Las autoridades de protección de datos y los tribunales nacionales garantizan una tutela judicial efectiva cuando las medidas de vigilancia, tanto por parte de agentes privados como

<sup>104</sup> Por ejemplo, [https://www.beuc.eu/publications/beuc-x-2020-074\\_two\\_years\\_of\\_the\\_gdpr\\_a\\_cross-border\\_data\\_protection\\_enforcement\\_case\\_from\\_a\\_consumer\\_perspective.pdf](https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf) y <https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf>.

<sup>105</sup> <https://edri.org/our-work/technological-testing-grounds-border-tech-is-experimenting-with-peoples-lives/>.

<sup>106</sup> Véase, por ejemplo: <https://edri.org/wp-content/uploads/2020/10/20201020-EDRI-Open-letter-CSAM-and-encryption-FINAL.pdf> o <https://netzpolitik.org/2021/finfisher-wir-verklagen-das-bka-auf-den-staatstrojaner-vertrag/>.

<sup>107</sup> Véase, por ejemplo: <https://www.statewatch.org/news/2020/november/eu-council-set-to-adopt-declaration-against-encryption/> o [https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf?utm\\_source=dsms-](https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf?utm_source=dsms-) o [https://www.bitkom.org/sites/default/files/2020-12/201211\\_pp\\_bitkom\\_grundsatzerklaerung-verschlussselung\\_0.pdf](https://www.bitkom.org/sites/default/files/2020-12/201211_pp_bitkom_grundsatzerklaerung-verschlussselung_0.pdf) [auto&utm\\_medium=email&utm\\_campaign=Encryption%3A+Council+adopts+resolution+on+security+through+encryption+and+security+despite+encryption.](https://www.bitkom.org/sites/default/files/2020-12/201211_pp_bitkom_grundsatzerklaerung-verschlussselung_0.pdf)

públicos, constituyen una vulneración de los derechos fundamentales. A continuación se exponen algunos ejemplos: i) la decisión de la autoridad de protección de datos de Suecia relativa al uso de cámaras corporales por parte los revisores en el transporte público de Estocolmo, que criticaba la falta de transparencia y una recopilación de datos excesiva, dio lugar a una multa de 16,1 millones SEK<sup>108</sup>; ii) el *Conseil d'Etat* (Consejo de Estado) de Francia decidió que la policía tenía que dejar de utilizar drones para comprobar si se respetaban las normas de distanciamiento social, ya que dichos aparatos tenían capacidad técnica para identificar a particulares y su uso no era conforme con la ley de protección de datos<sup>109</sup>.

La propuesta de Marco para una Identidad Digital Europea ofrecerá a todos los ciudadanos de la UE y residentes de forma voluntaria una cartera digital segura y fiable bajo el control total del usuario, como un facilitador «autosoberano» que permite el acceso a servicios públicos y privados digitales y a compartir una variedad de atributos y credenciales<sup>110</sup>.

### 8.1 Conservación de los datos

Desde 2014, el Tribunal de Justicia de la UE ha concluido que las leyes nacionales que establecen la conservación de metadatos de telecomunicaciones (datos de tráfico y de localización) con fines policiales y de inteligencia no cumplen los requisitos del Derecho de la UE. El Tribunal ha considerado que estas leyes nacionales constituyen una injerencia grave y desproporcionada en los derechos a la privacidad y la protección de datos, ya que los metadatos de las comunicaciones pueden revelar información sobre un número significativo de aspectos de la vida privada de las personas en cuestión<sup>111</sup>. Aunque reconoce que las medidas de conservación de datos persiguen objetivos de interés público legítimo, el Tribunal de Justicia había concluido a menudo que, salvo algunas excepciones<sup>112</sup>, el Derecho de la UE se opone a las medidas legislativas que impongan a los proveedores de servicios de comunicaciones electrónicas, con carácter preventivo, una obligación que exija la conservación generalizada e indiferenciada de los datos de tráfico y de localización. En **la estrategia de la UE contra la delincuencia organizada 2021-2025** de 14 de abril de 2021, la Comisión anunció que analizará y planteará posibles estrategias, conforme a las sentencias del Tribunal, que respondan a las necesidades policiales y judiciales de un modo que sea útil desde el punto de vista operativo, técnicamente posible y jurídicamente correcto, lo que incluye respetar plenamente los derechos fundamentales, y que consultará a los Estados miembros antes de que concluya junio de 2021. La Comisión ha entablado actualmente un

<sup>108</sup> [https://edpb.europa.eu/news/national-news/2021/unlawful-use-body-cams-stockholms-public-transport\\_en;https://www.imy.se/tillsyner/storstockholms-lokaltrafik-sl/](https://edpb.europa.eu/news/national-news/2021/unlawful-use-body-cams-stockholms-public-transport_en;https://www.imy.se/tillsyner/storstockholms-lokaltrafik-sl/).

<sup>109</sup> <https://www.conseil-etat.fr/actualites/actualites/le-conseil-d-etat-ordonne-a-l-etat-de-cesser-immediatement-la-surveillance-par-drone-du-respect-des-regles-sanitaires>.

<sup>110</sup> [COM\(2021\)281 final](#).

<sup>111</sup> Véase, por ejemplo, la sentencia del Tribunal de Justicia de 2 de marzo de 2021, Prokuratuur, asunto C-746/18, ECLI:EU:C:2021:152.

<sup>112</sup> Véase la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, asuntos acumulados C-511/18, C-512/18 y C-520/18, ECLI:EU:C:2020:791, en la que el Tribunal permitió la conservación generalizada de los datos de tráfico y de localización para fines de protección frente a amenazas graves contra la seguridad pública, de las direcciones IP atribuidas al origen de una comunicación para luchar contra delitos graves, y de los datos relativos a la identidad civil para combatir la delincuencia en general.

proceso de consulta y analizará detenidamente los resultados de dicha consulta antes de tomar una decisión acerca del posible camino a seguir.

## **8.2 Cifrado**

El cifrado es esencial para proteger los derechos fundamentales, así como los sistemas y las transacciones. La legislación de la UE contempla el cifrado como una medida para garantizar la protección de derechos fundamentales como la privacidad, la protección de datos personales<sup>113</sup> y la libertad de expresión, así como para garantizar la ciberseguridad<sup>114</sup>. Por otra parte, el cifrado también es importante para la protección de los secretos empresariales y ayuda por ende a las personas a disfrutar de su derecho a la libertad de empresa. Desde el inicio de la pandemia de COVID-19, junto con el aumento del uso de las herramientas digitales en todos los ámbitos de la vida, se ha registrado un incremento del número de ciberataques. Estos ataques han causado importantes daños a empresas y servicios esenciales, incluidos los sistemas sanitarios, y han puesto en peligro los derechos de las personas, destacando la importancia del cifrado para los actores públicos y privados, ya que protege la confidencialidad de la información<sup>115</sup>.

Sin embargo, el uso del cifrado también permite a los delincuentes ocultar su identidad y oculta el contenido de sus comunicaciones. Atendiendo a los llamamientos de los Estados miembros, la Comisión se comprometió a estudiar soluciones técnicas, operativas y jurídicas equilibradas para estos retos. Estas soluciones deben mantener la eficacia del cifrado en cuanto a la protección de la privacidad y la seguridad de las comunicaciones y, al mismo tiempo, proporcionar una respuesta eficaz contra la delincuencia y el terrorismo<sup>116</sup>. La Comisión tiene intención de proponer, en 2022 «el camino a seguir para abordar la cuestión del acceso legal y focalizado a información cifrada en el contexto de investigaciones y acciones penales. Su propuesta deberá basarse en un análisis exhaustivo de cómo afrontarán los Estados miembros el cifrado, así como en un proceso en el que múltiples interesados estudien y valoren las opciones concretas (jurídicas, éticas y técnicas)»<sup>117</sup>.

## **8.3 Identificación biométrica remota**

Las normas de protección de datos de la UE prohíben, en principio, el tratamiento de datos biométricos dirigido a identificar de manera unívoca a una persona física, excepto en condiciones específicas<sup>118</sup>. El tratamiento de dichos datos debe tener una base jurídica

<sup>113</sup> Artículo 32, apartado 1, letra a), artículo 34, apartado 3, letra a), artículo 6, apartado 4, letra e), considerando 83 del Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE; considerando 60, artículo 31, apartado 3, letra a) de la Directiva sobre protección de datos en el ámbito penal; considerando 20, en relación con el artículo 4 de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas.

<sup>114</sup> Artículo 40, apartado 1, del Código Europeo de las Comunicaciones Electrónicas y considerando 96; considerando 40 del Reglamento (UE) 2019/881 («Reglamento sobre la Ciberseguridad»).

<sup>115</sup> El Comité Europeo de Protección de Datos (CEPD) adoptó sus Directrices 01/2021 sobre ejemplos relativos a la notificación de violaciones de la seguridad de los datos (versión para consulta pública). El cifrado desempeña un papel destacado en la reducción al mínimo de los riesgos de violación de la seguridad de los datos personales.

<sup>116</sup> El compromiso forma parte de la Estrategia para una Unión de la Seguridad de julio de 2020.

<sup>117</sup> Estrategia contra la delincuencia organizada, adoptada el 14 de abril de 2021.

<sup>118</sup> Véase el artículo 9 del Reglamento general de protección de datos y el artículo 10 de la Directiva sobre protección de datos en el ámbito penal. Con arreglo al RGPD, este tratamiento solo puede tener lugar en un

fundamentada en la legislación sobre protección de datos. Dicha base jurídica puede ser el consentimiento dado libremente de todas las personas afectadas, que es difícil de obtener en la práctica, o, alternatively, una ley de la UE o del Estado miembro que persiga un interés público esencial, como la prevención de una amenaza concreta e inmediata de un atentado terrorista. En el ámbito de la aplicación de la ley, el tratamiento será autorizado por ley. Cuando el tratamiento de los datos biométricos esté autorizado por la legislación, la legislación debe ser proporcional al objeto perseguido, respetar en lo esencial el derecho a la protección de datos y otros derechos fundamentales y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales de las personas afectadas.

Las OSC manifiestan preocupaciones ante el aumento de las tecnologías de identificación biométrica remota en varios Estados miembros y han pedido que se prohíba su uso<sup>119</sup>. El uso de sistemas biométricos remotos también ha sido criticado por el Supervisor Europeo de Protección de Datos, el Comité Europeo de Protección de Datos que congrega a las autoridades nacionales de protección de datos<sup>120</sup>, y otros organismos nacionales relacionados con los derechos fundamentales como el *Defenseur des Droits* en Francia<sup>121</sup>. Existen varios ejemplos de intervenciones de las autoridades de protección de datos para poner fin al uso de estas tecnologías, por ejemplo en una escuela en Francia, por parte de la policía en Suecia o por parte de un supermercado neerlandés<sup>122</sup>.

Además del marco existente, el Reglamento sobre la IA propuesto por la Comisión en abril de 2021 (véase el capítulo 4) incluye la prohibición de la identificación biométrica remota en tiempo real en espacios de acceso público y permite dicha identificación con fines de policiales, en tres casos concretos, y con la condición de que se apliquen salvaguardias específicas<sup>123</sup>.

---

número limitado de situaciones, principalmente por motivos de interés público significativo. En este caso, el tratamiento debe tener lugar sobre la base del Derecho nacional o de la UE, estar sujeto al requisito de proporcionalidad, al respeto del derecho a la protección de los datos y a garantías adecuadas. Con arreglo a la Directiva sobre protección de datos en el ámbito penal, para efectuar dicho tratamiento debe existir una necesidad estricta al respecto; en principio, una autorización de la legislación nacional o de la UE y garantías adecuadas.

<sup>119</sup> <https://edri.org/our-work/biometric-mass-surveillance-flourishes-in-germany-and-the-netherlands/> y <https://reclaimyourface.eu/>.

<sup>120</sup> [https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en).

<sup>121</sup> <https://www.defenseurdesdroits.fr/fr/communiqu%C3%A9-de-presse/2021/07/technologies-biometriques-la-defenseure-des-droits-appelle-au-respect>.

<sup>122</sup> Autoridad de protección de datos neerlandesa: [La autoridad de protección de datos neerlandesa emite una advertencia formal a un supermercado por su uso de la tecnología de reconocimiento facial](#) . Comité Europeo de Protección de Datos (europa.eu); La autoridad de protección de datos de Suecia multa a la policía por el uso de Clearview [Suecia multa a la policía por el uso ilegal de tecnología de reconocimiento facial - POLITICO Pro](#) La autoridad de protección de datos de Francia sobre el uso del reconocimiento biométrico en las escuelas: [La organización francesa de defensa de la privacidad declara ilegal una prueba de reconocimiento facial realizada en los institutos - POLITICO Pro](#).

<sup>123</sup> El artículo 5, apartado 1, letra d) de la propuesta establece que dicho uso debe ser estrictamente necesario para i) la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos; ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista; o iii) la detección de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en la orden de detención europea y para el que el Estado miembro implicado imponga una pena cuya duración máxima sea al menos de tres años. Su uso estará sujeto a la

## 8.4 Educación

Durante la pandemia de COVID-19, los centros de enseñanza y formación utilizaron distintas plataformas y herramientas en línea. El uso de soluciones comerciales de aprendizaje digital y de programas informáticos para vigilar a los alumnos durante la realización de exámenes a distancia, a las que se recurrió con frecuencia a modo de «soluciones rápidas», suscitó la preocupación de que su diseño pudiera aprovechar los datos de los usuarios para fines lucrativos y no para prácticas pedagógicas significativas.

El Centro de Educación Digital europeo, creado en el marco del Plan de Acción de Educación Digital, es un foro para la formulación de medidas que garanticen una colaboración intersectorial más robusta, promover el intercambio entre educadores, desarrollar medios para el aseguramiento de la calidad y garantizar el respeto de la protección de datos y la privacidad. Entre dichas medidas, la garantía de calidad y la confianza tendrán un papel crucial: la garantía de calidad para promover una comprensión compartida de los estándares de calidad clave para la educación digital; la confianza para garantizar el respeto de los principios clave relativos al uso de los datos, la ética y la privacidad. Estos dos elementos, además de impulsar el nivel de preparación digital de las instituciones europeas de educación y formación, pueden aumentar la cooperación para mejorar la calidad general de las soluciones digitales disponibles.

## 8.5 Salud

Numerosos aspectos de la **respuesta a la pandemia de COVID-19** conllevan el tratamiento de datos personales, incluidos datos sanitarios, que debido a su carácter sensible están sujetos a normas adicionales dentro del RGPD. El tratamiento de los datos personales debe limitarse a lo que sea necesario y proporcionado para el cumplimiento del objetivo y cumplir los requisitos del RGPD. En esto se ha basado el enfoque de la UE. Por ejemplo, la Comisión ha proporcionado orientaciones<sup>124</sup> a los Estados miembros sobre aplicaciones para la lucha contra la pandemia, y apoyó su trabajo en una caja de herramientas con requisitos relacionados con las aplicaciones<sup>125</sup> y especificaciones técnicas para la interoperabilidad<sup>126</sup> entre las aplicaciones nacionales de alerta en la UE. La Comisión ha creado una pasarela que permite enviar dichas alertas a través de las fronteras y entre las aplicaciones de los distintos Estados miembros. La Comisión también ha presentado una plataforma para el intercambio de datos de los formularios de localización de pasajeros<sup>127</sup> para contribuir al rastreo transfronterizo de contactos en contextos relacionados con el transporte. Como paso siguiente, se comprometió a proponer un marco jurídico de la UE para adoptar un enfoque coordinado sobre el registro, en la medida necesaria, de historiales de viajes recientes para frenar la propagación de la COVID-19, en base a la experiencia adquirida a partir de los formularios de localización de pasajeros.

---

autorización de un órgano judicial u otro organismo independiente y a los límites adecuados desde el punto de vista de la duración, el alcance geográfico y las bases de datos exploradas.

<sup>124</sup> [https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020XC0417\(08\)](https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020XC0417(08)).

<sup>125</sup> [https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19\\_apps\\_en.pdf](https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf).

<sup>126</sup> [https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing\\_mobileapps\\_guidelines\\_en.pdf](https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf).

<sup>127</sup> <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A02017D0253-20210726>.

Además, el Parlamento Europeo y el Consejo adoptaron, el 14 de junio de 2021, un Reglamento por el que se establece el sistema de certificados COVID digitales de la UE, que tiene por objeto facilitar la libre circulación durante la pandemia COVID-19<sup>128</sup>. Se creó una infraestructura para apoyar la expedición y verificación de los certificados de vacunación, de prueba diagnóstica y de recuperación, con el fin de agilizar la comprobación de las medidas de salud pública en los viajes (por ejemplo, para exenciones de los requisitos de cuarentena). Para facilitar su uso, los certificados están disponibles tanto en formato digital como en papel. En todos los casos, las categorías de datos y su tratamiento se limitan a lo necesario para el fin en cuestión, por ejemplo, quienes verifican los certificados tienen prohibido conservar su contenido tras la verificación. Además, el marco de confianza establecido para el certificado COVID digital de la UE garantiza que la verificación de todos los certificados pueda llevarse a cabo fuera de línea, sin que el emisor ni ningún otro tercero sean informados de la verificación. La transparencia siempre es fundamental, tanto para garantizar el cumplimiento legal de la Carta y la legislación aplicable, como para generar confianza y mantenerla. Los resultados demuestran que cuando las medidas se diseñan minuciosamente, la protección de datos es coherente y puede ayudar a promover la aceptación de medidas de salud pública eficaces y a garantizar que el marco de protección de datos de la UE ofrezca la flexibilidad necesaria.

La Comisión está preparando actualmente una propuesta legislativa sobre el **espacio europeo de datos sanitarios**, cuya adopción está prevista para principios de 2022. Dicho espacio tiene por objeto facilitar la prestación de servicios sanitarios digitales y promover el acceso a datos sanitarios para actividades reguladoras, de investigación, innovación y formulación de políticas, mejorando aún más el control que tienen las personas de sus datos personales. La iniciativa del espacio europeo de datos sanitarios cumplirá íntegramente las normas aplicables para la protección de datos de la UE.

## 8.6 Ejecución

Las autoridades nacionales de control competentes para la supervisión y ejecución de las normas de privacidad y protección de datos son la piedra angular del sistema de gobernanza para la protección de datos de la UE. Estas autoridades y órganos jurisdiccionales nacionales son responsables de la supervisión y ejecución de las normas contempladas en el RGPD, las leyes nacionales por las que se transpone la Directiva sobre protección de datos en el ámbito penal<sup>129</sup> y la Directiva sobre la privacidad y las comunicaciones electrónicas. Para la Comisión, uno de los objetivos principales es que los Estados miembros apliquen estas normas correcta y eficazmente. Los Estados miembros tienen la obligación, en virtud del Derecho de la UE, de garantizar que sus autoridades de protección de datos sean independientes y de asignarles recursos suficientes para el desempeño de sus tareas de supervisión<sup>130</sup>. La Comisión sigue los avances concernientes a la independencia de las labores, competencias y recursos de las autoridades de control y en el caso de que los Estados

<sup>128</sup> <http://data.europa.eu/eli/reg/2021/953/oj>, acompañado por <https://eur-lex.europa.eu/eli/reg/2021/954/oj>.

<sup>129</sup> <http://data.europa.eu/eli/dir/2016/680/2016-05-04>.

<sup>130</sup> Resumen del CEPD sobre los recursos puestos a disposición de las autoridades de protección de datos por parte de los Estados miembros y sobre las medidas de ejecución de las autoridades de protección de datos (documento en inglés), de 5 de agosto de 2021, publicado el 11 de agosto en [https://edpb.europa.eu/system/files/2021-08/edpb\\_report\\_2021\\_overviewsaressourcesandenforcement\\_v3\\_en\\_0.pdf](https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf).

miembros no cumplan las normas de la UE, se incoan procedimientos de infracción para garantizar la correcta aplicación de dichas normas.

Las autoridades de protección de datos trabajan conjuntamente con el Comité Europeo de Protección de Datos (CEPD) para garantizar la coherencia en la ejecución del RGPD, en particular en los casos transfronterizos. Después de tres años de aplicación del RGPD, la eficacia de su cooperación ha suscitado críticas<sup>131</sup> y el CEPD seguirá trabajando para aumentar la eficiencia<sup>132</sup>. La Comisión comparte la opinión del Consejo<sup>133</sup>, el Parlamento Europeo y el CEPD<sup>134</sup> de que ahora hay que centrar la atención en la mejora de la aplicación y en acciones que refuercen la ejecución de la legislación de la UE en materia de protección de datos.

## **8.7 Proteger los datos personales fuera de la UE**

Un aspecto esencial de la protección de los derechos fundamentales en un entorno en línea consiste en garantizar la continuidad de la protección de las personas cuando sus datos salen de la UE. Teniendo en cuenta que los datos personales viajan fácilmente a través de las fronteras en un mundo interconectado y los flujos de datos han pasado a formar parte integral del comercio, la cooperación en materia legislativa e incluso la interacción social, las protecciones garantizadas por el RGPD y la Directiva sobre protección de datos en el ámbito penal serán ineficaces si están limitadas al ámbito de la UE.

En ese contexto, la Comisión siguió trabajando en su ambiciosa agenda concebida para promover un alto nivel de protección cuando se realicen transferencias de datos de los europeos a terceros países, y, al mismo tiempo, facilitar los flujos de datos. Esto incluyó la colaboración con socios clave para alcanzar una «decisión de adecuación», que establece que un tercer país ofrece un nivel de protección de los datos «equivalente en lo esencial» al de la UE. Esto dio lugar a importantes resultados, como la adopción de dos decisiones de adecuación para el Reino Unido (en el marco del RGPD y de la Directiva sobre protección de datos en el ámbito penal) y la culminación de las conversaciones sobre adecuación con la República de Corea.

Además, tras la invalidación, por parte del Tribunal de Justicia, de la anterior decisión de idoneidad sobre el Escudo de Privacidad, la UE y los Estados Unidos han intensificado las negociaciones sobre un nuevo marco de privacidad UE-EE. UU. para las transferencias de datos transatlánticas que garantiza el pleno cumplimiento de la sentencia del Tribunal.

Además, en junio de 2020, la Comisión adoptó cláusulas contractuales tipo modernizadas para la transferencia de datos personales a un tercer país, que reflejan los nuevos requisitos establecidos en el RGPD y están adaptadas a las necesidades de la economía digital moderna. Son modelos de cláusulas de protección de datos que un exportador de datos y un importador de datos pueden, de forma voluntaria, incorporar a sus acuerdos contractuales (por ejemplo,

<sup>131</sup> Véase, por ejemplo, la resolución [2020/2717 (RSP)] del Parlamento Europeo.

<sup>132</sup> Estrategia 2021-2023 del CEPD, adoptada el 15 de diciembre de 2020, disponible en [edpb\\_strategy2021-2023\\_es.pdf \(europa.eu\)](https://edpb.europa.eu/strategy/2021-2023/es/pdf/europa.eu).

<sup>133</sup> Posición del Consejo y conclusiones acerca de la aplicación del Reglamento General de Protección de Datos (RGPD) – Adopción, 14994/1/19 REV 1, 19 de diciembre de 2019, disponible en [pdf \(europa.eu\)](https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32019D14994).

<sup>134</sup> Memoria anual 2020 del CEPD, 2 de junio de 2021, disponible en [Memoria anual 2020 del CEPD | Comité Europeo de Protección de Datos \(europa.eu\)](https://edpb.europa.eu/strategy/2021-2023/es/pdf/europa.eu).

un contrato de servicios que requiera la transferencia de datos personales) y que tienen por objeto garantizar unas salvaguardias de protección de datos adecuadas.

La Comisión también sigue participando en la iniciativa «Data Free Flow with Trust» (Libre circulación de datos basada en la confianza), puesta en marcha por Japón en 2019, y refrendada posteriormente por el G20 y el G7. Un elemento central de este concepto, que se está debatiendo actualmente en el seno de la OCDE, con la participación activa de la UE y sus Estados miembros, consiste en trazar una línea entre el acceso legítimo por parte de las autoridades públicas, con limitaciones y salvaguardias apropiadas, y la vigilancia abusiva por parte del Estado.

## **9. Unir fuerzas para que la era digital sea una oportunidad para los derechos fundamentales**

Si se tienen en cuentas los retos interrelacionados y las correspondientes medidas que se analizan en este informe, no cabe duda de que la UE y sus Estados miembros están comprometidos a proteger y promover los derechos fundamentales en la era digital y están trabajando juntos para identificar la forma más adecuada de hacerlo. Los ejemplos mencionados en los capítulos anteriores representan algunas de muchas oportunidades para aprender unos de otros y configurar los cambios derivados de la transición digital de forma positiva.

La Comisión utiliza numerosas herramientas para garantizar el respeto de los derechos consagrados en la Carta —tanto en el diseño de sus iniciativas legislativas y políticas como en la ejecución del Derecho de la UE—. En particular, la Comisión evaluará exhaustivamente los efectos en los derechos fundamentales y la intención de equilibrar esos efectos en las nuevas iniciativas que emprenda en 2022, así como propuestas legislativas relativas a:

- un derecho a la reparación,
- ciberresiliencia,
- servicios digitales de movilidad,
- pago inmediato,
- acceso recíproco a la información relacionada con la seguridad para los agentes de primera línea entre la UE y terceros países clave,
- una Ley sobre la libertad de los medios de comunicación y
- normas vinculantes para los organismos de igualdad.

Además, en el contexto de la Década Digital, la Comisión propondrá incluir un conjunto de principios digitales en una declaración solemne interinstitucional entre la Comisión Europea, el Parlamento Europeo y el Consejo. Esta declaración informará a los usuarios y guiará a los responsables políticos y a los operadores digitales sobre la vía europea hacia la transformación digital.

La Comisión insta al Parlamento Europeo, al Consejo y a los Estados miembros a que utilicen el presente Informe Anual sobre la aplicación de la Carta de los Derechos Fundamentales para participar en intercambios relativos a los retos y las oportunidades para la protección de estos derechos en la era digital. Acoge con satisfacción el compromiso del Consejo de

intercambiar impresiones sobre la base de los informes de la Comisión<sup>135</sup> y también acogerá con satisfacción un debate en el Parlamento Europeo. En particular, estos intercambios podrían ayudar a abordar mejor los retos futuros, concretamente la lucha contra la incitación al odio y la desinformación, la forma de garantizar los controles y equilibrios en las medidas de vigilancia y, en términos más generales, la forma de aplicar de manera efectiva las leyes para la protección de los derechos fundamentales en el entorno digital. Estos intercambios pueden ayudar a enmarcar la evolución de las políticas de la UE de un modo constructivo y beneficioso.

Estos esfuerzos conjuntos para hacer efectiva la Carta en la era digital, junto con el Plan de Acción para la Democracia Europea<sup>136</sup> y el Mecanismo del Estado de Derecho<sup>137</sup>, ilustran el compromiso de la UE para promover y proteger los valores en los que está fundamentada.

<sup>135</sup> [Conclusiones del Consejo](#) sobre el refuerzo de la aplicación de la Carta de los Derechos Fundamentales en la Unión Europea, de 8 de marzo de 2021, apartado 26.

<sup>136</sup> Comunicación de la Comisión sobre el Plan de Acción de Educación Digital, [COM \(2020\)790](#).

<sup>137</sup> [https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism\\_es](https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism_es).