

Francisco Javier Arrieta Idiakez  
Dirección y coordinación

# Consecuencias jurídicas de la transición digital. Especial mención al empleo

LABORAL



**CONSECUENCIAS JURÍDICAS  
DE LA TRANSICIÓN DIGITAL.  
ESPECIAL MENCIÓN AL EMPLEO**

## CONSEJO EDITORIAL

MIGUEL ÁNGEL COLLADO YURRITA

JOAN EGEA FERNÁNDEZ

JOSÉ IGNACIO GARCÍA NINET

LUIS PRIETO SANCHÍS

FRANCISCO RAMOS MÉNDEZ

SIXTO SÁNCHEZ LORENZO

JESÚS-MARÍA SILVA SÁNCHEZ

JOAN MANUEL TRAYTER JIMÉNEZ

ISABEL FERNÁNDEZ TORRES

BELÉN NOGUERA DE LA MUELA

RICARDO ROBLES PLANAS

JUAN JOSÉ TRIGÁS RODRÍGUEZ

*Director de publicaciones*

# **CONSECUENCIAS JURÍDICAS DE LA TRANSICIÓN DIGITAL. ESPECIAL MENCIÓN AL EMPLEO**

**Francisco Javier Arrieta Idiakez**

Dirección y coordinación

AUTORES

**Vega María Arnáez Arce**

**Francisco Javier Arrieta Idiakez**

**Alberto Atxabal Rada**

**Enrique Gadea Soler**

**Eba Gaminde Egia**

**Santiago Larrazabal Basañez**

**Gonzalo Martínez Etxeberria**

**Colección: Atelier Laboral**

**Director:**

**José Ignacio García Ninet**

*Catedrático de Derecho del Trabajo y de la Seguridad Social*



**EUSKO JAURLARITZA  
GOBIERNO VASCO**

HEZKUNTZA SAILA  
DEPARTAMENTO DE EDUCACIÓN

Reservados todos los derechos. De conformidad con lo dispuesto en los arts. 270, 271 y 272 del Código Penal vigente, podrá ser castigado con pena de multa y privación de libertad quien reproducere, plagiar, distribuyere o comunicare públicamente, en todo o en parte, una obra literaria, artística o científica, fijada en cualquier tipo de soporte, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

© 2025 Los autores

© 2025 Atelier

Santa Dorotea 8, 08004 Barcelona

e-mail: [atelier@atelierlibros.es](mailto:atelier@atelierlibros.es)

[www.atelierlibrosjuridicos.com](http://www.atelierlibrosjuridicos.com)

Tel. 93 295 45 60

I.S.B.N.: 978-84-19773-89-0

Depósito legal: B 14802-2025

Diseño y composición: Addenda, Pau Claris 92, 08010 Barcelona

[www.addenda.es](http://www.addenda.es)

Impresión: Safekat

## Capítulo 5

# **NUEVOS RETOS PARA LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES EN LA TRANSICIÓN DEL ENTORNO ANALÓGICO AL ENTORNO DIGITAL**

*Santiago Larrazabal Basañez*

Catedrático de Derecho Constitucional

Universidad de Deusto

## **1. LOS RETOS DEL NUEVO «CONSTITUCIONALISMO DIGITAL»**

La lucha por el Estado de Derecho<sup>1</sup>, es una batalla que no cesa a lo largo de los tiempos y es uno de los objetivos irrenunciables de un sistema constitucional democrático. En cada momento, en cada situación, en cada contexto histórico, siempre se presentan amenazas para el ejercicio de los derechos fundamentales. También en la nueva generación digital que se avecina surgen nuevos retos para la protección de los derechos y libertades fundamentales, para la salvaguarda de una auténtica democracia, de una democracia de calidad<sup>2</sup> y nos encontramos ahora en un momento decisivo, en un momento de transición: el momento de dar el salto del entorno analógico al entorno digital.<sup>3</sup> En el ámbito del derecho constitucional, y cuando hablamos de derechos, hemos venido distinguiendo

---

1. LUCAS VERDÚ, 1975.

2. SÁNCHEZ NAVARRO / FERNÁNDEZ RIVEIRA, 2023

3. QUERALT JIMÉNEZ, 2021: 217 y ss.

hasta ahora entre distintas generaciones de derechos: derechos civiles y políticos, derechos económicos y sociales, los denominados derechos de «tercera generación», y ahora aparece una nueva generación: la cuarta, la relativa a los derechos digitales<sup>4</sup>.

Se trata, en efecto, de un cambio de marco y de paradigma, pero los retos y los peligros para la efectividad de los derechos siguen existiendo, algunos son los de siempre y otros son nuevos. Porque los derechos «clásicos» han de ser adaptados ahora al marco digital<sup>5</sup>, y así seguimos hablando, por ejemplo, de derecho al honor, del derecho a la educación o de la libertad de expresión o de información, pero ahora no solamente en su marco clásico, el que hemos conocido hasta ahora («analógico», por utilizar una imagen más gráfica), sino también en un nuevo marco, en un nuevo contexto: el «digital». Y además de los derechos de siempre, tanto en el ámbito analógico como digital, van surgiendo derechos nuevos, directamente vinculados con el ámbito digital, como, por ejemplo, uno de los más famosos de entre ellos, el denominado *derecho al olvido*. Pero unos y otros, en un ámbito y en otro, no solo deben ser reconocidos sino también eficazmente protegidos en lo que algunos autores han denominado un nuevo «paradigma constitucional»<sup>6</sup> y, por ende, la teoría constitucional debe ofrecer nuevos instrumentos para hacer frente a la transformación digital y a las nuevas tecnologías<sup>7</sup>, para que, en definitiva, podamos seguir hablando de un verdadero Estado social y democrático de Derecho y por eso también, algunos autores, han empezado a hablar ya de «constitucionalismo digital»<sup>8</sup>.

Como es lógico, el Derecho va por detrás de la realidad que tiene que regular, pero a veces el retraso en regular jurídicamente los fenómenos, hace que la normativa nazca ya obsoleta. En materia de derechos digitales nos puede ocurrir esto si no «espabilamos». Ya nos ocurrió con la regulación de las redes sociales, y corremos el riesgo de que vuelva a ocurrirnos con los derechos digitales. Como han escrito RECHE TELLO y TUR AUSINA<sup>9</sup>, aludiendo a la paradoja de Collingridge respecto al control social de la tecnología, en las primeras fases de implantación de las nuevas tecnologías, no sería difícil ponerles ciertos límites por parte del poder público, pero como no tenemos el conocimiento necesario para regularlas, no lo hacemos y cuando posteriormente tenemos un conocimiento mayor del tema, la tecnología ha avanzado tanto que la situación creada se nos escapa de las manos y la regulación llega tarde y es ineficaz. Mientras en un primer momento, los Estados tenían más margen de maniobra y se podían

---

4. RALLO LOMBARTE, 2017 y 2020.

5. Sobre estas materias, conviene consultar las distintas colaboraciones incluidas en QUADRA SALCEDO / PIÑAR MAÑAS (dirs.), 2018. En el ámbito de la Administración pública, pueden consultarse las colaboraciones incluidas en MEDINA GUERRERO (coord.), 2023.

6. SARRIÓN ESTEVE, 2023.

7. RECHE TELLO / TUR AUSINA, 2022.

8. POLLICINO, 2021; DE GREGORIO, 2022; BALAGUER CALLEJÓN, 2022; BALAGUER CALLEJÓN / SARLET, 2023.

9. RECHE TELLO / TUR AUSINA, 2022: 15.

haber adoptado políticas públicas preventivas para encauzar la gestión de estas nuevas tecnologías, ahora el fenómeno ha superado el marco de los Estados y se necesitan políticas supranacionales que establezcan barreras reguladoras, sobre todo para los grandes operadores digitales, si queremos seguir protegiendo eficazmente y no sólo nominalmente los derechos fundamentales. Como dicen las autoras, y estoy plenamente de acuerdo con ello, necesitamos una nueva «gobernanza constitucional-digital».

Eso quiere decir que, si el reto es global, las medidas deberían ser globales. Por poner un ejemplo reciente: si, como hizo Italia, se decide bloquear un sistema de chat basado en inteligencia artificial porque se considera que no respeta la normativa de protección de datos, la medida adoptada en un país tiene efectos muy limitados y debe ser tomada a una escala mucho más amplia. En todo caso, tampoco podemos ser ingenuos y negarnos a aceptar la realidad porque los avances tecnológicos son irreversibles, una vez producidos no se puede volver a la situación anterior, pero tampoco podemos encogernos de hombros y no hacer nada, con la excusa de que nada de lo que lo hagamos tendrá efectos prácticos. Se pueden y se deben tomar medidas de control y obligar a los operadores globales a respetar los derechos digitales y la normativa que los regula. En cualquier caso, creo que es mejor hacer algo que no hacer nada y que no nos ocurra de nuevo lo que nos ocurrió al principio con las nuevas tecnologías de la información y la comunicación. Hay que ser mucho más rápidos y, como se dice ahora, más resilientes. Pero las medidas deberían ser también globales. Ello nos llevará tiempo y requerirá un consenso que no siempre es fácil de alcanzar, entre otras cosas porque las perspectivas de las distintas culturas jurídicas no siempre son coincidentes.

Veamos un ejemplo de ello, en relación con la libertad de expresión e Internet, siguiendo la exposición de POLLICINO: en la mentalidad norteamericana, claramente expuesta por el Tribunal Supremo de los Estados Unidos en el caso *Reno* en 1997, el Tribunal considera que la protección de la libertad de expresión, amparada por la Primera Enmienda de la Constitución de los Estados Unidos debe ser extendida al ámbito digital con la mayor amplitud, considerando a Internet como un nuevo canal para promover el «libre mercado de ideas»<sup>10</sup>. Frente a esta posición, la jurisprudencia europea, simbolizada por la Sentencia del Tribunal Europeo de Derechos Humanos en el *asunto Consejo Editorial Pravoye Delo y Shtekel contra Ucrania* de 2011<sup>11</sup>, hace incapié en que la comunica-

---

10. *Reno v. American Civil Liberties Union*, 521 US 844 (1997). Y este era un caso especialmente delicado pues hacía referencia a la Ley de Decencia en las Comunicaciones (Communications Decency Act —CDA—) de 1996, que fue dictada para proteger a los menores de 18 de años de la transmisión de mensajes obscenos o indecentes.

11. La Sentencia del Tribunal Europeo de Derechos Humanos en el *asunto Consejo Editorial Pravoye Delo y Shtekel contra Ucrania* de 5 de mayo de 2011 (ECLI:CE:ECHR:2011:0505J UD003301405), dice en su párrafo n° 63 que: «Es cierto que Internet es una herramienta de información y de comunicación que se distingue particularmente de la prensa escrita, principalmente en cuanto a su capacidad para almacenar y difundir información. Esta red electrónica, que comunica

ción *online* y su contenido corren más riesgo que la prensa de atentar contra el ejercicio y disfrute de los derechos y libertades fundamentales, en particular el derecho al respeto de la vida privada. Como bien ha explicado POLLICINO, «es evidente que el Tribunal Europeo de Derechos Humanos, sin negar el valor añadido de la tecnología digital, pone el énfasis menos en los beneficios de la mayor expansión en el ejercicio de la libertad de expresión on line y más en los riesgos que tal expansión podría ocasionar en la protección de efectiva de los derechos y libertades que pueden entrar en conflicto. En otras palabras, los dos Tribunales parecen trabajar sobre bases de presunciones opuestas. Mientras el Tribunal Supremo de los Estados Unidos presume que la regulación de contenidos no genera mayores beneficios para la libertad, el Tribunal Europeo de Derechos Humanos, que es más renuente, considera el entorno digital como una amenaza a los derechos y libertades por lo que subraya la necesidad de adoptar medidas proporcionadas y necesarias para limitar el ejercicio de la libertad de expresión»<sup>12</sup>. En su opinión, el auge de Internet ha supuesto el incremento de la protección del derecho a la libertad de expresión en Estados Unidos, mientras que, por el contrario, en Europa ha supuesto la consolidación y emancipación del derecho a la protección de datos en la Unión Europea.<sup>13</sup> Y no le falta razón porque en los últimos tiempos los enfoques del Tribunal Europeo de Derechos Humanos (por ejemplo, en la reciente Sentencia de la Gran Sala de 15 de mayo de 2023<sup>14</sup>, asunto *Sánchez contra Francia*) y del Tribunal Supremo de los Estados Unidos (por ejemplo, las Sentencias de 18 de mayo de 2023, *Gonzalez v. Google LLC*<sup>15</sup> y *Twitter, Inc. v. Taamneh*<sup>16</sup>), son completamente divergentes, como bien ha puesto de manifiesto COTINO HUESO<sup>17</sup>.

*Aunque las dos visiones no son antitéticas, utilizan perspectivas distintas. En este sentido, es posible que, como ha escrito POLLICINO*<sup>18</sup>, en la Unión Europea pequemos de cierto eurocentrismo, creamos que lo que se dice en Europa es directamente exportable a todo el mundo y que todos los demás deben seguir-

---

a millones de usuarios por todo el mundo, no es y posiblemente nunca sea sometida a las mismas reglas ni al mismo control. Seguramente, la comunicación online y su contenido corren más riesgo que la prensa de atentar contra el ejercicio y disfrute de los derechos y libertades fundamentales, en particular el derecho al respeto de la vida privada. Así mismo, la reproducción de materiales sacados de la prensa escrita y de material publicado en Internet puede ser sometido a un régimen diferente. Las reglas que regulan la reproducción del segundo deben ajustarse en función de las características particulares de la tecnología de manera que pueda asegurar la protección y la promoción de los derechos y libertades en causa».

12. POLLICINO, 2021: 94-95.

13. POLLICINO, 2021: 208.

14. Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 15 de mayo de 2023, asunto *Sánchez contra Francia*. ECLI:CE:ECHR:2023:0515JUD004558115.

15. [https://www.supremecourt.gov/opinions/22pdf/21-1333\\_6j7a.pdf](https://www.supremecourt.gov/opinions/22pdf/21-1333_6j7a.pdf) (última consulta, 24 de julio de 2023)

16. [https://www.supremecourt.gov/opinions/22pdf/21-1496\\_d18f.pdf](https://www.supremecourt.gov/opinions/22pdf/21-1496_d18f.pdf) (última consulta, 24 de julio de 2023).

17. COTINO HUESO, 2023 b.

18. POLLICINO, 2021: 144, 146, 183.

nos en nuestras decisiones. Pero ya vemos que no todo el mundo comparte necesariamente nuestra perspectiva, y hay que ser humildes, sobre todo teniendo en cuenta el modesto tamaño de la Unión Europea comparado con el poder de las grandes empresas tecnológicas del sector y de algunos de los países que son líderes en estas nuevas tecnologías. Hay que tener en cuenta que, visto desde fuera de la Unión Europea, hay ciertas reticencias a la normativa y jurisprudencia europeas en estas materias, porque hay quien piensa que se está creando un «superderecho» fundamental a la privacidad y que se está extendiendo su ámbito territorial de aplicación más allá de la Unión Europea, con ciertas tentaciones de aplicación extraterritorial.

Es lo que este autor denomina el «proceso de europeización de Internet» y puede que tenga razón en que la naturaleza internacional del asunto sea difícilmente compatible con una protección regional, como la que puede brindar la Unión Europea, aunque el proceso esté inspirado por el loable propósito de incrementar la protección de los derechos, lo que podría conducir a una cierta fragmentación o como él dice «balcanización» de los instrumentos de protección frente a los retos que plantea Internet, pero aún así, como dice el refrán, «lo mejor es enemigo de lo bueno» y será mejor hacer algo que no hacer nada y además, habría que empezar a hacerlo rápidamente para que, si se me permite la expresión, «no nos vuelva a pillar el toro».

Y en este sentido, hay que reconocer que los Tribunales y la jurisprudencia han ido por delante del legislador, en particular los Tribunales europeos, que han demostrado una gran versatilidad a la hora de identificar posibles conflictos en la protección de los derechos fundamentales frente las nuevas tecnologías y de tomar medidas para evitarlos. Pondré dos ejemplos al respecto: uno en el ámbito de la Unión Europea y otro en el ámbito interno de un país miembro de la Unión Europea.

Respecto al primer ejemplo, el caso más claro es, en el ámbito del derecho de la Unión Europea, el papel que jugó el Tribunal de Justicia de Luxemburgo, quien en la práctica «creó» el denominado «derecho al olvido», en su Sentencia de 13 de mayo de 2014, en el *caso Google Spain S.L. y Google Inc. contra la Agencia Española de Protección de Datos y Mario Costeja González*<sup>19</sup> y sólo después de ella, la Unión Europea, directamente influida por esta Sentencia dictó el muy relevante Reglamento (UE) 2016/679, de 27 de abril de 2016 de protección de datos, asuntos a los que me referiré más adelante. El segundo ejemplo para comprobar el activismo de los Tribunales nacionales en estas materias, lo constituye la reciente Sentencia del Tribunal Constitucional alemán de 16 de febrero de 2023<sup>20</sup>, que declara inconstitucionales dos leyes de los Länder de Hesse y Hamburgo, que permitían utilizar bases de datos policiales en una plataforma

---

19. Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, en el *caso Google Spain S.L. y Google Inc. contra la Agencia Española de Protección de Datos y Mario Costeja González*, Asunto C-131/12. ECLI:EU:C:2014:317.

20. Sentencia del Tribunal Constitucional alemán (1ª Cámara), de 16 de febrero de 2023 (1 BvR 1547/19, 1 y BvR 2634/20).

para el análisis de datos (Hesse), o en una evaluación de datos (Hamburgo), para combatir determinados delitos o evitar amenazas y daños relevantes, normativa que, como ha escrito COTINO HUESO<sup>21</sup>, refuerza la protección contra el tratamiento automatizado de datos y prohíbe la utilización de sistemas de autoaprendizaje en estos casos.

Dejando a un lado por un momento la perspectiva europea, y enfocado el tema desde el punto de vista del derecho constitucional clásico interno, el de cada país, el reto es también de una gran envergadura.<sup>22</sup> ¿Es suficiente la actual protección constitucional de los derechos fundamentales «clásicos» en el marco digital y de los nuevos derechos digitales que se van creando o tenemos que buscar nuevos caminos para su efectiva protección? Hay algunos autores que defienden que, antes de reescribir nuevas normas constitucionales, todavía hay margen para, por vía de interpretación, aplicar las libertades constitucionales a los fenómenos de la tecnología informática.<sup>23</sup> Puede que aún no hayamos agotado el margen de interpretación, pero antes o después tendremos que entrar en la dinámica de la reforma constitucional y si ello no se ve posible a corto plazo, como en el caso español, al que me referiré más adelante, habrá que ir adoptando normativa específica, aún sabiendo que su cobertura constitucional, tal y como está redactada la Constitucional española hoy en día, resulta un tanto endeble.

Pero es que, además, la tecnología no nos da tregua. Ya no solo se trata de los derechos clásicos en «soporte digital», y de los nuevos derechos digitales, es que ahora tenemos que ofrecer también algún tipo de regulación a los derechos fundamentales en el ámbito de la Inteligencia Artificial<sup>24</sup>. En este ámbito teníamos importantes declaraciones y textos de *soft law*, jurídicamente no vinculantes<sup>25</sup> y, por fin, hemos dado el paso de la promulgación de normas jurídicas

---

21. COTINO HUESO, 2023 a.

22. Sobre estas cuestiones, pueden consultarse: AGUILAR CALAHORRO, 2022; ARCE JIMÉNEZ, 2022; BALAGUER CALLEJÓN F., 2021 a y b; BARRIO ANDRÉS, 2022; HOFFMANN-RIEM, 2022; LLANO ALONSO / GARRIDO MARTÍN, 2021; MADRID PARRA, 2022; SÁNCHEZ BARRILAO, 2016: 225 y ss.; PEREA ORTEGA, 2020; RODRÍGUEZ AYUSO, 2022; VALLS PRIETO, 2018; VALPUESTA GASTAMINZA / HERNÁNDEZ PEÑA, 2021.

23. FROSINI, 2022: 46 y ss.

24. Sobre esta materia, pueden consultarse, por ejemplo, y entre las publicaciones más recientes: el número monográfico de la Revista El Crónista del Estado Social y Democrático de Derecho, n° 100 (2022) o PRESNO LINERA, 2023; REBOLLO DELGADO, 2023; BALAGUER CALLEJÓN Y COTINO HUESO, 2023; SIMÓN CASTELLANO, 2023.

25. Por ejemplo, por destacar algunos: la Declaración de Toronto, las Directrices Universales para la Inteligencia Artificial aprobadas por The Public Voice, la Declaración sobre Ética y Protección de Datos en la Inteligencia Artificial de la Conferencia Internacional de Instituciones dedicadas a la Protección de Datos y la Privacidad, el estudio *Artificial Intelligence: the global landscape of ethics guidelines*, *Health Ethics & Policy Lab*, de la Escuela Politécnica Federal de Zurich de 2019. En el ámbito del Consejo de Europa, la Recomendación del Comité de Ministros a los Estados miembros sobre los impactos de los sistemas algorítmicos en los derechos humanos, de 8 de abril de 2020. En el ámbito de la Unión Europea, el Informe de 2021 de la agencia de los Derechos Fundamentales de la Unión Europea (FRA) sobre Inteligencia Artificial y Derechos Fundamentales, y en ámbito español, la

vinculantes (*hard law*), tras los sucesivos pronunciamientos de las instituciones europeas en materia de inteligencia artificial<sup>26</sup>. En efecto, ya tenemos Reglamento de la Unión Europea en materia de Inteligencia Artificial<sup>27</sup>. Los retos son enormes, y como han escrito RECHE TELLO y TUR AUSINA<sup>28</sup>, hay que poner el foco de atención sobre las aplicaciones actuales de la Inteligencia Artificial en el ámbito judicial, del derecho a la tutela judicial efectiva, de la libertad personal, del sistema electoral, del derecho a la participación política, pero también en la vigilancia masiva y el intercambio de datos biométricos y personales sensibles, las posibles discriminaciones provocadas por sistemas automatizados de compañías aseguradoras o bancarias que excluyen a personas del acceso a servicios esenciales como la vivienda, el empleo, etc.; los algoritmos de selección de personal y la discriminación por razón de género. Y ¿qué decir de los «neuroderechos»? Este es un campo totalmente nuevo. Como ocurre con la Inteligencia Artificial, convendría abordar su regulación a escala internacional (incorporándolos a la Declaración Universal de Derechos Humanos), regional (ámbito de la Unión Europea) y en los ordenamientos jurídicos nacionales<sup>29</sup>.

---

Estrategia Nacional de Inteligencia Artificial (ENIA), presentada en noviembre de 2020 en el marco de la Agenda Digital 2025, que complementa la regulación de la Inteligencia artificial en el apartado 5. XXIV de la Carta española de Derechos Digitales.

26. Por citar las más importantes: Libro Blanco de la Comisión de 2019 sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza; Conclusiones del Consejo Europeo de 2019 y de 2020, relativas al Plan Coordinado sobre la Inteligencia Artificial; Resoluciones del Parlamento Europeo relativas a la Inteligencia Artificial: 2020 (la ética, la responsabilidad civil y los derechos de propiedad intelectual), 2021 (ámbito penal y sectores educativo, cultural y audiovisual) o la Resolución del Parlamento Europeo de 2020 sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas.

27. Reglamento (UE) 2024/1689 del Parlamento y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), publicado en el DOUE núm. 1689, de 12 de julio de 2024.

28. RECHE TELLO / TUR AUSINA, 2022: 24-25.

29. Un ejemplo a destacar de cómo recoger la protección de los neuroderechos en un texto constitucional, ha sido el Proyecto de nueva Constitución chilena de 2022, en cuyo debate se incluyó una mención a la protección de la indemnidad mental respecto al avance de las neurotecnologías. Lamentablemente, como sabemos, la nueva Constitución chilena fue rechazada en referéndum por el pueblo chileno, pero el intento, además de innovador, ya marca una clara tendencia hacia dónde deben caminar las cosas. En el ámbito del *soft law*, y en el ámbito europeo, hay que destacar la Recomendación sobre Innovación Responsable en Neurotecnologías de la OCDE, de 2019, el Informe del Comité Internacional de Bioética de la UNESCO sobre las cuestiones éticas de la Neurotecnología de 15 de diciembre de 2021 o la Resolución del Parlamento Europeo de 3 de mayo de 2022 (puntos 36 y 247). En el ámbito español, hay que destacar la regulación de los derechos digitales en el empleo de las neurotecnologías, en el apartado 5.XXVI de la Carta de Derechos Digitales. Y en cuanto a iniciativas sociales, pueden citarse la Neuroright Initiative del Morningside Groupe de la Universidad de Columbia o la reciente Declaración de València de 2023 sobre la incorporación de los neuroderechos en la Declaración Universal de Derechos Humanos. Acerca de los retos que los neuroderechos plantean a los derechos fundamentales, puede consultarse: HERRÁN ORTIZ, 2023.

## **2. LOS DERECHOS DIGITALES EN EL ÁMBITO DEL CONSEJO DE EUROPA**

La regulación jurídica de todos estos temas en el ámbito del Consejo de Europa exige que nos refiramos expresamente al marco general del artículo 8º del Convenio Europeo de Derechos Humanos que, como es de sobra conocido, se refiere al derecho al respeto a la vida privada y familiar de toda persona, de su domicilio y de su correspondencia y al artículo 10, relativo a la libertad de expresión. En un marco más específico, también resulta obligado referirse al Convenio Europeo nº 108, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.<sup>30</sup> Y asimismo, hay que tener en cuenta su Protocolo Adicional (Convenio nº 181), hecho en Estrasburgo el 8 de noviembre de 2001<sup>31</sup> y el denominado Protocolo por el que se modifica el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del 10 de octubre de 2018 (Convenio nº 223)<sup>32</sup>.

Lo más novedoso en esta materia es el Convenio Marco del Consejo de Europa nº 255 sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho, adoptado en el seno de la 133 sesión del Comité de Ministros del Consejo de Europa, en Estrasburgo, el 17 de mayo de 2024<sup>33</sup>, que aún no ha entrado en vigor, y que intenta garantizar, como dice su artículo 1º, que las actividades durante el ciclo de vida de los sistemas de inteligencia artificial sean plenamente coherentes con los derechos humanos, la democracia y el Estado de Derecho. Su artículo 5º estipula que cada parte signataria adoptará medidas destinadas a garantizar que los sistemas de inteligencia artificial no se utilicen para socavar la integridad, independencia y eficacia de las instituciones y los procesos democráticos, citando expresamente los principios de separación de poderes, el respeto a la independencia judicial y el acceso a la justicia. Además, adoptará medidas destinadas a proteger sus procesos democráticos en el contexto de las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial, incluyendo el acceso justo de las personas al debate público y su participación en el mismo, así como su capacidad para formar libremente sus opiniones. En todo caso, el nivel de garantía establecido en el Convenio es de mínimos y en ningún caso impide una protección que vaya más allá del mismo.

---

30. Ratificado por España en 1984 y publicado en el Boletín Oficial del Estado nº 274, de 15 de noviembre de 1985.

31. Ratificado por España en 2010 y publicado en el Boletín Oficial del Estado nº 228, de 20 de septiembre de 2010.

32. Ratificado por España en enero de 2021.

33. Council of Europe, Ministers' Deputies, CM Documents, CM(2024)52-final, 17 May 2024. Este texto puede consultarse íntegramente en sus versiones oficiales en lengua inglesa y francesa en: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225> (última consulta, 19 de enero de 2025).

El capítulo 3º (arts. 6-13) del Convenio Marco recoge los principios relacionados con las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial, referidos a la dignidad humana y la autonomía individual, a la transparencia y supervisión, a la rendición de cuentas y la responsabilidad, a la igualdad y a la prohibición de discriminación, a la privacidad y a la protección de datos personales, a la fiabilidad de los sistemas de inteligencia artificial y la confianza en sus resultados y al establecimiento de entornos controlados para desarrollar, experimentar y probar sistemas de inteligencia artificial bajo la supervisión de sus autoridades competentes, evitando al mismo tiempo los efectos adversos sobre los derechos humanos, la democracia y el Estado de Derecho.

Su capítulo IV establece un cauce para la disponibilidad de vías de recurso accesibles y efectivas para las violaciones de los derechos humanos derivadas de las actividades durante el ciclo de vida de los sistemas de inteligencia artificial, incluyendo medidas para garantizar que la información relativa a los sistemas de inteligencia artificial que pueda afectar de forma significativa a los derechos humanos y su uso pertinente esté documentada, se facilite a los organismos autorizados a acceder a dicha información y cuando proceda, se ponga a disposición o se comunique a las personas afectadas, una información que debe ser suficiente para que las personas afectadas puedan impugnar las decisiones adoptadas mediante inteligencia artificial, incluyendo la posibilidad efectiva de que puedan presentar una denuncia ante las autoridades competentes (art. 14). Por su parte, el artículo 15 establece que las partes firmantes del Convenio deben garantizar que, cuando la inteligencia artificial incida significativamente en el disfrute de los derechos humanos, las personas afectadas tengan garantías procesales, salvaguardias y derechos efectivos, de conformidad no sólo con el derecho nacional sino también con el derecho internacional aplicables. Y, además, habrá que garantizar que se notifique a las personas que interactúen con los sistemas de inteligencia artificial, que están interactuando con dichos sistemas y no con seres humanos.

El capítulo VI (artículos 17-22) se refiere a la aplicación del Convenio e introduce cláusulas especiales de no discriminación, de protección especial de los derechos de las personas con discapacidad y de los niños. También se refuerza el derecho a la participación y a la consulta pública, con la garantía de que las cuestiones importantes relativas a la inteligencia artificial, se sometan a debate público y consulta con las partes interesadas, teniendo en cuenta sus implicaciones sociales, jurídicas, éticas, medioambientales, etc. y se incluye un compromiso de promoción de la alfabetización digital y de las capacidades digitales para todos los segmentos de la población, incluyendo las capacidades especializadas específicas para quienes se ocupen de los riesgos que plantean los sistemas de inteligencia artificial.

El Convenio establece también un mecanismo de seguimiento del cumplimiento del mismo, con la presentación de informes periódicos por las partes firmantes del mismo ante la denominada «Conferencia de las partes», obligándose cada parte a establecer mecanismos eficaces para supervisar el cumplimiento de las obligaciones del Convenio. Finalmente, en lo que se refiere a su aplica-

ción, pueden ser parte del Convenio los Estados miembros del Consejo de Europa, los Estados no miembros que hayan participado en su elaboración y la Unión Europea e incluso, con determinados requisitos, pueden adherirse al mismo Estados no miembros del Consejo de Europa que no hayan participado en la elaboración del Convenio. En cuanto a su aplicación territorial, el artículo 32 prevé que cualquier Estado, o la Unión Europea, podrá establecer el territorio o territorios a los que se aplicará el Convenio y el artículo 33 incluye una interesante cláusula federal al establecer que un Estado federal podrá reservarse el derecho de asumir obligaciones en virtud del presente Convenio en consonancia con los principios fundamentales que rigen la relación entre su Gobierno central y sus Estados constituyentes u otras entidades territoriales similares, siempre que el Convenio se aplique al Gobierno Central del Estado federal. Y en el caso de las disposiciones del Convenio cuya aplicación sea competencia de los Estados constituyentes u otras entidades territoriales similares que no estén obligadas por el sistema constitucional interno a adoptar medidas legislativas, el Gobierno federal informará con su dictamen favorable a las autoridades competentes de dichos Estados de dichas disposiciones y les alentará a adoptar las medidas adecuadas para su aplicación.

Este Convenio es un importante paso adelante en la creación de una normativa europea de protección de los derechos y libertades fundamentales en el nuevo marco generado por la Inteligencia Artificial. Cuando escribo estas líneas ha sido firmado ya por varios Estados y esperemos que sea ratificado por gran parte de los miembros del Consejo de Europa. Eso será una buena señal para todos. Y, de hecho, la Unión Europea ha querido dar ejemplo y lo ha firmado el 5 de septiembre de 2024, en virtud de la Decisión (EU) 2024/2218 del Consejo, de 28 de agosto de 2024<sup>34</sup>. Esperamos que se siga su ejemplo.

En cuanto a la jurisprudencia del Tribunal Europeo de Derechos Humanos, me referiré a algunas de sus Sentencias sobre estos asuntos que, en mi opinión, merecen ser destacadas, porque van creando una jurisprudencia cada vez más consolidada:

En la Sentencia de la Gran Sala de 16 de junio de 2015, asunto *Delfi AS. contra Estonia*<sup>35</sup>, se trataba de dilucidar si había habido violación del art. 10.1 del Convenio Europeo de Derechos Humanos en relación con la libertad de información. La empresa recurrente era propietaria de uno de los mayores portales de noticias en Internet de Estonia. En 2006, tras la publicación de un artículo en el portal sobre una empresa de transbordadores, se publicaron una serie de comentarios que contenían amenazas personales y lenguaje ofensivo dirigidos contra el propietario de la empresa de transbordadores. Se inició un procedimiento por difamación contra la empresa, que finalmente fue condenada al pago de una indemnización en concepto de daños y perjuicios. El caso llegó al Tribu-

---

34. DOUE-L, núm. 2218, de 4 de septiembre de 2024.

35. Sentencia de la Gran Sala de 16 de junio de 2015, asunto *Delfi AS. contra Estonia*. ECLI:CE:ECHR:2015:0616JUD006456909.

nal de Estrasburgo que, en una primera Sentencia de 10 de octubre de 2013, consideró por unanimidad que no había habido violación del artículo 10. El caso fue remitido a la Gran Sala que dictó esta nueva Sentencia, rechazando que hubiera violación del artículo 10 del Convenio por quince votos contra dos.

Este fue el primer caso en el que el Tribunal tuvo que examinar una denuncia relacionada con la libertad de expresión de los usuarios en Internet. Reconociendo los importantes beneficios que se pueden derivar de Internet en el ejercicio de la libertad de expresión, el Tribunal entendió que la responsabilidad por expresiones difamatorias u otros tipos de expresiones ilícitas debe, en principio, mantenerse y constituir un recurso efectivo para castigar las violaciones de los derechos de la personalidad. Además, observó que, en el presente caso, los comentarios impugnados constituían discurso de odio e incitación directa a la violencia; que el portal de noticias de la empresa demandante era uno de los mayores medios de comunicación en Internet del país y que existía preocupación pública por la controvertida naturaleza de los comentarios realizados en él. Por lo tanto, el alcance del examen del caso se limitó a la evaluación de los «deberes y responsabilidades» de los portales de noticias de Internet, a la luz del artículo 10 del Convenio.

El Tribunal entendió que los instrumentos jurídicos nacionales hacían previsible que un editor de medios de comunicación que gestiona un portal de noticias en Internet con fines económicos podría, en principio, ser considerado responsable en virtud de la legislación nacional, por la carga de comentarios claramente ilegales aparecidos en su portal. En su calidad de editor profesional, la empresa demandante estaba en condiciones de evaluar los riesgos relacionados con sus actividades y debió haber sido capaz de prever las consecuencias jurídicas que éstos podrían acarrear. En cuanto a la necesidad de la injerencia en la libertad de la empresa demandante para difundir información, el Tribunal dio especial importancia a la naturaleza profesional y comercial del portal de noticias de la demandante, y al hecho de que tenía un interés económico en la publicación de comentarios. Además, solo la empresa solicitante tenía los medios técnicos para modificar o eliminar los comentarios publicados en el portal de noticias. En este contexto, la implicación de la empresa demandante en la difusión de los comentarios sobre sus artículos en el portal iba más allá de la de un prestador de servicios pasivo y puramente técnico.

Respecto a si la responsabilidad de los autores reales de los comentarios podría servir como alternativa a la responsabilidad del portal de noticias de Internet, el Tribunal recordó que el anonimato en Internet, aunque es un valor importante, debe equilibrarse con otros derechos e intereses. Para llegar a esta conclusión, tuvo en cuenta el interés de los usuarios de Internet en no revelar su identidad, pero también señaló los efectos a veces muy negativos de una difusión ilimitada de información en Internet. En este sentido, el Tribunal se remitió al criterio del Tribunal de Justicia de la Unión Europea (TJUE) de que los derechos fundamentales de la persona, por regla general, prevalecen sobre los intereses económicos del operador del motor de búsqueda y los intereses de otros usuarios de Internet. En este caso, la incierta eficacia de las medidas que

permiten establecer la identidad de los autores de los comentarios, unida a la falta de instrumentos puestos en marcha por el portal de Internet para hacer posible que una víctima de incitación al odio pudiera interponer efectivamente una demanda contra los autores de los comentarios, hizo que el Tribunal de Estrasburgo apoyase la opinión de los tribunales nacionales estonios de que la persona perjudicada tenía que tener la opción de presentar una demanda contra la empresa solicitante o los autores de los comentarios.

En cuanto a las medidas adoptadas por la empresa solicitante para hacer frente a la publicación de comentarios ilícitos en su portal, la obligación de los grandes portales de noticias de tomar medidas efectivas para limitar la difusión de discursos de odio y discursos que inciten a la violencia no puede equipararse a «censura privada». Sin perjuicio de ciertos mecanismos para hacer frente a los comentarios que constituyan discurso de odio o incitación a la violencia existentes en la página web de la empresa que presentó el recurso a Estrasburgo, pudieran funcionar en muchos casos como una herramienta adecuada para equilibrar los derechos e intereses de todos los involucrados, en este caso habían sido insuficientes, ya que los comentarios ilegales habían permanecido en línea durante seis semanas.

En la Sentencia de 2 de febrero de 2016, asunto *Magyar Tartalomszolgáltatók Egyesülete and Index.Hu ZRT contra Hungría*<sup>36</sup>, El Tribunal examinó si unas publicaciones realizadas por usuarios en portales de Internet, que tenían por objeto actividades inmobiliarias, rebasaban el límite de lo permisible. El Tribunal declaró que había violación del art. 10 del Convenio por parte de Hungría. Los Tribunales húngaros habían decidido que los comentarios eran irrazonablemente ofensivos e injuriosos. Pero el Tribunal de Estrasburgo consideró que el uso de frases vulgares no era ofensivo en sí mismo y que era necesario tener en cuenta las particulares características del estilo de comunicación en determinados portales de Internet. Y la cuestión más relevante era que la responsabilidad objetiva por los comentarios de terceros podía tener consecuencias negativas para un portal de Internet, por ejemplo, obligándole a cerrar su espacio de comentarios, lo que podría tener un efecto disuasorio sobre la libertad de expresión en Internet, que resultaría especialmente perjudicial para un sitio Web no comercial, como era el caso.

En la Decisión de 19 de septiembre de 2017, asunto *Payam Tamiz contra Reino Unido*<sup>37</sup>, el demandante había interpuesto una demanda por difamación a raíz de la publicación de algunos comentarios en un blog, que consideraba difamatorios. En este caso se examinaban las responsabilidades del autor de un comentario a una publicación en un blog y a Google inc., titular de la plataforma donde estaba alojado dicho blog. El Tribunal declaró inadmisile (es decir, ma-

---

36. Sentencia del Tribunal Europeo de Derechos Humanos de 2 de febrero de 2016, *asunto Magyar Tartalomszolgáltatók Egyesülete and Index.Hu ZRT c. Hungría*. ECLI:CE:ECHR:2016:0202JUD002294713.

37. Decisión de 19 de septiembre de 2017, asunto *Tamiz c. Reino Unido*. ECLI:CE:ECHR:2017:0919DEC000387714.

nifiestamente infundado) el recurso. El atentado contra el honor y la reputación de las personas debe alcanzar cierto grado de gravedad y haberse llevado a cabo de manera que causara un perjuicio al disfrute personal del derecho al respeto de la vida privada, para suponer una violación del artículo 8 del Convenio. La realidad era que millones de usuarios de Internet publican comentarios en línea cada día y muchos de esos usuarios se expresan de forma que podía considerarse ofensiva o incluso difamatoria. Sin embargo, es probable que la mayoría de los comentarios tengan un carácter demasiado trivial y/o que el alcance de su publicación sea demasiado limitado para causar un daño significativo a la reputación de otra persona. El Tribunal de Justicia coincidió con los órganos jurisdiccionales británicos en que, si bien la mayoría de los comentarios sobre los que se quejaba la demandante eran indudablemente ofensivos, en su mayor parte eran poco más que «insultos vulgares» habituales en la comunicación en muchos portales de Internet.

En la Sentencia de 28 de junio de 2018, asunto *M.L. y W.W. contra Alemania*<sup>38</sup>, y en relación con la posible violación del artículo 8 del Convenio sobre el respeto a la vida privada, el Tribunal de Estrasburgo consideró que no hubo violación de tal artículo y realizó un detallado estudio de las consecuencias del papel desarrollado por los buscadores en la difusión de la información en Internet y sus repercusiones en el derecho a la vida privada. En este caso, los demandantes fueron declarados culpables del asesinato de un conocido actor y condenados a cadena perpetua en 1993. En 2007, acercándose la fecha de su salida de prisión, iniciaron acciones contra varios medios de comunicación, solicitando que «anonimizaran» documentos de archivo accesibles en sus sitios de Internet y fechados en el momento del juicio (un artículo, un expediente y la transcripción de un informe de audio). En 2009 y 2010, aunque reconoció que los demandantes tenían un interés considerable en no se les pudiese relacionar más con su condena, el Tribunal Federal de Justicia alemán falló a favor de los medios de comunicación, basándose en que:

- el crimen y el juicio habían atraído considerable atención de los medios de comunicación en ese momento; el público tenía interés en estar informado, lo que incluía la posibilidad de realizar investigaciones sobre hechos pasados; que era parte del rol de los medios participar en la formación de opinión democrática poniendo a disposición sus archivos;
- los demandantes habían intentado recientemente que se reabriera el procedimiento en su caso; apenas tres años antes de su liberación, habían llamado a la prensa a difundir información sobre su más reciente solicitud de un nuevo juicio y hasta 2006, el sitio web del abogado defensor penal del segundo demandante había incluido múltiples informes sobre su cliente;

---

38. Sentencia del Tribunal Europeo de Derechos Humanos de 28 de junio de 2018, asunto *M.L. y W.W. contra Alemania*. ECLI:CE:ECHR:2018:0628JUD006079810.

- los documentos en cuestión se habían colocado bajo títulos que indicaban claramente que no se trataba de informes nuevos.

Los solicitantes consideraron que este enfoque no tuvo en cuenta el poder de los motores de búsqueda de Internet y recurrieron al Tribunal Europeo de Derechos Humanos por violación del artículo 8 del Convenio. A este respecto, el Tribunal declaró que la vulneración inicial de la vida privada de los demandantes se produjo por la decisión de los medios de comunicación interesados de publicar la información y, especialmente, de mantenerla disponible en sus sitios web, incluso sin la intención de atraer la atención del público. La existencia de motores de búsqueda simplemente agravó la interferencia. Sin embargo, las obligaciones de los motores de búsqueda con respecto al individuo afectado por un elemento de información pueden ser diferentes de las de la entidad que originalmente publicó la información. En consecuencia, el equilibrio de los intereses contrapuestos podría dar lugar a diferentes resultados, dependiendo de si la solicitud de eliminación se hizo contra la entidad que había publicado originalmente la información (cuya actividad generalmente estaba en el centro de lo que se pretendía proteger la libertad de expresión) , o contra un motor de búsqueda (cuyo principal interés no era publicar la información inicial sobre el interesado, sino facilitar la identificación de toda la información disponible sobre él o ella y crear un perfil del mismo).

El Tribunal de Estrasburgo concluyó que la negativa a conceder la solicitud de los demandantes no había violado las obligaciones positivas del Estado alemán de proteger la vida privada de los demandantes. En vista del margen de apreciación de las autoridades nacionales en tales materias al sopesar intereses divergentes, de la importancia de mantener la disponibilidad de informes cuya legalidad no había sido cuestionada cuando se publicaron inicialmente, y de la conducta de los demandantes frente a la prensa, el Tribunal no percibió motivos de peso que le obligaran a cambiar la interpretación jurídica realizada por el del Tribunal Federal de Justicia alemán. En este caso, se planteaban cuestiones muy interesantes, por ejemplo:

- a) la contribución a un debate de interés general y la cuestión de la «anoni-mización» previa solicitud: a pesar de su importancia, los derechos de una persona que había sido objeto de una publicación disponible en Internet también debían sopesarse frente al interés público. —amparado por el artículo 10 de la Convención— en ser informado sobre los acontecimientos pasados y la historia contemporánea a través de los archivos digitales públicos de la prensa. En el presente caso, la disponibilidad de los informes impugnados en los sitios web de los medios de comunicación en el momento en que los demandantes presentaron sus solicitudes siguió contribuyendo a un debate de interés general que no había disminuido con el paso de algunos años.
- b) El grado de notoriedad del interesado y objeto de la denuncia: es cierto que con el paso del tiempo el interés público por el delito en cuestión

había disminuido. Sin embargo, los demandantes habían vuelto a ser objeto de atención pública cuando intentaron que se reabriera su juicio penal y se habían puesto en contacto con la prensa al respecto. Por lo tanto, no eran simplemente personas privadas desconocidas para el público.

- c) El contenido, la forma y las consecuencias de la publicación: los textos impugnados describieron, de manera objetiva, una decisión judicial. Es cierto que algunos de los artículos en cuestión proporcionaron detalles sobre la vida de los acusados. Sin embargo, esos detalles formaban parte de la información que los jueces penales debían tener en cuenta regularmente al evaluar las circunstancias del delito y los elementos de culpabilidad individual y, en consecuencia, generalmente formaban parte de las deliberaciones durante las audiencias públicas. Además, estos artículos no reflejaban la intención de presentar a los solicitantes de manera denigrante o de dañar su reputación. En cuanto al alcance de su publicación, dada su posición en la arquitectura de los sitios web en cuestión, no era probable que los informes impugnados atrajeran la atención de los usuarios de Internet que no buscaban información sobre los solicitantes. Del mismo modo, no había nada que sugiriera que mantener el acceso a esos informes hubiera tenido la intención de volver a difundir información sobre los solicitantes.
- d) Las circunstancias en las que se tomaron las fotos: las fotografías impugnadas no contenían ningún elemento comprometedor. La probabilidad de que las fotografías llevaran a terceros a reconocer a los solicitantes también se redujo por el hecho de que mostraban la apariencia de los solicitantes trece años antes de su liberación.

En la Sentencia de 25 de noviembre de 2021, asunto *Biancardi contra Italia*<sup>39</sup>, se discutía la sanción civil (indemnización) impuesta a un editor de un periódico on-line por haberse negado durante mucho tiempo (durante ocho meses) a «desindexar» un artículo sobre una causa penal contra unos particulares a petición de estos, información que era fácilmente accesible, tecleando sus nombres en un motor de búsqueda de Internet, aunque finalmente lo hizo, cuando fue demandado ante los Tribunales. Los Tribunales italianos condenaron a quien presentó el recurso ante el TEDH a una indemnización civil por vulneración de su derecho al honor. El Tribunal de Estrasburgo entendió que, en este caso, la clave estaba en la facilidad con que podía accederse a los datos en cuestión y no en su simple mantenimiento en Internet. El Tribunal prestó atención al tiempo excesivamente largo que se mantuvo la información disponible, al carácter sensible de los datos en cuestión (un procedimiento penal) y que el Sr. Biancardi había sido condenado civilmente y no penalmente, y entendió que

---

39. Sentencia del Tribunal Europeo de Derechos Humanos de 25 de noviembre de 2021, asunto *Biancardi contra Italia*. ECLI:CE:ECHR:2021:1125JUD007741916.

los Tribunales italianos no habían infringido el artículo 10 del Convenio, puesto que la restricción de su libertad de expresión estaba justificada.

También hay que hacer referencia a la controvertida<sup>40</sup> Sentencia de la Gran Sala de 15 de mayo de 2023<sup>41</sup>, asunto *Sánchez contra Francia*. El Sr. Sánchez era un político francés del grupo del Rassemblement national (hasta 2018 conocido como «Front national», FN), alcalde de Beaucaire y presidía el grupo de dicho partido en el Consejo Regional de Occitania. Fue responsable de la estrategia de Internet del FN durante varios años y cuando tuvieron lugar los hechos, candidato del Frente Nacional por Nîmes. Sanchez utilizaba su muro de Facebook para finalidades electorales y políticas y durante las elecciones, lanzó una publicación en su muro de Facebook sobre el primer teniente de alcalde de Nîmes y parlamentario europeo, el Sr. FP, uno de sus oponentes políticos. Dicha publicación no tenía nada conflictivo ni incitaba al odio o discriminación, pero al hilo de dicha publicación se generaron los mensajes conflictivos que se consideraron que eran ilícitos (en concreto, los de dos personas: SB y LR). El Tribunal de lo Penal de Nîmes en sentencia de 28 de febrero de 2013, declaró culpables a SB y LR por sus mensajes y al Sr. Sánchez por no moderar y eliminar tales mensajes (si bien uno fue eliminado de inmediato). La Sentencia fue apelada al Tribunal de Apelación de Nîmes, de fecha 18 de octubre de 2013, le impuso una multa de 3.000 euros y 1.000 euros en concepto de costas. El Sr. Sánchez recurrió al Tribunal de Casación francés, que rechazó su recurso por Sentencia de 17 de marzo de 2015. El proceso penal se originó a partir de una denuncia interpuesta por la pareja de uno de los opositores políticos del demandante, que se sintió insultada y tuvo un altercado con uno de los autores, quien inmediatamente eliminó su mensaje e informó al recurrente. El recurrente publicó en su «muro» de Facebook un mensaje invitando a los comentaristas a «tener cuidado con el contenido» de sus comentarios pero sin moderar los ya publicados. Tras su condena por los Tribunales franceses, el Sr. Sánchez recurrió al Tribunal Europeo de Derechos Humanos por violación del artículo 10 del Convenio Europeo de Derechos Humanos (libertad de expresión). En una primera Sentencia, la Sección 5ª del Tribunal, en Sentencia de 2 de septiembre de 2021, consideró, por seis votos contra uno, que no había habido violación del artículo 10. Recurrida dicha Sentencia a la Gran Sala, ésta por Sentencia de 15 de mayo de 2023 volvió a declarar por 13 votos a 4, que no hubo violación del artículo 10 del Convenio.

Desde el asunto *Delfi AS contra Estonia*, el Tribunal aceptó que era posible que los Estados contratantes declararan responsables a los portales de noticias de Internet sin violar el artículo 10 si esos portales no eliminaban comentarios claramente ilegales de terceros inmediatamente después de que fueran publicados, incluso en ausencia de notificación por parte de la víctima o de terceros,

---

40. Puede consultarse a este respecto, alguna opinión muy crítica con esta Sentencia como, por ejemplo, COTINO HUESO, 2023.

41. Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 15 de mayo de 2023, asunto *Sánchez contra Francia*. ECLI:CE:ECHR:2023:0515JUD004558115.

pero en este caso se plantea una novedad: la responsabilidad del titular individual de una cuenta de Facebook en el caso de contenidos ilegales o que incitaban al odio o la violencia. En el contexto concreto del caso, el Tribunal entendió que, teniendo en cuenta que los comentarios fueron colgados en el «muro» de Facebook de un político durante una campaña electoral, equivalían genuinamente a un discurso de odio, por su contenido y tono general, junto con la virulencia y vulgaridad de parte del lenguaje utilizado y que su alcance se había extendido más allá de un público estrictamente partidista.

El caso era delicado porque la libertad de expresión y más en un contexto de campaña electoral debe ser especialmente protegida. Dado que Internet se ha convertido en uno de los principales medios a través de los cuales las personas ejercen su derecho a la libertad de expresión, las injerencias en el ejercicio de ese derecho deben examinarse con especial cuidado, ya que es probable que tengan un efecto disuasorio («chilling effect»), lo que conlleva el riesgo de autocensura. Pero la existencia de ese riesgo no debe hacernos perder de vista la existencia de otros peligros para el ejercicio y goce de los derechos y libertades fundamentales. Por ello, sostiene el Tribunal, debe mantenerse, en principio, la posibilidad de que los particulares que denuncian expresiones difamatorias u otro tipo de expresiones ilícitas interpongan una acción de responsabilidad, constituyendo un recurso efectivo frente a las supuestas infracciones. Los Tribunales franceses estaban mejor situados para evaluar los hechos a la luz del difícil contexto local y su reconocida dimensión política, pero el lenguaje utilizado en los comentarios en cuestión claramente incitaba al odio y la violencia contra una persona por su religión y esto no podía ser disimulado o minimizado por el contexto electoral o por el deseo de discutir las dificultades locales.

En este caso, el político francés hizo accesible su muro de Facebook al público en general y, a juicio del Tribunal, todo el mundo, y por tanto especialmente un político experimentado en la comunicación al público, debe ser consciente del mayor riesgo de comentarios excesivos e inmoderados que pueden aparecer y hacerse necesariamente visibles a un público más amplio. Este fue sin duda un elemento fáctico importante, directamente relacionado con la elección deliberada del solicitante, quien no solo era un político sino también un profesional en cuestiones de estrategia de comunicación en línea y, por lo tanto, tenía cierta experiencia en el campo digital. El Sr. Sánchez consideró oportuno llamar la atención de sus «amigos» sobre la necesidad de asegurarse de que sus comentarios siguieran siendo legales, ya que había publicado un mensaje pidiéndoles que «tuvieran cuidado con el contenido de [sus] comentarios», demostrando así que al menos estaba al tanto de los problemas planteados por ciertos comentarios. Sin embargo, había enviado este mensaje de advertencia sin borrar los comentarios impugnados y, sobre todo, sin haberse tomado la molestia de verificar, o haber verificado, el contenido de los comentarios que entonces eran de acceso público. De hecho, el recurrente fue condenado por los Tribunales franceses, no por los comentarios hechos por los dos autores tomados aisladamente, sino por no haber procedido a la pronta eliminación de todos los comentarios ilegales en cuestión.

Es cierto que una condena penal podía tener efectos disuasorios para otros los usuarios de Facebook o de otras redes sociales, pero el Comité de Ministros del Consejo de Europa había propuesto hacer una distinción según la gravedad del discurso de odio, sin excluir el recurso a la ley penal. La imposición de una pena de prisión por un delito en el ámbito del discurso político puede ser compatible con la libertad de expresión, pero solo en circunstancias excepcionales, en particular en el caso del discurso del odio o la incitación a la violencia. Además, aunque una multa de una determinada cuantía pudiera parecer severa en relación con las circunstancias, debía evaluarse a la luz del hecho de que, en principio, podría haberse dictado una pena de prisión. La pena máxima a la que se enfrentaba el demandante había sido un año de prisión y una multa de 45.000 euros. Sin embargo, sólo había sido condenado a una multa de 3.000 euros junto con el pago de 1.000 euros a la parte civil en costas. Además, no hubo otras consecuencias para el Sr. Sánchez. De hecho, el recurrente no alegó que posteriormente se hubiese visto obligado a cambiar su conducta, o que su condena hubiese tenido un efecto paralizador en el ejercicio de su libertad de expresión o un impacto negativo en su carrera política posterior y sus relaciones con los votantes. De hecho, fue elegido alcalde en 2014 y continuó ejerciendo responsabilidades en su partido político.

En definitiva, a juicio de la mayoría del Tribunal, las decisiones de los tribunales nacionales se habían basado en razones pertinentes y suficientes, tanto en cuanto a la responsabilidad atribuida al demandante, en su calidad de político, por los comentarios ilegales publicados en el período previo a una elección en su «muro» de Facebook por terceros, que habían sido identificados y procesados como cómplices, como en cuanto a su condena penal. Por lo tanto, la injerencia impugnada podría considerarse «necesaria en una sociedad democrática» y no había violación del art. 10 del Convenio.

Por último, hay que citar la Sentencia de la Gran Sala de 4 de julio de 2023, en el *asunto Hurbain contra Bélgica*<sup>42</sup>. En este caso, la Sección tercera del Tribunal, por seis votos contra uno, dictó una primera Sentencia de fecha 22 de junio de 2021<sup>43</sup> en la que rechazó que hubiera violación del artículo 10 del Convenio europeo en el caso de una publicación que fue requerida para «anonimizar», en ejercicio del «derecho al olvido» la versión archivada en línea de un artículo publicado veinte años antes, de un conductor que había causado un accidente mortal. La demandante ante el Tribunal Europeo de Derechos Humanos, editora de un diario, fue condenada mediante sentencia civil de 2013 a «anonimizar» la versión digital de un artículo publicado en 1994 y añadido al archivo en línea en 2008, con el fin de respetar el «derecho al olvido» del conductor cuyos datos de identificación aparecían completos. Los recursos de la

---

42. Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala), de 4 de julio de 2023, *asunto Hurbain contra Bélgica*. ECLI:CE:ECHR:2023:0704JUD005729216.

43. Sentencia del Tribunal Europeo de Derechos Humanos (Sección 3ª) de 22 de junio de 2021, *asunto Hurbain contra Bélgica*. ECLI:CE:ECHR:2021:0622JUD005729216.

editora del diario contra esta sentencia fueron rechazados por los Tribunales belgas. En realidad, lo que aquí se discutía era si la sentencia ordenando la «anonimización» de los datos violaba el art. 10 del Convenio. El Tribunal entendió que no, porque los tribunales nacionales habían sopesado el derecho del conductor al respeto de su vida privada, por un lado, y el derecho del demandante a la libertad de expresión, por otro, de conformidad con los criterios establecidos en la jurisprudencia del Tribunal.

El Tribunal de Apelación belga había concedido especial importancia al perjuicio sufrido por el conductor a causa del acceso on-line al artículo, habida cuenta del tiempo transcurrido desde la publicación del artículo original y el hecho de que la «anonimización» del artículo en el sitio web del periódico dejaba intactos los propios archivos y constituía la medida más eficaz, entre todas las que podían contemplarse en el presente caso, sin interferir desproporcionadamente la libertad de expresión de la parte demandante. A juicio del Tribunal de Estrasburgo, los motivos aducidos por los tribunales belgas habían sido pertinentes y suficientes y el Tribunal no encontró ninguna razón de peso para sustituir la opinión de los tribunales nacionales por la suya propia o desestimar el resultado de su ejercicio de ponderación. Así pues, la medida impuesta podía considerarse proporcional al objetivo legítimo perseguido, estableciendo un justo equilibrio entre los derechos en conflicto.

El Tribunal de Estrasburgo dejó bien claro que su decisión no puede interpretarse en el sentido de que los medios de comunicación estén obligados a comprobar sus archivos de forma sistemática y permanente. Sin olvidar su deber de respetar la vida privada en el momento de la publicación inicial, en el momento de archivar los artículos no estarían obligados a realizar dicha comprobación y, por tanto, a ponderar los distintos derechos en juego, a menos que recibieran una solicitud expresa en ese sentido.

Esta primera Sentencia fue recurrida a la Gran Sala, que dictó la Sentencia definitiva de 4 de julio de 2023, que confirmó el criterio de la primera sentencia, manifestando que no hubo violación del artículo 10 del Convenio. El Tribunal hizo un detenido estudio del asunto, analizando con detalle la normativa internacional, del Consejo de Europa y de la Unión Europea y la jurisprudencia no sólo del propio Tribunal sino también del Tribunal de Justicia de la Unión Europea, de los Tribunales franceses, británicos, italianos y de los Tribunales Constitucionales alemán y español y, repasó los criterios de ponderación para establecer si debe darse prioridad al derecho al olvido o la libertad de información, que podrían resumirse de la siguiente manera:

- en relación con la naturaleza de la información archivada, siendo los hechos denunciados en el presente caso de carácter judicial, el criterio pertinente fue la naturaleza y gravedad del delito objeto del artículo original y que esos hechos, aunque trágicos, no entraban en la categoría de delitos cuya trascendencia, por su gravedad, no se alteraba con el paso del tiempo. Además, el caso no había atraído una amplia publicidad.

- respecto al tiempo transcurrido desde los hechos y desde la publicación inicial y en línea, en este caso había transcurrido un tiempo significativo (dieciséis años) entre la publicación inicial del artículo y la primera solicitud de *anonimización*. En esas circunstancias, G., quien había sido rehabilitado y tenía un interés legítimo después de todo ese tiempo en buscar que se le permitiera reintegrarse a la sociedad sin que se le recordara permanentemente su pasado.
- en cuanto al interés de la información hoy en día, debía determinarse si el artículo en cuestión continuaba contribuyendo a un debate de interés público, si había adquirido algún interés histórico, de investigación o estadístico y si seguía siendo relevante para el con el fin de contextualizar los hechos recientes para comprenderlos mejor. El Tribunal entendió que, veinte años después de eventos que claramente no tenían importancia histórica, la identidad de una persona que no era una figura pública no se sumaba al interés público del artículo, que simplemente hizo una contribución estadística a un debate público sobre la seguridad vial.
- acerca de si la persona que reclama el derecho al olvido era notoriamente conocida y su conducta desde los hechos, en este caso, el Sr. G. era una persona desconocida para el público, no había buscado ser el centro de atención y no había atraído una amplia publicidad ni en el momento de los hechos denunciados ni cuando la versión archivada del artículo se publicó on-line.
- respecto a las repercusiones negativas de la continua disponibilidad de la información on-line, para justificar la alteración de un artículo almacenado en un archivo de prensa digital, la persona interesada tenía que poder hacer una alegación debidamente fundamentada de daño grave a su o su vida privada. En este caso, la presencia del artículo en los archivos on-line había podido estigmatizar a G., que era médico, y dañar gravemente su reputación en el ojos de sus pacientes y colegas en particular e impedirle reintegrarse normalmente a la sociedad.
- en cuanto al grado de accesibilidad de la información en los archivos digitales, había que tener en cuenta que, en ausencia de una búsqueda activa (utilizando palabras clave), no era probable que un artículo contenido en los archivos digitales llamase la atención de los usuarios de Internet que no buscaban información precisa sobre una persona en particular. También era importante determinar el grado de accesibilidad del artículo archivado, es decir, si estaba disponible sin restricciones y de forma gratuita o si el acceso estaba limitado a los suscriptores o restringido de algún modo. En el presente caso, la presencia continua del artículo en cuestión en los archivos, a los que se podía acceder sin restricciones y de forma gratuita desde que se colgó on-line, indudablemente perjudicaba a G.
- en lo que respecta al impacto de la medida en la libertad de expresión o en la libertad de información, y dada la importancia de la integridad de los archivos de prensa digital, los tribunales nacionales, al juzgar contro-

versias de este tipo y decidir cuál de las diferentes medidas solicitadas por la persona, deben dar preferencia a la medida que sea más adecuada para el objetivo perseguido por esa persona, suponiendo que esté justificada, y al mismo tiempo que sea menos restrictiva de la libertad de prensa. Sólo pueden ordenarse medidas que respondan a ese doble objetivo. Esa ponderación podría llevarse a cabo de manera útil a la luz de las distintas medidas disponibles. Por ejemplo, el operador de un motor de búsqueda distinto al del proveedor de contenidos podría implementar, entre otras, las siguientes medidas: (a) reorganización de los resultados de búsqueda para que el enlace al sitio web en cuestión apareciera en un lugar menos destacado en la lista de resultados, o (b) eliminación total o parcial (referida únicamente a búsquedas basadas en el nombre de la persona en cuestión) mediante la eliminación del enlace del índice del motor de búsqueda. Mientras tanto, el editor de un sitio web podría, por ejemplo: (a) eliminar todo o parte de un texto almacenado en el archivo digital; (b) *anonimizar* los datos de la persona a la que se hace referencia en el texto; (c) agregar un aviso al texto, es decir, actualizar el texto mediante una rectificación digital (cuando la información fuera inexacta) o vía comunicación electrónica (cuando la información fuera incompleta); (d) eliminar el artículo del índice del motor de búsqueda interno del sitio web; o (e) hacer que el artículo sea *desindexado*, total o parcialmente (solo en relación con búsquedas basadas en el nombre de la persona en cuestión), por motores de búsqueda externos, sobre la base de códigos de acceso o directivas emitidas a los operadores de motores de búsqueda impidiendo que sus programas de búsqueda rastreen ciertas ubicaciones.

Los Tribunales belgas habían decidido que el medio más eficaz para proteger la privacidad de G. sin interferir de un modo desproporcionado con la libertad de expresión o información del demandante fue *anonimizar* el artículo en el sitio web del periódico. La versión original del artículo, no *anonimizada*, todavía estaba disponible en forma impresa y podía ser consultada por cualquier persona interesada, cumpliendo así su función inherente como registro de archivo. Por su parte, el Tribunal había sostenido anteriormente que la anonimización era menos perjudicial para la libertad de expresión que la eliminación de un artículo completo. Se refería únicamente al nombre y apellidos de la persona interesada y no afectaba de ningún otro modo al contenido de la información transmitida. La obligación de un editor de *anonimizar* un artículo que había sido publicado inicialmente de manera legal podría, en principio, formar parte de los «deberes y responsabilidades» de la prensa y de los límites que se le podrían imponer. Y en este caso concreto, no parece que la orden de *anonimización* hubiese tenido un impacto real en el desempeño por parte del diario de sus funciones periodísticas. Por ello, el Tribunal de Estrasburgo entiende que los Tribunales belgas habían encontrado un equilibrio entre los derechos en juego y el Convenio Europeo de Derechos Humanos y que la interferencia con la libertad de expresión y de comunicación protegida por el artículo 10 del Conve-

nio, se había limitado a lo que era estrictamente necesario y podía así, teniendo en cuenta las circunstancias concretas del caso, ser considerada como necesaria en una sociedad democrática y proporcionada, por lo que entendió por doce votos contra cinco, que no hubo violación del artículo 10 del Convenio.

### 3. LOS DERECHOS DIGITALES EN EL ÁMBITO DE LA UNIÓN EUROPEA

#### 3.1. Declaraciones y documentos (*soft law*)

Como hemos visto anteriormente, las iniciativas, para tener eficacia real, deben superar el ámbito de los Estados-nación y, al menos en nuestro entorno jurídico, deben ser llevadas a cabo en el marco de la Unión Europea. En este sentido, podemos destacar algunos instrumentos de *soft law*. Por ejemplo, en materia de Administración electrónica, las Declaraciones ministeriales de Bruselas (2001), Como (2003), Manchester (2005), Lisboa (2007), Malmö (2009), Tallin sobre la Administración Electrónica (2017) y la Declaración Ministerial de Sociedad Digital y Administración Digital basada en valores de Berlín (2020)<sup>44</sup>, cuyo objetivo general es «contribuir al avance de la transformación digital sobre la base de los valores europeos y aprovechar las oportunidades de futuro de la digitalización». También hay que tener en cuenta la Declaración de Lisboa sobre democracia digital con propósito de 2021<sup>45</sup>, que pretende fomentar la economía digital basada en los valores europeos de protección de los derechos de los ciudadanos y la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, sobre la Brújula Digital 2030: el enfoque de Europa para el Decenio Digital de 2021 (COM (2021) 118 final).<sup>46</sup>

Pero, sin duda, el documento más importante es la *Declaración Europea sobre los derechos y los principios digitales para la Década digital*, de 23 de enero de 2023, del Parlamento Europeo, el Consejo y la Comisión (2023/C 23/01)<sup>47</sup> que, aunque solamente tiene efecto declarativo y no afecta al contenido de las normas jurídicas ni a su aplicación, tiene, obviamente, una gran relevancia. Como se dice en su Preámbulo de una forma muy clara, «con la aceleración de la transformación digital, ha llegado el momento de que la UE exprese cómo han de aplicarse en el mundo digital sus valores y sus derechos fundamentales

---

44. [https://administracionelectronica.gob.es/pae\\_Home/pae\\_Estrategias/pae\\_lineas\\_ccoperacion/pae\\_Cooperacion\\_Internacional/pae\\_estrategias\\_de\\_administracion\\_electronica/pae\\_Ambito\\_Europeo\\_-\\_Las\\_Declaraciones\\_Ministeriales.html](https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_lineas_ccoperacion/pae_Cooperacion_Internacional/pae_estrategias_de_administracion_electronica/pae_Ambito_Europeo_-_Las_Declaraciones_Ministeriales.html) (última consulta, 16 de abril de 2023).

45. <https://www.lisbondeclaration.eu/>. (última consulta, 16 de abril de 2023).

46. <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021DC0118&from=ES> (última consulta, 16 de abril de 2023).

47. [https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32023C0123\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32023C0123(01)&from=EN) (última consulta, 16 de abril de 2023).

que se aplican fuera de línea. La transformación digital no debe implicar un retroceso en los derechos. Lo que es ilegal fuera de línea, es ilegal en línea» (Considerando nº 3). Y en su considerando nº 6, aclara cómo, es decir, cuál es la vía de la Unión para la transformación digital de nuestras sociedades y nuestra economía, que abarca la soberanía digital de manera abierta, el respeto de los derechos fundamentales, el Estado de Derecho y la democracia, la inclusión, la accesibilidad, la igualdad, la sostenibilidad, la resiliencia, la seguridad, la mejora de la calidad de vida, la disponibilidad de servicios y el respeto de los derechos y aspiraciones de todas las personas. La Declaración está dirigida a los responsables de las políticas públicas, pero también a los responsables de las empresas y otros agentes pertinentes a la hora de implantar las nuevas tecnologías, y guiar las relaciones de la Unión Europea con otras organizaciones internacionales y terceros países, y se refiere especialmente a la Agenda 2030 para el desarrollo sostenible y el enfoque multilateral de la gobernanza en Internet.

La Declaración fija en su capítulo primero cuál debe ser el núcleo de la transformación digital: Una transformación digital centrada en las personas; e introduce en su capítulo segundo los principios de solidaridad e inclusión, conectividad y derecho a la a la educación, la formación y el aprendizaje permanente, que debería permitir poder adquirir todas las capacidades digitales básicas y avanzadas, el derecho a unas condiciones de trabajo justas y equitativas en el entorno digital y en el puesto de trabajo físico y al acceso en línea a los servicios públicos esenciales de la UE. El capítulo III, relativo a la libertad de elección, se refiere a las interacciones con algoritmos y sistemas de inteligencia artificial y a un entorno digital justo. Por su parte, el capítulo IV hace referencia a la participación en el espacio público digital, con una especial referencia a derechos clásicos como la libertad de expresión e información, reunión y asociación en el entorno digital. El capítulo V hace referencia a la seguridad, protección y empoderamiento, con los derechos a un entorno digital protegido y seguro, y a la privacidad, protección de los datos personales y al control individual de sus datos personales. También se hace una especial referencia a la protección y empoderamiento de los niños y jóvenes en el entorno digital. Finalmente, su capítulo VI, se refiere a la sostenibilidad de los productos y servicios digitales.

### **3.2. Normativa (*hard law*)**

En cuanto al Derecho vigente en el ámbito de la Unión Europea y, en lo que se refiere al Derecho originario, hay que citar necesariamente el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea que recoge expresamente el derecho de toda persona a la protección de datos de carácter personal que le conciernan, que esos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley; que toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación y , finalmente, que el respeto de estas normas quedará sujeto al control de una autoridad independiente.

Por su parte, el artículo 16 del Tratado de Funcionamiento de la Unión Europea, recoge también el derecho a la protección de datos de carácter personal, de un modo muy similar a como se hace en la Carta de los Derechos Fundamentales de la Unión Europea y afirma también que el Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos, estando sometido el respeto de dichas normas al control de autoridades independientes, si bien las normas adoptadas lo serán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.

Y, finalmente, el artículo 39 del Tratado de la Unión Europea matiza que, en consonancia con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del capítulo 2º del Tratado, es decir en lo relativo a las disposiciones específicas sobre política exterior y seguridad común y sobre la libre circulación de dichos datos. Y una vez más, incluye la cláusula de que el respeto de dichas normas estará sometido al control de autoridades independientes.

En lo que se refiere al Derecho europeo derivado, hay que citar en primer lugar la derogada Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995<sup>48</sup>, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. Esta norma fue pionera en esta materia de protección de datos. Sin embargo, el transcurso del tiempo hizo que fuese necesaria una regulación más uniforme del derecho fundamental a la protección de datos en el ámbito de toda la Unión Europea. El siguiente paso a destacar fue la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas<sup>49</sup> (la conocida como *Directiva sobre la privacidad y las comunicaciones electrónicas*) en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009<sup>50</sup>.

Pero, sin duda, la norma más importante en esta materia es el 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 sus datos personales y a la libre circulación de estos datos y por el que se

---

48. DOCE núm. 281, de 23 de noviembre de 1995.

49. DOCE núm. 201, de 31 de julio de 2002.

50. DOUE núm. 337, de 18 de diciembre de 2009.

deroga la Directiva 95/46/CE<sup>51</sup> y que, como veremos posteriormente, está directamente influido por la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 13 de mayo de 2014, C-131/12, *caso Google Spain S.L. y Google Inc. contra la AEPD y Mario Costeja González*.

¿Por qué se dictó este Reglamento? Pues básicamente por los problemas ocasionados en la transposición de la Directiva 95/46 en los distintos países de la UE, por el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior y por los retos planteados por la rápida evolución tecnológica y la globalización, que ha hecho que los datos personales sean el recurso fundamental de la sociedad de la información. Dada la debilidad que evidenciaban los tradicionales derechos instrumentales de protección de datos (los denominados «derechos ARCO»: acceso, rectificación, supresión y oposición) en el entorno tecnológico, el nuevo Reglamento apostó por la creación de *nuevos derechos digitales* intrínsecamente vinculados al derecho de protección de datos, por ejemplo: a) el derecho reforzado de información al usuario; b) el *derecho al olvido*; c) el derecho a la notificación de la rectificación o supresión de datos y d) el derecho a la portabilidad.

Este Reglamento europeo que, a diferencia de las Directivas, según el derecho de fuentes de las normas de la Unión Europea, es directamente aplicable, y en principio, no necesitaría desarrollo en los países miembros de la UE, es desarrollado de alguna manera en España por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de Derechos Digitales. Para salvar este problema, la justificación que se da en el Preámbulo de la Ley Orgánica es que: «los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea».

También hay que tener en cuenta la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016<sup>52</sup>, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (que era previa al Tratado de Lisboa y que debía ser adaptada a éste).

Finalmente, convendría mencionar el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018<sup>53</sup>, relativo a la protec-

---

51. DOUE, núm. 119, de 4 de mayo de 2016.

52. DOUE núm. 119, de 4 de mayo de 2016.

53. DOUE núm. 295, de 21 de noviembre de 2018.

ción de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE.

Y el siguiente hito ha sido el Reglamento Europeo de Inteligencia Artificial de 2024<sup>54</sup> al que me he referido anteriormente.

### 3.3. Jurisprudencia

Como se ha comentado anteriormente, el Tribunal de Justicia de la Unión Europea ha jugado un papel muy relevante en la protección de los derechos fundamentales frente a las nuevas tecnologías, hasta el extremo de llegar a «crear» nuevos derechos digitales, el más famoso de los cuales es el «derecho al olvido», en su famosa Sentencia de 13 de mayo de 2014, en el *caso Google Spain S.L. y Google Inc. contra la Agencia Española de Protección de Datos y Mario Costeja González*<sup>55</sup>, al resolver una cuestión prejudicial planteada por la Audiencia Nacional española en relación la Directiva 95/46, que se ha convertido en un «leading case» en la materia.

El problema planteado en ella era el siguiente: cuando un internauta introducía el nombre del Sr. Costeja González en el motor de búsqueda de Google, obtenía como resultado vínculos hacia dos páginas del periódico La Vanguardia, del 19 de enero y del 9 de marzo de 1998, respectivamente, en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre del Sr. Costeja González. El Sr. Costeja solicitó que se exigiese al periódico eliminar o modificar la publicación para que no apareciesen sus datos personales, o utilizar las herramientas facilitadas por los motores de búsqueda para proteger estos datos. Por otro lado, solicitó que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia. Y todo ello porque el Sr. Costeja afirmaba que el embargo al que se vio sometido en su día estaba totalmente solucionado y resuelto desde hace años y carecía de relevancia actualmente.

Mediante resolución de 30 de julio de 2010, la Agencia Española de Protección de Datos (AEPD) desestimó la reclamación en la medida en que se refería

---

54. Reglamento (UE) 2024/1689 del Parlamento y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) 300/2008, (UE), 167/2013, (UE), 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), publicado en el DOUE núm. 1689, de 12 de julio de 2024.

55. Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, en el *caso Google Spain S.L. y Google Inc. contra la Agencia Española de Protección de Datos y Mario Costeja González*, Asunto C-131/12. ECLI:EU:C:2014:317.

a La Vanguardia, al considerar que la publicación que ésta había llevado a cabo estaba legalmente justificada, dado que había tenido lugar por orden del Ministerio de Trabajo y Asuntos Sociales y tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores.

En cambio, estimó la misma reclamación en la medida en que se dirigía contra Google Spain y Google Inc. A este respecto, la AEPD consideró que quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y que actúan como intermediarios de la sociedad de la información. La AEPD consideró que estaba facultada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los gestores de motores de búsqueda cuando considere que su localización y difusión puede lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona entendida en un sentido amplio, lo que incluye la mera voluntad del particular afectado cuando quiere que tales datos no sean conocidos por terceros. La AEPD estimó que este requerimiento puede dirigirse directamente a los explotadores de motores de búsqueda, sin suprimir los datos o la información de la página donde inicialmente está alojada, incluso cuando el mantenimiento de esta información en dicha página esté justificado por una norma legal. Google Spain y Google Inc. interpusieron sendos recursos contra dicha resolución ante la Audiencia Nacional, que fue quien presentó la cuestión prejudicial ante el TJUE. En esta Sentencia, el TJUE creó en la práctica el denominado «derecho al olvido» y sentó jurisprudencia en el sentido de que los derechos fundamentales de la vida privada y de protección de datos personales «prevalecen con carácter general» y «en principio» sobre el interés del público en tener acceso a dicha información.

También hay que destacar la Sentencia (Gran Sala) de 10 de julio de 2018, *Tietosuojavaluutettu*, Asunto C-25/17<sup>56</sup>. Se trataba de una cuestión prejudicial planteada por el Tribunal Supremo de lo Contencioso-Administrativo de Finlandia, en relación con el art. 3 de la Directiva 95/46 y con el art. 20 de la Carta de los Derechos Fundamentales de la Unión Europea. El asunto planteado era analizar la legalidad de una Resolución de la Comisión de Protección de Datos finlandesa que prohibía a la Comunidad de los Testigos de Jehová recoger o tratar datos personales en relación con la actividad de predicación puerta a puerta, sin que concurriesen los requisitos de la legislación finlandesa relativa al tratamiento de datos personales. El Tribunal declaró que una comunidad religiosa es responsable, junto con sus miembros de los tratamientos de datos personales efectuados por estos últimos en relación con una actividad de predicación puerta a puerta organizada, coordinada y fomentada por dicha comunidad, sin que sea necesario que la comunidad tenga acceso a los datos ni haga falta demostrar que ha impartido a sus miembros instrucciones por escrito o consignas en relación con esos tratamientos.

---

56. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 10 de julio de 2018, *Tietosuojavaluutettu*, Asunto C-25/17. ECLI:EU:C:2018:551.

En la Sentencia (Gran Sala) de 2 de octubre de 2018, *Ministerio Fiscal de España*, Asunto C-207/16<sup>57</sup>, se resolvió una cuestión prejudicial presentada por Audiencia Provincial de Tarragona, en un recurso interpuesto por el Ministerio Fiscal español contra la resolución del Juzgado de Instrucción n.º 3 de Tarragona, que denegaba el acceso de la Policía Judicial a datos personales almacenados por proveedores de servicios de comunicaciones electrónicas en aplicación de la Directiva 2002/58. El Tribunal dijo que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, consagrados en la Carta de los Derechos Fundamentales que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

En la Sentencia de 24 de septiembre de 2019, *GC y otros contra la Comisión Nacional de la Informática y de las libertades (CNIL)*, Asunto C-136/17<sup>58</sup>, el Tribunal resolvió una cuestión prejudicial presentada por el Consejo de Estado francés en relación con la interpretación de la Directiva 95/46 CE. Cuatro personas habían solicitado a Google que retirara diversos enlaces a páginas web publicadas por terceros de la lista de resultados obtenida por el motor de búsqueda gestionado por esta sociedad tras una búsqueda efectuada a partir de sus respectivos nombres, a lo que dicha sociedad se negó. Contra dicha negativa, presentaron sendas denuncias ante la CNIL, que fueron archivadas. Contra las decisiones de archivo de la CNIL, recurrieron al Consejo de Estado francés, que presentó la cuestión prejudicial. El Tribunal de Justicia entendió que el derecho a la protección de datos personales no constituye un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales con arreglo al principio de proporcionalidad, entre otros, la libertad de información de los internautas potencialmente interesados en acceder a esa página web mediante tal búsqueda, libertad garantizada por el artículo 11 de la Carta de Derechos Fundamentales de la Unión Europea. Y concluyó que el gestor de un motor de búsqueda que reciba una solicitud de retirada de un enlace que dirige a una página web en la que se publican datos personales comprendidos en las categorías especiales a las que se refiere el artículo 8, apartados 1 y 5, de la Directiva, basándose en todos los elementos pertinentes del caso concreto y teniendo en cuenta la gravedad de la injerencia en los derechos fundamentales del interesado al respeto de la vida privada y a la protección de los datos personales consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, a la luz de

---

57. En la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 2 de octubre de 2018, *Ministerio Fiscal de España*, Asunto C-207/16. ECLI:EU:C:2018:788.

58. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 24 de septiembre de 2019, *GC y otros contra la Commission nationale de l'informatique et des libertés (CNIL)*, Asunto C-136/17. ECLI:EU:C:2019:773.

los motivos de interés público importantes a los que se refiere el artículo 8, apartado 4, de dicha Directiva y respetando los requisitos establecidos en esta disposición, deberá comprobar si la inclusión de dicho enlace en la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre del interesado es estrictamente necesaria para proteger la libertad de información de los internautas potencialmente interesados en acceder a esa página web mediante tal búsqueda, libertad consagrada en el artículo 11 de la Carta.

En la Sentencia de 24 de septiembre de 2019, *Google contra la Comisión Nacional de la Informática y de las Libertades (CNIL)*, Asunto C 507/17<sup>59</sup>, se resolvió otra cuestión prejudicial presentada por el Consejo de Estado francés en relación con la Directiva 95/46. En este caso, se trataba de un recurso de Google contra la CNIL francesa, que le había impuesto una multa de 100.000 euros al negarse a retirar enlaces de una lista de resultados en todas las extensiones de nombre de dominio de su motor de búsqueda. Se planteaba en ese caso el alcance territorial del derecho a la retirada de enlaces. En este caso, el Tribunal declaró que la Directiva 95/46 y el Reglamento 2016/679, deben interpretarse en el sentido de que, cuando el gestor de un motor de búsqueda estime una solicitud de retirada de enlaces en virtud de estas disposiciones, estará obligado a proceder a dicha retirada no en todas las versiones de su motor, sino en las versiones de este que correspondan al conjunto de los Estados miembros, combinándola, en caso necesario, con medidas que, con pleno respeto de las exigencias legales, impidan de manera efectiva o, al menos, dificulten seriamente a los internautas que efectúen una búsqueda a partir del nombre del interesado desde uno de los Estados miembros el acceso, a través de la lista de resultados que se obtenga tras esa búsqueda, a los enlaces objeto de la solicitud de retirada.

La Sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020, *Comisionado de Protección de Datos de Irlanda contra Facebook Irlanda*, asunto C 311/18<sup>60</sup>, tuvo su origen en una cuestión prejudicial presentada por el Tribunal Superior de Irlanda. El caso planteado era el siguiente: el Sr. Schrems era un ciudadano austríaco, usuario de Facebook. Todo usuario de Facebook en la Unión Europea debía firmar un contrato con Facebook Irlanda, filial de Facebook Inc. (situada en Estados Unidos). Los datos personales de usuarios de Facebook de la Unión son transferidos a Facebook Inc., que se encarga de su tratamiento. Pero el Sr. Schrems se oponía a que sus datos se transfiriesen a Facebook Inc., porque la normativa norteamericana obliga a poner a disposición de las autoridades de seguridad norteamericanas dichos datos, utilizándose en programas de vigilancia incompatibles con los derechos protegidos por la Carta de los Derechos Fundamentales de la Unión Europea. El Tribunal de Luxembur-

---

59. Sentencia de 24 de septiembre de 2019, *Google contra la Commission nationale de l'informatique et des libertés (CNIL)*, Asunto C 507/17. ECLI:EU:C:2019:772.

60. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 16 de julio de 2020, asunto C-311/18, *Data Protection Commissioner y Facebook Ireland y Maximilian Schrems*. ECLI:EU:C:2020:559.

go dijo que está comprendida dentro del ámbito de aplicación del Reglamento Europeo de Protección de Datos una transferencia de datos personales realizada con fines comerciales por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero, a pesar de que, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades del país tercero en cuestión con fines de seguridad nacional, defensa y seguridad del Estado. Y que debe garantizarse que los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión Europea por el referido Reglamento, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea.

La Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2020, *Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros*, Asunto C-623/17<sup>61</sup>, se respondió a una cuestión prejudicial planteada por el Tribunal de las Facultades de Investigación del Reino Unido, interpretando, una vez más la Directiva 2002/58, modificada por la Directiva 2009/136. El caso se refería a un Informe del Comité de Información y Seguridad del Parlamento británico que recogía prácticas de recopilación y utilización de datos de comunicaciones masivos por parte de las distintas agencias de seguridad e inteligencia del Reino Unido, por lo que la ONG Privacy International interpuso una demanda ante el Tribunal de las Facultades de Investigación del Reino Unido contra el Foreign Office (Ministerio de Asuntos Exteriores y de la Commonwealth), Home Office (Ministerio del Interior) y las mencionadas agencias de seguridad en las que impugnaba estas prácticas. El Tribunal entendió que está comprendida en el ámbito de aplicación de esta Directiva una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a transmitir a las agencias de seguridad e inteligencia datos de tráfico y de localización con el fin de proteger la seguridad nacional y que la Directiva debe interpretarse en el sentido de que se opone a una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a realizar una transmisión generalizada e indiferenciada de datos de tráfico y de datos de localización a las agencias de seguridad e inteligencia con el fin de proteger la seguridad nacional.

En la Sentencia del Tribunal de Justicia (Gran Sala) de 2 de marzo de 2021, *H.K.*, Asunto C-746/18<sup>62</sup>, se respondió a una cuestión prejudicial presentada por el Tribunal Supremo de Estonia, en relación con la Directiva 2002/58, modificada por la Directiva 2009/136 y la Carta de los Derechos Fundamentales de la

---

61. Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2020, *Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros*, Asunto C-623/17. ECLI:EU:C:2020:790.

62. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 2 de marzo de 2021, *H.K.*, Asunto C-746/18. ECLI:EU:C:2021:152.

Unión Europea. En este caso, se trataba de un proceso penal incoado a la Sra H.K. por los cargos de robo, utilización de la tarjeta bancaria de un tercero y violencia contra los intervinientes en un procedimiento judicial. La condena se basaba en varios atestados confeccionados a partir de datos relativos a las comunicaciones electrónicas, obtenidos con arreglo a la normativa estonia, recabados por la autoridad investigadora de un proveedor de servicios de telecomunicaciones electrónicas durante el procedimiento de instrucción, después de haber obtenido la autorización de la Fiscalía. El Tribunal de Justicia entendió que el derecho de la Unión Europea se opone a una normativa nacional que autoriza el acceso de autoridades públicas a un conjunto de datos de tráfico o de localización que pueden facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice y permitir extraer conclusiones precisas sobre su vida privada, a efectos de la prevención, la investigación, el descubrimiento y la persecución de delitos, sin que dicho acceso se limite a procedimientos que tengan por objeto la lucha contra la delincuencia grave o la prevención de amenazas graves contra la seguridad pública, y ello con independencia de la duración del período para el que se solicite acceder a los citados datos y de la cantidad o naturaleza de los datos disponibles en ese período. Y además, estableció que el derecho europeo también se opone a una normativa nacional que atribuye competencia a la Fiscalía —cuya función es dirigir el procedimiento de instrucción penal y ejercer, en su caso, la acusación pública en un procedimiento posterior— para autorizar el acceso de una autoridad pública a los datos de tráfico y de localización a efectos de la instrucción penal.

Por su parte, en la Sentencia del Tribunal de Justicia (Gran Sala) de 20 de septiembre de 2022, *Alemania contra SpaceNet AG y Telekom Deutschland GmbH*, Asuntos C-793/19 y C- 794/19<sup>63</sup>, se resolvió una cuestión prejudicial planteada por el Tribunal Supremo de lo Contencioso-Administrativo de Alemania, que tuvo origen en los litigios entre la Agencia Federal de las Redes de Electricidad, Gas, Telecomunicaciones, Correos y Ferrocarriles de Alemania y las empresas SpaceNet AG y Telekom Deutschland AG, en relación con la obligación impuesta a estas últimas de conservar datos de tráfico y de localización relativos a las telecomunicaciones de sus clientes y la interpretación de la Directiva 2002/58, modificada por la Directiva 2009/136.

El Tribunal de Justicia dijo que la normativa europea se opone a que la legislación nacional establezca, con carácter preventivo y a los efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, la conservación generalizada e indeferenciada de datos de tráfico y de localización relativos a las telecomunicaciones de sus clientes. Pero no se opone a las medidas legislativas nacionales:

---

63. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 20 de septiembre de 2022, *Alemania contra SpaceNet AG y Telekom Deutschland GmbH*, Asuntos C-793/19 y C- 794/19.

- que permitan, a efectos de la protección de la seguridad nacional, recurrir a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas para que procedan a una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en situaciones en las que el Estado miembro en cuestión se enfrenta a una amenaza grave para la seguridad nacional que resulte real y actual o previsible, pudiendo ser objeto la decisión que contenga dicho requerimiento de un control efectivo bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter vinculante, que tenga por objeto comprobar la existencia de una de estas situaciones, así como el respecto de las condiciones y de las garantías que deben establecerse, y teniendo en cuenta que dicho requerimiento únicamente podrá expedirse por un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse en caso de que persista dicha amenaza;
- que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las amenazas graves contra la seguridad pública, una conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse;
- que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario;
- que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia y de la protección de la seguridad pública, una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas, y
- que permitan, a efectos de la lucha contra la delincuencia grave y, *a fortiori*, de la protección de la seguridad nacional, recurrir a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan estos proveedores de servicios, siempre que dichas medidas garanticen, mediante normas claras y precisas, que la conservación de los datos en cuestión está supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas disponen de garantías efectivas contra los riesgos de abuso.

En la Sentencia del Tribunal de Justicia (Gran Sala) de 8 de diciembre de 2022, *TU RE contra Google LLC.*, Asunto C-460/20<sup>64</sup>, el Tribunal analizó el caso a partir de una cuestión prejudicial planteada por el Tribunal Supremo de lo Civil y Penal de Alemania, en relación con el Reglamento Europeo de Protección de Datos 2016/679 y en relación con la Carta de los Derechos fundamentales de la Unión Europea. El fondo del asunto era un litigio entre TU y RE, por una parte, y Google LLC, por otra, respecto a la solicitud de que, por un lado, se retiraran de los resultados obtenidos tras una búsqueda efectuada a partir de sus nombres los enlaces a determinados artículos en los que se los identificaba y, por otro lado, se suprimieran de los resultados de una búsqueda de imágenes fotografías, mostradas en forma de imágenes de previsualización en miniatura (thumbnails), que los representan.

Se plantea aquí, el clásico debate de cómo hacer compatibles en estos temas los derechos contenidos en los arts. 7 (respeto de la vida privada y familiar) y 8 (protección de datos de carácter personal) y 11 (libertad de expresión y de información) de la Carta. En este caso, el Tribunal dijo que en el marco de la ponderación que debe efectuarse entre los derechos recogidos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea y los recogidos en el artículo 11 de la Carta de los Derechos Fundamentales, a los efectos del examen de una solicitud de retirada de enlaces dirigida al gestor de un motor de búsqueda para que se suprima de la lista de resultados de una búsqueda el enlace a un contenido que incluye afirmaciones fácticas que la persona que ha formulado la solicitud considera inexactas, dicha retirada no está condicionada a una aclaración, al menos provisional, de la cuestión de la exactitud del contenido indexado en el marco de un recurso interpuesto por dicha persona contra el proveedor de contenidos. Y también dijo que al examinar una solicitud de retirada de enlaces dirigida al gestor de un motor de búsqueda para que se supriman de los resultados de una búsqueda de imágenes efectuada a partir del nombre de una persona física fotografías mostradas en forma de previsualizaciones que representan a dicha persona, procede atender al valor informativo de dichas fotografías con independencia del contexto de su publicación en la página web de la que procedan, pero teniendo en cuenta cualquier elemento textual que acompañe directamente a esas fotografías en los resultados de la búsqueda y que pueda arrojar luz sobre su valor informativo.

En la Sentencia del Tribunal (Sala Primera) de 12 de enero de 2023, *BE contra la Autoridad Nacional de Protección de Datos y Libertad de Información de Hungría*, asunto C-123/21<sup>65</sup>, el Tribunal General de la capital de Hungría, planteó una cuestión prejudicial acerca de la interpretación de las vías de recurso en materia de protección de datos, derivadas de los artículos 77 y siguientes del

---

64. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 8 de diciembre de 2022, *TU RE contra Google LLC.*, Asunto C-460/20. ECLI:EU:C: 2022:962.

65. Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera) de 12 de enero de 2023, en el caso *BE contra Nemzeti Adatvédelmi és Információszabadság Hatóság* (Autoridad Nacional de Protección de Datos y Libertad de Información de Hungría), asunto C-123/21.

Reglamento Europeo de Protección de Datos (Reglamento UE 2016/679). El Tribunal contestó que dichos artículos deben interpretarse en el sentido de que permiten un ejercicio concurrente e independiente de las vías de recurso previstas, por una parte, en los citados artículos 77, apartado 1, y 78, apartado 1, y, por otra parte, en el referido artículo 79, apartado 1. Corresponde a los Estados miembros, de acuerdo con el principio de autonomía procesal, establecer la forma de articular estas vías de recurso para salvaguardar la efectividad de la protección de los derechos garantizados por dicho Reglamento, la aplicación coherente y homogénea de las disposiciones de este y el derecho a la tutela judicial efectiva consagrado en el artículo 47 de la Carta de los Derechos Fundamentales.

En otra Sentencia del Tribunal (Sala Primera), de 12 de enero de 2023, *RW contra Correos de Austria*, asunto C-154/21<sup>66</sup>, el Tribunal analizó una cuestión prejudicial presentada por el Tribunal Supremo de lo Civil y de lo Penal de Austria, en un litigio entre el Sr. RW y Correos de Austria, en relación con una solicitud de acceso a datos personales, en virtud del art. 15.1.c) del Reglamento europeo de Protección de Datos 2016/679. El Tribunal considera que dicho artículo ha de interpretarse en el sentido de que el derecho de acceso del interesado a los datos personales que le conciernen, establecido en dicha disposición, implica, cuando esos datos hayan sido o vayan a ser comunicados a destinatarios, la obligación del responsable del tratamiento de facilitar a ese interesado la identidad de esos destinatarios, a menos que no sea posible identificarlos o que dicho responsable del tratamiento demuestre que las solicitudes de acceso del interesado son manifiestamente infundadas o excesivas en el sentido del artículo 12, apartado 5, del Reglamento 2016/679, en cuyo caso este podrá indicar al interesado únicamente las categorías de destinatarios de que se trate.

En la Sentencia del Tribunal (Sala Quinta) de 26 de enero de 2023, , en el caso de *VS*<sup>67</sup>, Asunto C-205/21, el Tribunal respondió a una cuestión prejudicial planteada por el Tribunal Penal especial de Bulgaria en un procedimiento penal contra V.S., en relación con la Directiva (UE) 2016/680, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. En relación con los artículos 47 (derecho a la tutela judicial efectiva y a un juez imparcial) y 48 (presunción de inocencia y derechos de la defensa) de la Carta de Derechos Fundamentales de la Unión Europea, la Directiva ha de interpretarse en el sentido de que no se oponen a una normativa nacional que establece que, en caso de que la persona investigada por un delito público doloso se niegue a colaborar voluntariamente

---

66. Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera), de 12 de enero de 2023, *RW contra Österreichische Post AG* (Correos de Austria), asunto C-154/21. ECLI:EU:C:2023:3.

67. Sentencia del Tribunal de Justicia de la Unión Europea (Sala Quinta) de 26 de enero de 2023, en el caso *VS*, , Asunto C-205/21. ECLI: EU:C: 2023:49.

en la recogida de sus datos biométricos y genéticos a efectos de su registro, el órgano jurisdiccional penal competente esté obligado a autorizar una medida de recogida forzosa, sin poder apreciar si existen motivos fundados para presumir que el interesado ha cometido la infracción penal por la que es investigado, siempre que el Derecho nacional garantice posteriormente el control jurisdiccional efectivo de las condiciones de esa investigación, de la que deriva la autorización para la recogida. Pero la interpretación de la Directiva sí se opone a una normativa nacional que establece la recogida sistemática de datos biométricos y genéticos de cualquier persona investigada por un delito público doloso a efectos de su registro, sin obligar a la autoridad competente a comprobar y demostrar, por una parte, si esa recogida es estrictamente necesaria para satisfacer los objetivos concretos perseguidos y, por otra parte, si tales objetivos no pueden lograrse mediante medidas que constituyan inferencias menos graves en los derechos y libertades del interesado.

En la Sentencia del Tribunal (Sala Primera), de 4 de mayo de 2023, *F.F. contra la Autoridad de Protección de Datos de Austria*<sup>68</sup>, asunto C-487/21, el Tribunal se pronuncia sobre una cuestión prejudicial planteada por el Tribunal Federal de lo Contencioso-Administrativo de Austria, en relación con la interpretación del art. 15.3. del Reglamento General de Protección de Datos sobre el derecho de acceso del interesado a sus datos objeto de tratamiento, y en concreto, sobre la entrega de una copia de los datos y el concepto de «copia». El Tribunal insiste en que dicho artículo debe interpretarse en el sentido de que el derecho a obtener del responsable del tratamiento una copia de los datos personales objeto de tratamiento implica que se entregue al interesado una reproducción auténtica e inteligible de todos esos datos. Este derecho incluye el de obtener copia de extractos de documentos, o incluso de documentos enteros, o de extractos de bases de datos, que contengan, entre otros, dichos datos, si la entrega de tal copia es indispensable para permitir al interesado ejercer efectivamente los derechos que le confiere ese Reglamento, debiendo tenerse en cuenta también los derechos y libertades de los terceros.

Finalmente, me referiré a la Sentencia del Tribunal (Sala Primera) de 22 de junio de 2023, *Pankki S.*, asunto C-579/21<sup>69</sup>, en la que el Tribunal se pronuncia sobre una cuestión prejudicial planteada por el Tribunal de lo Contencioso-Administrativo de Finlandia Oriental, acerca de la interpretación de los arts. 4 y 15 del Reglamento General de Protección de Datos. El Sr JM, empleado y cliente del Banco Pankki S., que luego fue despedido del Banco, tuvo conocimiento de que sus datos como cliente habían sido consultados por el Banco y pidió información acerca de qué empleados del Banco los habían consultado. El Banco se negó a facilitar la identidad de los empleados porque consideraba que esa información

---

68. Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera), de 4 de mayo de 2023, *F.F. contra la Autoridad de Protección de Datos de Austria*, asunto C-487/21. ECLI:EU:C:2023:369.

69. Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera) de 22 de junio de 2023, *Pankki S.*, asunto C-579/21. ECLI:EU:C:2023:501.

aludía a datos personales de esos trabajadores. El Srl. JM recurrió al Supervisor Adjunto de Protección de Datos de Finlandia, que le denegó su solicitud de ordenar al Banco Pankki S., que le comunicase dicha información. Finalmente, el caso llegó al Tribunal de lo Contencioso-Administrativo de Finlandia Oriental, que planteó la cuestión prejudicial al Tribunal de Luxemburgo. El Tribunal de Justicia de la Unión Europea respondió que la información relativa a operaciones de consulta de datos personales de una persona, relativas a las fechas y a los fines de estas operaciones, constituye información que esa persona tiene derecho a obtener del responsable del tratamiento en virtud de esa disposición. En cambio, dicha disposición no consagra tal derecho en lo que respecta a la información relativa a la identidad de los empleados de dicho responsable que llevaron a cabo esas operaciones bajo su autoridad y de conformidad con sus instrucciones, a menos que esa información sea indispensable para permitir al interesado ejercer efectivamente los derechos que le confiere ese Reglamento y siempre bajo la condición de que se tengan en cuenta los derechos y libertades de esos empleados.

#### 4. ALGUNOS EJEMPLOS DE REGULACIONES NACIONALES DE LOS DERECHOS DIGITALES

Como estamos viendo, la regulación de los asuntos relacionados con los derechos en Internet o con los derechos digitales comenzó con la aprobación de Líneas Directrices o Resoluciones adoptadas por distintas organizaciones internacionales, que supusieron un gran paso adelante, pero que no dejaban de ser *soft law*<sup>70</sup>.

Tenemos también otros precedentes a escala nacional como la Declaración de Derechos en Internet de la Cámara de Diputados Italiana del 26 de junio de 2015<sup>71</sup>, la Ley brasileña 12.965 de 23 de abril de 2014, sobre el establecimiento de principios, garantías, derechos y deberes para el uso de Internet<sup>72</sup> o las modificaciones constitucionales en México en 2013 y 2016<sup>73</sup>. Pero un paso de gigante, más cercano a nuestro contexto jurídico, y regulando ya estas materias a través de normas jurídicas vinculantes (*hard law*), lo dio la Ley francesa n°

---

70. Pensemos, por ejemplo, en las *Guidelines of the protection of privacy and transborder flows of personal data* de la OCDE, adoptadas en 1980, actualizadas en 2013, (pueden consultarse en <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>) (última consulta, 17 de abril de 2023), o en un documento tan relevante como la *Resolución del Consejo de Derechos Humanos de Naciones Unidas de 27 de junio de 2016, sobre Promoción, Promoción y Disfrute de los Derechos Humanos en Internet* ([https://ap.ohchr.org/documents/S/HRC/d\\_res\\_dec/A\\_HRC\\_32\\_L20.pdf](https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf)) (última consulta, 17 de abril de 2023).

71. [https://www.camera.it/application/xmanager/projects/leg17/commissione\\_internet/TESTO\\_ITALIANO\\_DEFINITIVO\\_2015.pdf](https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/TESTO_ITALIANO_DEFINITIVO_2015.pdf) (última consulta, 17 de abril de 2023).

72. ([https://eva.fing.edu.uy/pluginfile.php/99128/mod\\_resource/content/1/marco\\_%20civil%20internet.pdf](https://eva.fing.edu.uy/pluginfile.php/99128/mod_resource/content/1/marco_%20civil%20internet.pdf)) (última consulta, 17 de abril de 2023).

73. [https://www.dof.gob.mx/nota\\_detalle.php?codigo=5301941&fecha=11/06/2013#gsc.tab=0](https://www.dof.gob.mx/nota_detalle.php?codigo=5301941&fecha=11/06/2013#gsc.tab=0)  
[https://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM\\_ref\\_227\\_29ene16.pdf](https://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_227_29ene16.pdf) (última consulta, 17 de abril de 2023).

2016/1321, de 7 de octubre de 2016, para una República digital<sup>74</sup>, que crea un auténtico catálogo de derechos digitales, Ley en la que, de alguna manera, se inspiró la Ley Orgánica española 3/2018.

Esta Ley se promulgó después de un proceso de consulta nacional sobre temas digitales, iniciado en 2014, que continuó después con una consulta online del texto del Proyecto de Ley. Se trataba de fomentar la innovación y la economía digital y la promoción de una sociedad digital a todas las personas. Como ha escrito RALLO LOMBARTE<sup>75</sup>, «aborda un amplio y sistemático catálogo de derechos digitales: a) derecho de acceso a datos públicos y de interés general; b) derecho de acceso seguro para investigadores y estadísticos públicos; c) derecho de acceso libre a los resultados de la investigación pública; d) derecho a la neutralidad de la red; e) derecho a la portabilidad; f) derecho a información leal; g) derecho a la protección de datos personales; h) penalización de la revancha pornográfica que se produce cuando se publica contra alguien imágenes eróticas o pornográficas; i) derecho a la muerte digital decidiendo el destino de la información personal online ante servicios de internet y terceros de confianza; j) derecho al mantenimiento de la conexión a internet de las personas económicamente más desfavorecidas en caso de mora o impago, y k) garantía de accesibilidad digital de las Administraciones públicas».

En palabras del profesor castellonense, «Francia se ha convertido en un modelo de referencia y su legislación opera en todos los ámbitos: garantizando la dimensión prestacional mediante la neutralidad de la red, con un derecho de acceso universal sin brechas socioeconómicas, geográficas o por condiciones de vulnerabilidad; promoviendo el acceso al conocimiento digital mediante una estrategia decidida de open data; fortaleciendo derechos tradicionales como el de protección de datos o el secreto de las comunicaciones; incidiendo en el ámbito laboral mediante el derecho a la desconexión; persiguiendo conductas delictivas, y garantizando nuevos derechos como el de portabilidad o la muerte digital. La relevancia de estas iniciativas radica en que los poderes públicos franceses, lejos de sucumbir a los ineficientes impulsos autorregulatorios, han otorgado rango legal a estos derechos y a las obligaciones que derivan de los mismos». En este mismo sentido, hay que tener en cuenta la Carta portuguesa de derechos humanos en la era digital, que también tiene carácter vinculante<sup>76</sup>.

Y coincido plenamente con él: este es un paso decisivo porque ya no estamos hablando de códigos de autorregulación, recomendaciones, informes, guías, etc., en definitiva, soft law, sino de una auténtica norma jurídica de hard law que crea obligaciones y derechos subjetivos. Ese es el camino a seguir en el ámbito de los distintos países.

---

74. <http://www.legifrance.gouv.fr/eli/loi/2016/10/7/ECFI1524250L/jo/texte>, (última consulta, 17 de abril de 2023).

75. RALLO LOMBARTE, 2020: 110-120.

76. Lei n° 27/2021, de 17 de mayo. Carta Portuguesa de Direitos Humanos na era digital.

Diário da República, n° 95, de 17 de mayo de 2021. Serie I, págs. 5-10. <https://data.dre.pt/eli/lei/27/2021/05/17/p/dre> (última consulta, 29 de julio de 2023).

## **5. LA REGULACIÓN DE LOS «DERECHOS DIGITALES» EN EL ÁMBITO DE LA CONSTITUCIÓN ESPAÑOLA Y DE SU NORMATIVA DE DESARROLLO**

Pensemos en el derecho constitucional español: en este momento, la única referencia constitucional a estos derechos se encuentra en el artículo 18.4 de la Constitución de 1978 que establece que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Este texto que, sin duda, fue un gran avance en el momento en que se aprobó la Constitución, resulta claramente insuficiente hoy, aunque introduce una cláusula bastante abierta que, como veremos, ha utilizado posteriormente el legislador, para ir más allá de la simple protección de datos<sup>77</sup>. Probablemente, la mejor solución sería reformar la Constitución para incluir los nuevos derechos digitales, pero, como es bien conocido, la extraordinaria rigidez del procedimiento establecido en el artículo 168 de la Constitución española para introducir cualquier modificación de la Constitución en el ámbito de los derechos fundamentales recogidos en la sección primera del capítulo II del Título I hace prácticamente inviable una modificación constitucional en este sentido.

El legislador español ha utilizado una discutible vía (al menos desde el punto de vista de la ortodoxia jurídica de la teoría de fuentes del derecho) para introducir esos derechos digitales en nuestro ordenamiento jurídico: el cauce de una Ley Orgánica, la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales, «adaptando», por decirlo de alguna manera, el 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 sus datos personales y a la libre circulación de estos datos. En primer lugar, podríamos preguntarnos por qué hay que dictar una normativa de derecho interno para garantizar la aplicación de un Reglamento europeo que, por sí mismo, tiene eficacia directa en todos los países de la Unión Europea. Y a este respecto, la argumentación ofrecida en el Preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, parece bastante discutible<sup>78</sup>.

---

77. Como ocurrió con la regulación introducida por la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, que fue sustituida por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Por último, y con motivo de la aprobación del 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 sus 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), se aprobó la actualmente vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, a la que me referiré inmediatamente.

78. El Preámbulo de la Ley Orgánica, en su apartado III, dice que «el Reglamento general de protección de datos contiene un buen número de habilitaciones, cuando no imposiciones, a los

Y, en segundo lugar, también resulta dudosa la técnica de incluir en el título X de la Ley Orgánica un elenco de derechos digitales. Esos derechos, deberían estar en la propia Constitución y no en una Ley Orgánica, por mucho que se quieran hacer «colgar» de la cláusula abierta del artículo 18.4 de la Constitución. La propia justificación que aparece en el Preámbulo de la Ley, pasa de puntillas, sobre este tema, con una, a mi juicio, demasiado escueta explicación del procedimiento seguido<sup>79</sup>. Y a este respecto se podrá decir: claro que lo ideal sería modificar la Constitución, pero visto que ello es muy difícil, dado el procedimiento establecido para ello en el artículo 168 de la misma, ¿qué otra cosa se podía hacer si se quieren regular los derechos digitales en un instrumento jurídico con auténtico valor jurídico (*hard law*) y no solamente instrumentos jurídicos sin fuerza legal vinculante (*soft law*)?<sup>80</sup> La pregunta es pertinente, pero aún así, sigo dudando de la corrección jurídica de la solución jurídica adoptada. En otras palabras, se puede «estirar» la interpretación del art. 18.4 de la Constitución («la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»), pero no sé si se puede «estirar» tanto,

---

Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión Europea que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión. En este punto hay que subrayar que no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Así, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico. En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada «mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse» (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia). Por último, los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea. La adaptación al Reglamento general de protección de datos, que será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual».

79. En su apartado V, la Exposición de Motivos de la Ley dice al respecto que: «Finalmente, el Título X de esta ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución».

80. A este respecto, puede consultarse BARRIO ANDRÉS, 2021: 197 y ss.

porque incluso la flexibilidad constitucional tiene sus límites. Y podríamos hacernos algunas preguntas como éstas: además de regular los derechos clásicos («analógicos») desde el punto de vista del nuevo contexto digital ¿se pueden crear nuevos derechos fundamentales, es decir, derechos subjetivos y, por tanto, plenamente exigibles ante los Tribunales, en una Ley Orgánica, sin modificar la Constitución?, ¿no sería esto es una modificación encubierta de la Constitución?, o acaso ¿una mutación constitucional?

Es cierto que en los Estatutos de Autonomía españoles de última generación se han incluido declaraciones de derechos que crean auténticos derechos subjetivos (por poner un ejemplo, en materia de vivienda), eso sí, solamente aplicables en la Comunidad Autónoma a la que se refiere el Estatuto de Autonomía y ello ha sido aceptado por el Tribunal Constitucional, pero ahora hemos dado un paso más: crear derechos fundamentales nuevos por Ley Orgánica, no previstos en la Constitución, utilizando una redacción un tanto abierta del artículo 18.4 de la Constitución, ante la imposibilidad práctica de modificar la Constitución para introducirlos en su texto, como en buena técnica jurídica debería hacerse. Una vez más, se pone de manifiesto los problemas que el procedimiento de reforma constitucional previsto en el artículo 168 de la Constitución provoca: es tan garantista y tan rígido en materia de reforma constitucional, que en puede impedir que la Constitución evolucione como debería, que se petrifique y que se convierta en algo obsoleto. La reforma constitucional pretende proteger la supremacía constitucional, pero «protegerla» tanto, puede llegar a «petrificarla», impedir que se actualice y se convierta en un instrumento jurídico cada vez menos útil.

La realidad es bastante terca, y si hay que regular nuevas realidades y la Constitución es tan rígida, habrá que buscar soluciones alternativas, porque la interpretación jurisprudencial tiene sus límites y la «ingeniería constitucional» (como, por ejemplo, crear derechos fundamentales nuevos por Ley orgánica con un fundamento constitucional endeble), también. Y todo esto se parece bastante a lo que en derecho constitucional denominamos «mutación constitucional». En palabras de RECHE TELLO Y TUR AUSINA, «... es, si se quiere y cuanto menos, una mutación constitucional que, ha de producirse en el contexto de un serio debate social, político y académico, aunque no se hayan llevado a cabo, por su propia naturaleza, los procedimientos «formales» que acompañan a los procesos de reforma constitucional expresa».<sup>81</sup>

Visto lo visto, el legislador orgánico introdujo los derechos digitales en el título X de la Ley Orgánica 3/2018, de 5 de diciembre<sup>82</sup>, que sí tiene pleno valor

---

81. RECHE TELLO / TUR AUSINA, 2022: 15.

82. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (Boletín Oficial del Estado, n° 294, de 6 de diciembre de 2018), artículos 79-97.

normativo (*hard law*)<sup>83</sup>. Como ha escrito con toda razón Rallo Lombarte<sup>84</sup>, esta Ley «... constituye un salto cualitativo en la necesidad de garantizar en la sociedad digital contemporánea derechos que garanticen la subordinación de la tecnología al individuo y que preserven su dignidad en la totalidad de ámbitos en que las personas actúan en sociedad». Pero resulta que esos derechos fueron ampliados en el marco de la Agenda Digital 2025, mediante la elaboración por parte del Gobierno español, de una Carta de Derechos Digitales de 2021<sup>85</sup>, que es un instrumento de *soft law*, es decir, que no tiene valor normativo y en la que aparecen agrupados los derechos de libertad, de igualdad, de participación y conformación del espacio público, los derechos del entorno laboral y empresarial, los denominados «derechos digitales en entornos específicos» (incluidos los derechos ante la Inteligencia Artificial y los derechos digitales en el empleo de las neurotecnologías).

El problema de la Carta de Derechos Digitales<sup>86</sup>, es que se trata de una norma de *soft law*. El apartado 6 de la Carta, dedicado a las garantías y eficacia de la misma, se ocupa de las garantías: en concreto el apartado 6.XVII, dice que todas las personas tienen derecho a la tutela administrativa y judicial de sus derechos en los entornos digitales, de acuerdo con la legislación vigente. También afirma que se promoverá la garantía de los derechos reconocidos en la Carta en el marco de la Administración de Justicia, en particular los derechos relacionados con la inteligencia artificial; que se promoverán mecanismos de autorregulación y procedimientos de resolución alternativa de conflictos (incluyendo incentivos para su utilización) y la evaluación de las leyes administrativas y procesales para ver si se adecuan a entorno digital. Y termina en su apartado 6.XXVIII, con una especie de «brindis al sol», con la habitual coletilla de que «el Gobierno adoptará las disposiciones oportunas, en el ámbito de sus competencias, para garantizar la efectividad de la presente Carta». Pero el problema es, precisamente, ese la falta de efectividad de la misma.

Y es que, como ocurre con la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital de 2023, a la que me referiré posteriormente, sigue tratándose de *soft law* y mientras sus contenidos no se incorporen a instrumentos con pleno valor normativo, la Carta de Derechos Digitales, puede tener valor interpretativo, pero no es fuente de derecho en nuestro sistema jurídico y los nuevos derechos que recoge no son derechos subjetivos, ni son alegables ante los Tribunales, mientras una norma no los recoja. Así que, actualmente, tenemos una amalgama de derechos digitales: unos que son auténticos derechos, los recogidos en la Ley Orgánica 3/2018, de 5 diciembre y otros, los recogidos en la Carta de Derechos Digitales de 2021, que no lo son, porque

---

83. Un detenido estudio de la Ley puede consultarse en: ARENAS RAMIRO / ORTEGA JIMÉNEZ, 2019; BERROCAL LANZAROT, 2020; GARCÍA MAHAMUT / TOMÁS MALLÉN, 2019 y TRONCOSO REIGADA, 2021.

84. RALLO LOMBARTE, 2020: 131.

85. <https://derechodigital.pre.red.es/> (última consulta, 16 de abril de 2023).

86. Para un estudio más detallado de la Carta de Derechos Digitales: COTINO HUESO, 2022.

carecen de eficacia jurídica. Todo esto resulta profundamente confuso y, obviamente, por razones de seguridad jurídica, convendría que estos derechos recogidos en la Carta de Derechos Digitales fueran regulados por una auténtica norma de *hard law*, bien a través de una reforma la Ley Orgánica 3/2018, o a través de una Ley nueva, descartada, de momento, por las razones que acabamos de ver, la reforma constitucional, o incluso tratar estos temas en Leyes específicas, aunque los problemas de encaje en el sistema de fuentes del ordenamiento jurídico español persisten.

Por ejemplo, para trasponer al ordenamiento jurídico español Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, se ha promulgado la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales<sup>87</sup>, que incluye la protección y la prevención frente a las amenazas contra la seguridad pública, cuando dicho tratamiento se lleve a cabo por los órganos que, a efectos de la Ley Orgánica, tengan la consideración de autoridades competentes y cuya finalidad principal es que los datos sean tratados por estas autoridades competentes de manera que se cumplan los fines previstos y para establecer mayores estándares de protección de los derechos fundamentales y las libertades de los ciudadanos, en cumplimiento del artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea, del artículo 16.1 del Tratado de Funcionamiento de la Unión Europea y, por supuesto, del artículo 18.4 de la Constitución.

También se pueden citar, en este mismo sentido, las novedades introducidas por normas laborales recientes, como la Ley 10/2021, de 9 de julio, de trabajo a distancia<sup>88</sup> y su regulación de los derechos relacionados con el uso de medios digitales, en sus artículos 17 y ss. (derecho a la intimidad y a la protección de datos o el derecho a la desconexión digital) y la Ley 12/2021, de 28 de septiembre<sup>89</sup>, que modifica el Estatuto de los Trabajadores, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de las plataformas digitales (la conocida como ley «rider»), en particular el

---

87. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Boletín Oficial del Estado, n° 126, de 27 de mayo de 2021.

88. Ley 10/2021, de 9 de julio, de trabajo a distancia. Boletín Oficial del Estado, n° 164, de 10 de julio de 2021.

89. Ley 12/2021, de 28 de septiembre, por la que se modifica el texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales. Boletín Oficial del Estado, n° 233, de 29 de septiembre de 2021.

nuevo artículo 64.4.d) del Estatuto de los Trabajadores, en relación con el derecho que tienen los trabajadores de recibir información por parte de la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles, incluyendo también una Disposición Adicional 23<sup>a</sup>, que presume la laboralidad en el ámbito de las plataformas digitales de reparto.

Finalmente, convendría citar también la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación<sup>90</sup> que, según su art. 3 será de aplicación en el ámbito de Internet, redes sociales y aplicaciones móviles (letra n) e inteligencia artificial y gestión masiva de datos, así como otras esferas de análoga significación (letra o) y regula en su artículo 23 la aplicación del principio de igualdad en relación con la inteligencia artificial y los algoritmos (mecanismos de toma de decisión automatizados) para evitar su potencial impacto discriminatorio<sup>91</sup>. Como ha escrito ARENAS RAMIRO<sup>92</sup>, la Ley se refiere al uso de algoritmos por parte del sector público (aunque evita referirse al sector privado), a la obligación de favorecer la puesta en marcha de mecanismos para que los algoritmos minimicen sesgos y se sometan a los principios de transparencia y rendición de cuentas, siempre que ello sea factible técnicamente. Y cuando habla de Inteligencia Artificial establece la obligación del sector público y a las empresas de promover el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales.

Como vamos viendo, ante la imposibilidad práctica de una pronta reforma de la Constitución en estas materias, el legislador, sea orgánico o sea ordinario, va abriendo paso a una regulación jurídica de estos nuevos fenómenos. Quizá la regulación sea dispersa y sería mejor una regulación exhaustiva sobre estas materias, pero al menos, tenemos una regulación de derecho positivo, que crean derechos y también obligaciones. Pero seguir con esta mezcla de auténticos derechos subjetivos con derechos que no lo son, de normas de *hard law* con normas de *soft law* resulta jurídicamente perturbador.

## **6. LA JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL ESPAÑOL EN LA MATERIA**

Finalmente, intentaré recoger brevemente algunas de las Sentencias a mi juicio más relevantes del Tribunal Constitucional en estas materias. Comenzaré

---

90. Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación. Boletín Oficial del Estado, n° 167, de 13 de julio de 2022.

91. AÑÓN ROIG, 2022: 17 y ss.

92. ARENAS RAMIRO, 2022: 132-133.

por la Sentencia 254/1993, de 20 de julio de 1993<sup>93</sup>. Se trata de un recurso de amparo promovido por un conocido político vasco que solicitó conocer los datos personales relativos a él en poder de la Administración del Estado. Su solicitud fue rechazada por la Administración por denegación presunta y dicha denegación fue confirmada por los Tribunales del orden jurisdiccional contencioso-administrativo. El recurrente entendía que ello violaba los artículos 18.1 y 18.4 de la Constitución. El Tribunal Constitucional le dio la razón y le concedió el amparo. Para ello, el Tribunal interpretó el artículo 18.4 de la Constitución, conjuntamente con el artículo 10.2 de la misma, según lo establecido en el artículo 8 del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, antes citado. Además de la protección de la intimidad desde el punto de vista de la no intromisión, la Sentencia añade unas facultades positivas y activas de información y de control y empezó a aproximarse a lo que el Tribunal Constitucional denominó como libertad informática denominada *libertad informática*, es decir, «un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama ‘la informática’».

Las Sentencias 290/2000 y 292/2000, ambas de 30 de noviembre de 2000<sup>94</sup>, resolvieron sendos recursos de inconstitucionalidad contra la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, presentados por el Consejo Ejecutivo de la Generalitat catalana, el Parlamento catalán, el Defensor del Pueblo y el Grupo Parlamentario Popular. Estas Sentencias tienen una gran importancia porque introdujeron una nueva visión interpretación del artículo 18.4 de la Constitución, entendiéndolo como *habeas data* e interpretándolo no tanto como un derecho vinculado a la intimidad o a la privacidad, —es decir, visto desde la óptica de impedir las intromisiones en el ámbito de la intimidad del interesado— sino más bien como un derecho fundamental de la personalidad, autónomo o independiente del derecho a la intimidad, aunque directamente relacionado con ella, esto es, como un poder de disposición y de control de la persona sobre sus datos personales, que le faculta para decidir cuáles de esos datos proporcionar a un tercera, sea una Administración Pública o un particular, o qué datos personal puede este

---

93. Sentencia del Tribunal Constitucional 254/1993, de 20 de julio de 1993. BOE, n° 197, de 18 de agosto de 1993. ECLI:ES:TC:1993:254. Tiene especial interés su fundamento jurídico n° 6 y esa doctrina se reitera en las Sentencias del Tribunal Constitucional 143/1994, de 9 de mayo (fundamento jurídico n° 7), 11/1998, de 13 de enero (fundamento jurídico n° 4), 94/1998, de 4 de mayo (fundamento jurídico n° 6) y 202/1999, de 8 de noviembre, fundamento jurídico n° 2).

94. Sentencias del Tribunal Constitucional 290/2000, de 30 de noviembre. ECLI:ES:TC:2000:290 y 292/2000 de 30 de noviembre. ECLI:ES:TC:2000:292, publicadas ambas en el BOE n° 4 de 4 de enero de 2001.

tercero recabar, y que también permite a cada persona saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso<sup>95</sup>.

---

95. En efecto, en los Fundamentos Jurídicos 5º, 6º y 7º de la STC 292/2000, se distingue claramente entre el derecho a la intimidad y el derecho a la protección de datos:

« 5. (...) Pues bien, en estas decisiones el Tribunal ya ha declarado que el art. 18.4 CE contiene, en los términos de la STC [254/1993](#), un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (FJ 6, reiterado luego en las SSTC [143/1994](#), FJ 7, [11/1998](#), FJ 4, [94/1998](#), FJ 6, [202/1999](#), FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC [11/1998](#), FJ 5, [94/1998](#), FJ 4).

6.: (...) La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC [144/1999](#), de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC [134/1999](#), de 15 de julio, FJ 5; [144/1999](#), FJ 8; [98/2000](#), de 10 de abril, FJ 5; [115/2000](#), de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC [170/1987](#), de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos

En la Sentencia de 96/2012, de 7 de mayo de 2012<sup>96</sup>, el Tribunal otorgó el amparo interpuesto por una entidad bancaria frente a la resolución judicial que ordenaba la entrega a una asociación de la la identificación completa de todos aquellos clientes que habían suscrito con dicha entidad bancaria determinados

---

personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC [73/1982](#), de 2 de diciembre, FJ 5; [110/1984](#), de 26 de noviembre, FJ 3; [89/1987](#), de 3 de junio, FJ 3; [231/1988](#), de 2 de diciembre, FJ 3; [197/1991](#), de 17 de octubre, FJ 3, y en general las SSTC [134/1999](#), de 15 de julio, [144/1999](#), de 22 de julio, y [115/2000](#), de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC [254/1993](#), FJ 7).

7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele».

96. Sentencia del Tribunal Constitucional 96/2012, de 7 de mayo de 2012, BOE nº 134, de 5 de junio de 2012. ECLI:ES:TC:2012:96.

productos financieros, para interponer una demanda colectiva. La entidad bancaria estimaba que tal resolución judicial vulneraba el derecho a la tutela judicial efectiva, el derecho a la intimidad y a la protección de datos personales. El Tribunal Constitucional otorgó el amparo por violación del derecho a la tutela judicial efectiva y a la protección de datos personales. En lo que se refiere a la protección de datos personales, entendió que pedir a una entidad bancaria la entrega de datos personales de sus clientes, sin el consentimiento previo de los mismos, para ponerlos a disposición de una asociación de consumidores implica un claro límite al derecho fundamental a la protección de datos de carácter personal que sólo se justificaría sobre la base de principios de motivación y proporcionalidad, imprescindibles para proteger derechos fundamentales frente a limitaciones o constricciones que proceden de normas o resoluciones singulares, lo que no ocurría en el caso concreto. El Tribunal reitera en sus fundamentos jurídicos 6º y 7º su doctrina sobre el derecho a la protección de datos.

En la Sentencia 58/2018, de 4 de junio de 2018<sup>97</sup>, el Tribunal resolvió un recurso de amparo en el que se planteó un caso en relación con la hemeroteca de El País Digital (que permitía recuperar una información el periódico de hacía veinte años en relación con el desmantelamiento de una red de tráfico de drogas y la condición de toxicómanas de las recurrentes en amparo, que habían sufrido síndrome de abstinencia durante su estancia en prisión). El Tribunal dio la razón a las personas demandantes de amparo y declaró que se habían violado sus derechos a la intimidad y a la protección de datos. El Tribunal reconoce expresamente un nuevo derecho digital, el derecho al olvido y considera que el derecho contenido en el artículo 17 del Reglamento General de Protección de Datos (derecho de supresión o derecho al olvido) es una vertiente del derecho a la protección de datos personales frente al uso de la informática del artículo 18.4 de la Constitución española y un mecanismo de garantía para la preservación de los derechos a la intimidad y al honor, con los que está directamente relacionado, si bien se trata de un derecho autónomo<sup>98</sup>.

---

97. Sentencia del Tribunal Constitucional 58/2018, de 4 de junio de 2018. Boletín Oficial del Estado nº 164, de 7 de julio de 2018. ECLI:ES:TC:2018:58.

98. Concretamente, dice en sus fundamentos jurídicos 5º y 6º:

«Lo que plantean las personas recurrentes en amparo, a través de la invocación del artículo 18.1 y 4 CE, es el ejercicio del denominado jurisprudencialmente «derecho al olvido» (conclusiones del Abogado General asunto Niilo Jääskinen, de 25 de junio de 2013, en el asunto Google Spain, S.L. y Google Inc. c. Agencia Española de Protección de Datos y Mario Costeja González y Sentencia del Tribunal de Justicia de 13 de mayo de 2014, en el asunto C 131/12 —asunto Google—).

Este es definido, exactamente bajo esta denominación, sólo en el artículo 17 del 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), norma europea que entró en vigor el 25 de mayo de 2018. Se concreta como el derecho a obtener, sin dilación indebida, del responsable del tratamiento de los datos personales relativos a una persona, la supresión de esos datos, cuando ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados; cuando se retire el consentimiento en que se basó el tratamiento; cuando la persona interesada se oponga al tratamiento; cuando los datos se hayan tratado de forma ilícita;

En la Sentencia 76/2019, de 22 de mayo de 2019<sup>99</sup>, el Tribunal resolvió favorablemente el recurso de inconstitucionalidad promovido por el Defensor del Pueblo contra el artículo 58 bis 1º de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado por la Disposición Final Tercera, apartado dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, que decía que «La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.» Este inciso fue declarado inconstitucional por el Tribunal Constitucional. Dicho apartado fue declarado inconstitucional por violación del derecho a la protección de datos, recogido en el art. 18.4 de la Constitución.

En palabras del propio Tribunal en el fundamento jurídico 9º de la Sentencia: «la ley no ha identificado la finalidad de la injerencia para cuya realización se habilita a los partidos políticos, ni ha delimitado los presupuestos ni las condiciones de esa injerencia, ni ha establecido las garantías adecuadas que para la debida protección del derecho fundamental a la protección de datos personales reclama nuestra doctrina, por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de

---

cuando se deba dar cumplimiento a una obligación legal establecida en el Derecho de la Unión o de los Estados miembros; o cuando los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información. En suma, en el Reglamento se viene a legislar de forma más clara el derecho a la supresión de los datos personales de una determinada base que los contuviera. Eso, y no otra cosa, es el derecho al olvido. Un derecho a la supresión de los datos personales, existente ya por obra de la Directiva 95/46/CE, estrechamente vinculado con la salvaguardia del derecho fundamental a la protección de datos personales frente al uso de la informática (art. 18.4 CE), y con la protección del artículo 8 de la Carta de los derechos fundamentales de la Unión Europea y del Convenio núm. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Así considerado, el derecho al olvido es una vertiente del derecho a la protección de datos personales frente al uso de la informática (art. 18.4 CE), y es también un mecanismo de garantía para la preservación de los derechos a la intimidad y al honor, con los que está íntimamente relacionado, aunque se trate de un derecho autónomo. (...) Por tanto, si las libertades informáticas pueden definirse como derecho fundamental, también lo es, porque se integra entre ellas, el derecho al olvido. Esta conclusión puede extraerse sin dificultad de la configuración que hace nuestra jurisprudencia del artículo 18.4 CE, al definirlo como un conjunto de derechos que el ciudadano puede ejercer «frente a quienes sean titulares, públicos o privados, de ficheros de datos personales» (STC [290/2000](#), FJ 7), y establecer que tales derechos son, entendidos como haz de facultades de su titular, el derecho a consentir la recogida y el uso de sus datos personales y a conocer los mismos, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, y el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos, esto es el derecho de supresión (en este sentido, STC [290/2000](#), FJ 7).

(...) Este reconocimiento expreso del derecho al olvido, como facultad inherente al derecho a la protección de datos personales, y por tanto como derecho fundamental, supone la automática aplicación al mismo de la jurisprudencia relativa a los límites de los derechos fundamentales».

99. Sentencia del Tribunal Constitucional 76/2019, de 22 de mayo de 2019. BOE nº 151 de 25 de junio de 2019. ECLI:ES:TC:2019:76.

sus actividades electorales. De esta forma, se han producido tres vulneraciones del art. 18.4 CE en conexión con el art. 53.1 CE, autónomas e independientes entre sí, todas ellas vinculadas a la insuficiencia de la ley y que solo el legislador puede remediar, y redundando las tres en la infracción del mandato de preservación del contenido esencial del derecho fundamental que impone el art. 53.1 CE, en la medida en que, por una parte, la insuficiente adecuación de la norma legal impugnada a los requerimientos de certeza crea, para todos aquellos a los que recopilación de datos personales pudiera aplicarse, un peligro, en el que reside precisamente dicha vulneración y, por otra parte, la indeterminación de la finalidad del tratamiento y la inexistencia de «garantías adecuadas» o las «mínimas exigibles a la Ley» constituyen en sí mismas injerencias en el derecho fundamental de gravedad similar a la que causaría una intromisión directa en su contenido nuclear».

En la Sentencia 27/2020, de 24 de febrero de 2020<sup>100</sup>, se plantéo un típico conflicto de derechos fundamentales, en este caso entre el derecho a la propia imagen y el derecho a la información, pero en el ámbito de las redes sociales. Un diario publicó un reportaje sobre un hecho violento en la que se incluía la fotografía de la persona agredida, tomada de su perfil de Facebook sin su autorización. Esta persona recurrió a los Tribunales ordinarios que confirmaron que se había violado su derecho a la propia imagen y condenaron a la editora del periódico. Ésta recurrió en amparo al Tribunal Constitucional, alegando violación de la libertad de información, pero el Tribunal rechazó el recurso de amparo porque entendió que no se pueden publicar informaciones o imágenes obtenidas de redes sociales sin consentimiento expreso de las personas afectadas. En los fundamentos jurídicos 3º y 4º de la Sentencia, el Tribunal se ocupa de lo relativo a la sociedad digital y a la utilización no autorizada de la propia imagen. En palabras del propio Tribunal: «aceptando que la aparición de las redes sociales ha cambiado el modo en el que las personas se socializan, hemos de advertir sin embargo —por obvio que ello resulte— que los usuarios continúan siendo titulares de derechos fundamentales y que su contenido continúa siendo el mismo que en la era analógica. Por consiguiente, salvo excepciones tasadas, por más que los ciudadanos compartan voluntariamente en la red datos de carácter personal, continúan poseyendo su esfera privada que debe permanecer al margen de los millones de usuarios de las redes sociales en Internet, siempre que no hayan prestado su consentimiento de una manera inequívoca para ser observados o para que se utilice y publique su imagen». Por eso el Tribunal rechaza expresamente que la «... existencia de autorización por el titular del derecho a la imagen para su uso por terceros por el solo hecho de haber publicado o «subido» una fotografía suya en su perfil de la red Facebook, cuya finalidad es la interrelación social con otros usuarios».

---

100. Sentencia del Tribunal Constitucional 27/2020, de 24 de febrero de 2020. BOE nº 83, de 26 de marzo de 2020. ECLI:ES:TC:2020:27.

En la Sentencia 8/2022, de 27 de enero de 2022<sup>101</sup>, se plantea la cuestión de la protección al derecho al honor y a la libertad de expresión en redes sociales y el problema de los *bulos* en Internet<sup>102</sup>. Se trata de un recurso de amparo, que el Tribunal desestimó planteado por un periodista que fue condenado civilmente por violación del derecho al honor por un mensaje publicado en su cuenta de la red social Twitter en el que afirmaba haber sido agredido por otro periodista que participaba en la misma tertulia radiofónica que él. Finalmente se demostró que no hubo tal agresión física y el Tribunal entendió que su mensaje no estaba amparado por la libertad de información, ya que la agresión no existió. En relación con la doctrina del Tribunal Constitucional sobre el derecho a la libertad de información en colisión con el derecho al honor en las redes sociales, el Tribunal, en el fundamento jurídico 3º de la Sentencia, se remite a la su Sentencia 27/2020, afirmando de nuevo que respecto al impacto que pueden tener las redes sociales en los derechos de la personalidad, «algunos contornos derechos fundamentales al honor, a la intimidad y a la propia imagen (art. 18 CE), garantes todos ellos de la vida privada de los ciudadanos, pueden quedar desdibujados y que la utilización masificada de estas tecnologías de la información y de la comunicación, unida a los cambios en los usos sociales que ellas mismas han suscitado, añaden nuevos problemas jurídicos a los ya tradicionales» (FJ 3), pero también lo es «que los usuarios continúan siendo titulares de derechos fundamentales y que su contenido continúa siendo el mismo que en la era analógica» (*ibidem*). Esta identidad de contenido no impide que se tengan en cuenta las particularidades que presentan las redes sociales a la hora de evaluar cómo los derechos de la personalidad actúan en tanto límites de las libertades de comunicación». Y a este respecto, el Tribunal analiza algunos elementos que hay que tener en cuenta acerca del derecho al honor como límite del ejercicio de las libertades de comunicación canalizadas a través de Internet y de las redes sociales (inmediatez, rapidez y amplitud en la difusión de sus contenidos; distintos tipos de autoría— es distinto el caso de quien crea el contenido, quien lo reproduce haciéndolo suyo o quien lo traslada sin más—; los destinatarios del mensaje y el contenido de los mensajes; la difusión on-line de ataques personales que van más allá del intercambio de ideas; y el posible efecto disuasorio del establecimiento del pago de indemnizaciones en relación con la libertad de expresión). En el caso concreto que analiza el Tribunal, y por mucho que el conflicto se desarrollase en el ámbito de una red social, dado que la información no era veraz, prevalece —como ocurre también en el ámbito *analógico*— el derecho al honor.

En la Sentencia 89/2022, de 29 de junio de 2022<sup>103</sup>, el Tribunal reafirma la doctrina contenida en la Sentencia 58/2018 en relación con el *derecho al olvido*. En este caso, se trataba de una solicitud de cancelación, a través de una recla-

---

101. Sentencia del Tribunal Constitucional 8/2022, de 27 de enero de 2022. BOE nº 46, de 23 de febrero de 2022. ECLI:ES:TC:2022:8.

102. Sobre esta cuestión, puede consultarse MOLINA MARTÍNEZ, 2023.

103. Sentencia del Tribunal Constitucional 89/2022, de 29 de junio de 2022. BOE nº 181, de 29 de julio de 2022. ECLI:ES:TC:2022:89.

mación dirigida por un particular a Google, pidiendo que sus datos personales no se asociasen en los resultados de su motor de búsqueda a tres direcciones de páginas de Internet que dirigían a unos comentarios que una usuaria había dejado en unos portales de queja de Internet en Estados Unidos. En dichas publicaciones aparecían los datos personales del recurrente y contenían comentarios negativos realizados por personas que, supuestamente, habían tenido relación con él y su empresa inmobiliaria. Dichos comentarios incluían términos descalificadores como «estafador», «timador», o «abusador de trabajadores». Google desestimó la petición, al entender que dichos comentarios podían tener interés público y que podían ser de interés para posibles clientes, usuarios o participantes en sus servicios. Recurrida dicha negativa a la Agencia Española de Protección de Datos (AEPD), ésta dio la razón al reclamante. Google recurrió la resolución de la AEPD a la Audiencia Nacional y el Tribunal le dio la razón a Google porque entendió que el derecho a la información, a la libertad de expresión y el interés general del público en acceder a la información sobre la actividad profesional del reclamante prevalecía sobre el derecho a la protección de datos. El Tribunal Supremo mantuvo el mismo criterio que la Audiencia Nacional y el reclamante presentó recurso de amparo ante el Tribunal Constitucional que, finalmente, le concedió el amparo (con un voto particular en sentido contrario suscrito por dos magistrados) y entendió que se había violado el artículo 18.4 de la Constitución, dando prioridad en este caso al *derecho al olvido*.

El Tribunal, en el fundamento jurídico 3º, menciona expresamente la Sentencia del Tribunal Europeo de Derechos Humanos de 25 de noviembre de 2021, *asunto Biancardi c. Italia y la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 asunto Google Spain* y expone cómo el denominado *derecho al olvido* o el *derecho al desindexado*, entendido como derecho a la supresión del uso de datos personales, puede verse significativamente afectado por los motores de búsqueda y encuentra sus límites en el resto de derechos fundamentales y bienes jurídicos constitucionalmente protegidos. En su fundamento jurídico 4º, alude a que han de ponderarse los derechos concurrentes (*derecho al olvido* y derecho de acceso a la información), así como la relevancia temporal de los datos en cuestión y siguiendo la jurisprudencia del Tribunal de Justicia de la Unión Europea establece que hay que presumir que, en principio, prevalece el *derecho al olvido* frente al derecho de acceso a la información, salvo que existan razones concretas en sentido contrario.

Se refiere también a la responsabilidad de los motores de búsqueda y dice que, una vez se ha recibido la solicitud de retirada de enlaces, el gestor del motor de búsqueda, deberá examinar si existe algún interés prevalente del público en el momento de la solicitud de acceder a dicha información y si el gestor del motor de búsqueda concluye que existe un interés prevalente del público en acceder a la información, le corresponderá examinar si la imagen global que deriva de la estructura de la lista de resultados es proporcionada o si debe reestructurar los enlaces para no afectar al derecho fundamental a la protección de datos personales. También se pronuncia sobre el alcance territorial del *derecho al olvido*.

En el caso concreto analizado en el recurso de amparo, el Tribunal descarta que exista un interés público superior que justifique la no prevalencia del *derecho al olvido* porque entiende que el acceso a los comentarios publicados no contribuye a la formación de la opinión pública: las informaciones, aunque descalifican al recurrente no tienen carácter difamatorio, pero la persona a la que se refieren no era una persona pública ni ha adquirido notoriedad pública, y la actividad que realizaba (la promoción inmobiliaria) no puede considerarse que constituya una actividad profesional que dote de relevancia pública a cualquier publicación relativa a cualquier profesional de dicho sector. Por otro lado, no estaríamos ante una publicación que tenga carácter informador o periodístico, sino ante plataformas en las que los usuarios publican y denuncian lo que ellos consideran fraudes y lo hacen de forma anónima. Además, el Tribunal señaló que, al tratarse de un enlace, la aplicación del criterio de relevancia pública debía ser más restrictivo, ya que su supresión no conllevaba la supresión de la web que contenía la información original. Y respecto a la antigüedad de los datos publicados, a juicio del Tribunal, en ninguno de los comentarios en Internet se hace alusión alguna a las informaciones contenidas en las noticias que se han tenido en cuenta por las resoluciones judiciales para sustentar la actualidad de las opiniones publicadas y que se refieren a un procedimiento judicial penal en el que está supuestamente incurso don M.J.L. Si bien dichas noticias sobre ese procedimiento penal podían ser actuales, y, en consecuencia, podían justificar un interés superior del público en acceder a las mismas, la actualidad no se trasladaba a las opiniones vertidas sobre el recurrente en los portales de quejas que no tenían por objeto esas diligencias penales. Por eso, en opinión de la mayoría del Tribunal, las resoluciones judiciales recurridas en amparo no habían aplicado correctamente los criterios de ponderación, vulnerándose así el derecho del recurrente a la protección de datos.

En la Sentencia 33/2023, de 18 de abril de 2023<sup>104</sup> se planteó un caso en el que un ciudadano presentó un recurso de amparo, tras las Sentencias del Juzgado de Primera Instancia nº 10 de Barcelona, Salas de lo Civil de la Audiencia Provincial de Barcelona y Sala de lo Civil del Tribunal Supremo, que desestimaron su demanda de protección civil de su intimidad y de su derecho a la propia imagen, puesto que la Policía Autonómica Catalana (Mossos d'Esquadra) había publicado en su página Web su fotografía solicitando la colaboración ciudadana contra la violencia urbana por su presunta implicación en unos disturbios que eran objeto de investigación. El argumento central de la demanda de amparo se refería a la intromisión ilegítima que supuso la publicación y difusión de la fotografía del recurrente en su derecho a la propia imagen, en conexión directa con el derecho a la protección de datos (art. 18.4 CE). El Tribunal no admitió a trámite el recurso de amparo por ser planteado fuera de plazo (fuera del de veinte días previsto por el artículo 43 de la Ley Orgánica del Tribunal Constitu-

---

104. Sentencia del Tribunal Constitucional 33/2023, de 18 de abril de 2023. BOE nº 121, de 22 de mayo de 2023. ECLI:ES:TC:2023:33.

cional) y no entró en el fondo del asunto. Aún así, la Sentencia contó con dos votos particulares, uno de ellos suscrito por dos magistrados, que consideran que el Tribunal debería haber entrado en el fondo del asunto.

En el voto particular de la magistrada Segoviano Astaburuaga, al que se adhirió el magistrado Sáez Valcárcel, se abogaba por haber admitido a trámite el recurso de amparo. Por su parte, en el voto particular de la magistrada Balaguer Callejón, ésta también defiende que el recurso debería haber sido admitido a trámite en virtud del artículo 44 (y no el 43) de la Ley Orgánica del Tribunal Constitucional, pero va más allá en su argumentación, entrando al fondo del asunto. En su opinión, era exigible que la publicación y la difusión de las imágenes en la web de la policía hubieran sido medidas expresamente y previstas en una norma de rango legal que reuniera las condiciones mínimas suficientes requeridas por las exigencias de seguridad jurídica y certeza del Derecho. Estas condiciones no concurrían en ese momento, porque la Directiva (UE) 2016/680 no había sido transpuesta al ordenamiento jurídico español en aquel momento, la publicación de dichas imágenes se había realizado sin autorización judicial y en su opinión, los órganos judiciales no realizaron adecuadamente el pertinente test de proporcionalidad.

Finalmente, en la Sentencia 83/2023, de 4 de julio de 2023<sup>105</sup> se resolvía un recurso de amparo planteado contra una Providencia del Tribunal Supremo que rechazó el incidente de nulidad de actuaciones contra una Sentencia de la Sala de lo Civil del mismo Tribunal que había desestimado el recurso de casación contra una Sentencia de la Audiencia Provincial de Málaga. El caso era el siguiente: una empresa de comunicación alojó en su página Web un enlace a una noticia externa que había sido publicada en un medio de comunicación digital en la que se hacía referencia a unos gastos realizados por el concejal de fiestas de una localidad malagueña. Con ocasión de la incorporación de este enlace al sitio web, varios usuarios redactaron y remitieron comentarios escritos en la sección expresamente habilitada para introducir mensajes relacionados con ese concreto contenido. En el segundo de ellos, un usuario se refirió al concejal llamándole «h... de p...», «ladrón» y «ladrón de toda la p... vida». Estos textos fueron incorporados al sitio web por sus responsables sin identificación de su autor y resultaban accesibles a cualquier usuario de la red. El concejal solicitó que los referidos comentarios fueran retirados o borrados del portal y que se le facilitara la identidad de sus autores, con apercibimiento de iniciar acciones legales de no ser atendida su reclamación. No fue respondido ni los comentarios fueron retirados, por lo que presentó demanda civil de protección al honor contra la empresa de comunicación.

La empresa responsable de la página Web contestó a la demanda rechazando toda responsabilidad por las noticias enlazadas en su sitio web y por los comentarios introducidos por los usuarios, diciendo que no tenía la condición de medio de comunicación sino de mero agregador de contenidos de internet que

---

105. Sentencia del Tribunal Constitucional 83/2023, de 4 de julio de 2023. ECLI:ES:TC:2023:83.

se limita a incorporar enlaces a noticias publicadas en medios ajenos y que los «calificativos» controvertidos constituyen mensajes procedentes de los usuarios de la página Web de la empresa, publicados por sus propios autores, no por la empresa responsable de la página Web y que, por tanto, eran de aplicación los arts. 16 y 17 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información, que establecen la inexistencia de responsabilidad de un prestador intermediario por los datos y enlaces introducidos por los usuarios, cuando no hay conocimiento efectivo de la ilicitud de los mismos.

El Juzgado de Primera Instancia consideró que los comentarios efectuados se enmarcaban en un contexto social de una profunda crisis económica y de una creciente preocupación por los numerosos casos de corrupción que existían en territorio nacional y que el carácter coloquial de las expresiones utilizadas, unido al ámbito más tolerable de la crítica en relación con las actuaciones de empleados públicos, han de considerarse amparados por el ejercicio de la libertad de expresión y que, por tanto, no había intromisión ilegítima en el derecho al honor. Sin embargo, la Audiencia Provincial de Málaga consideró que sí había intromisión en el derecho al honor, porque si bien había algunas expresiones que sí podían quedar amparadas por la libertad de expresión, había otras que eran claramente atentatorias contra el honor del concejal. La Sentencia de la Audiencia Provincial fue recurrida al Tribunal Supremo por la entidad propietaria de la Web, pero el Tribunal Supremo rechazó en su Sentencia el recurso de casación y la nulidad de actuaciones interpuesta contra su propia Sentencia.

La empresa responsable de la Web presentó entonces recurso de amparo ante el Tribunal Constitucional por vulneración de la tutela judicial efectiva y de libertad de expresión. El Tribunal rechazó el recurso (aunque se emitieron dos votos particulares uno concurrente con el criterio de la mayoría y otro discrepante). Me centraré en este sucinto comentario en lo relativo a la presunta vulneración de la libertad de expresión. A juicio del Tribunal Constitucional, lo que la entidad recurrente venía a decir es que rapidez e inmediatez con la que se entablan las comunicaciones en Internet, unido al elevadísimo volumen de datos que se mueven constantemente en dicha red electrónica, debe conducir, en la doctrina constitucional, a una suerte de equiparación de las comunicaciones entabladas en internet con las conversaciones orales que se producen en el contexto ordinario de la vida diaria. De este modo, proponía la demandante, que lo que es tolerable en una conversación oral debería ser considerado, igualmente, tolerable en el ámbito de Internet. Sin embargo, el Tribunal responde a este argumento diciendo que no puede aceptarse la consideración genérica de Internet como un contexto comunicativo puramente ocasional o trivial y que las específicas características del uso de Internet y redes sociales, así como del modo y difusión que alcanza el mensaje objeto de controversia, deben ser tenidas en cuenta en orden a concretar las reglas de delimitación entre derechos, para garantizar su promoción, pero también su debida protección. Y citando su propia Sentencia 92/2021, dijo que «si la conducta es lesiva del derecho al honor fuera de la red, también lo es en ella» y que la difusión en línea de ataques personales,

que sobrepasan el marco de un debate sobre las ideas, no está protegida por la libertad de expresión.

El Tribunal reitera su criterio de que incluso en el ámbito de la crítica política, donde los límites a la crítica son más amplios, la Constitución no reconoce un pretendido derecho al insulto, lo que significa que de la protección constitucional que otorga el art. 20.1 a) CE, están excluidas las expresiones absolutamente vejatorias, es decir, las que, en las concretas circunstancias del caso, y al margen de su veracidad, sean ofensivas o ultrajantes y resulten impertinentes para expresar las opiniones o informaciones de que se trate, porque quienes participan en la vida pública no quedan privados de ser titulares del derecho al honor. Por todo ello, rechazó el amparo entendiendo el carácter constitucionalmente ilegítimo, por innecesariamente vejatorio, de los comentarios publicados en la página web.

También tienen mucho interés, y por ello los menciono expresamente, los votos particulares emitidos con la Sentencia. En el voto particular concurrente con el criterio de la mayoría, formulado por los magistrados Sáez Valcárcel y Díez Bueso, se afirma que están de acuerdo con la denegación del amparo y con que la libertad de expresión no ofrece cobertura al puro insulto. Ambos magistrados opinan que la responsabilidad de la empresa propietaria de la Web no sólo deriva de no haber retirado los contenidos difamatorios, según lo establecido en el artículo 16.1 de la ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico, sino que la Sentencia debía haber incidido en su responsabilidad general por los mismos, porque, en su opinión, el régimen de dicha Ley sólo se aplica a «los operadores de la red que se limitan a aportar infraestructuras tecnológicas y técnicas, en la medida en que intervienen en el proceso de comunicación de manera neutral y sin controlar los datos, la información y las opiniones en cuya transmisión participan de modo «ciego», es decir, sin «conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero» (art. 16.1 ley 34/2002). Una actividad que se define como «meramente técnica, automática y pasiva», sin conocimiento ni control sobre la información, «cuando [el prestador del servicio] no tenga participación alguna en el contenido de los datos transmitidos», lo que requiere que no modifique los datos, salvo manipulaciones técnicas que no alteren su integridad (considerandos 42 y 43, Directiva 2000/31)». Consideran que esa Web «no es un simple intermediario técnico ni un operador neutral y pasivo y que lo importante es que la entidad realiza labores propias de edición, mucho más allá de la mera manipulación técnica que pide la norma. De actividad editorial se habla cuando se toman decisiones sobre qué se publica y qué se descarta, cuando se valoran las informaciones, se califican y ordenan con rúbricas, secciones y etiquetas (actualidad, política, cultura, ciencia, economía, series, artículos, portada, populares, más visitadas, nuevas, comunidades, fisgona, comentarios destacados, mejores hilos...), y se establecen prioridades, todo ello en función de algoritmos que responden a un código que se define en atención al interés mercantil. Toda esta actividad permite identificar a (dicha entidad) como un editor de contenidos y descartar que opere en el proceso de comunicación

de manera neutra, automática y pasiva». Y además, añaden, «La plataforma no solo no pide a sus usuarios que se identifiquen antes de divulgar contenidos, sino que tampoco facilita su identidad, que negó al titular del derecho al honor cuando se los reclamó. De esta manera, garantiza la total impunidad de quienes vulneran la reputación u otros derechos de terceros en su plataforma o medio de comunicación». Los magistrados echaron de menos un debate más profundo sobre todos estos asuntos en la Sentencia.

En el voto particular discrepante de la magistrada Balaguer Callejón, se defiende, por el contrario, que debería haber sido aceptado el recurso de amparo. En opinión de la magistrada, los términos empleados se enmarcaban en un mensaje común que iba dirigido directamente a censurar la información publicada y a expresar el descontento con la conducta en ella reflejada. Tal declaración, por lo tanto, guardaba relación directa con las circunstancias en las que el mensaje fue publicado y con las irregularidades que su destinatario presuntamente había cometido, siendo que en castellano el citado término —de uso coloquial— permitía numerosas acepciones en función del contexto donde era proferido. Bajo esta contextualización, no puede considerarse que la expresión «h...de p... » fuera susceptible de añadir un descredito adicional en relación con la información ya publicada, por lo que no puede estimarse que el citado término fuera gravemente ofensivo o insultante.

Además de este aspecto, el voto particular plantea un asunto interesante en el que la opinión mayoritaria no entró: la consideración de si la persona jurídica privada recurrente, titular de la página Web es titular de un derecho fundamental a la libertad de expresión, o en su caso de información, o si solamente es portadora de un interés legítimo. A este respecto, el voto particular entra en una interesante reflexión exponiendo dos líneas argumentales muy debatidas actualmente: «a) si las plataformas de Internet son canales de comunicación entre personas de todo el mundo y por tanto, deben ser asimiladas, en general, a los medios de comunicación basándose, sobre todo, en la función que ejercen y en la vertiente objetiva de las libertades comunicativas, al ser instrumentos de fomento, al menos en principio, del pluralismo sobre el que se basa nuestro sistema social y democrático (art. 1.1 CE), de tal modo que, además de ser titulares de la libertad de empresa, serían titulares de las libertades de expresión y de comunicar información, incluida, en este último caso, el derecho a la creación de medios de comunicación [art. 20.1 d) CE] y se les aplicaría, por tanto, el mismo régimen jurídico-constitucional que a los medios de comunicación audiovisuales, radiofónicos e impresos, también en lo relativo al ejercicio de las libertades de expresión e información, alcance y límites; b) si las plataformas comunicativas pueden configurarse como personas jurídico-privadas de interés general, dado que prestan servicios públicos o esenciales, lo que vendría a condicionar su régimen jurídico. Así, el papel privilegiado que juegan en la comunicación o, dicho de otra forma, el haberse convertido en un foro o instrumento percibido como público por sus usuarios y el haber adoptado políticas de moderación que acaban delimitando, cuando no limitando, el alcance del ejercicio de las libertades comunicativas justifica que sean tratadas jurídicamen-

te no como meras empresas privadas, sino como personas jurídicas con trascendencia jurídico-constitucional, de forma similar a las personas jurídico públicas».

En el caso concreto de la empresa propietaria de la Web, la magistrada cree que quizá no se pueda decir aún que es un medio de comunicación, pues es una plataforma de agregación de contenidos, pero sí que participa en el proceso de comunicación actual, difundiendo noticias y permitiendo que los sujetos de su comunidad las comenten, y por ello le parece razonable reconocerle la titularidad de la libertad de expresión y de información.

## **7. CONCLUSIONES**

Los derechos «clásicos» han de ser adaptados ahora al marco digital, y así seguiremos hablando, por ejemplo, de derecho al honor, del derecho a la educación o de la libertad de expresión o de información, pero ahora no solamente en su marco clásico, el que hemos conocido hasta ahora («analógico», por utilizar una imagen más gráfica), sino también en un nuevo marco, en un nuevo contexto: el «digital». Y además de los derechos de siempre, tanto en el ámbito analógico como digital, van surgiendo derechos nuevos, directamente vinculados con el ámbito digital, como, por ejemplo, uno de los más famosos de entre ellos, el denominado *derecho al olvido*. Y los retos son crecientes, por ejemplo en relación con la Inteligencia Artificial y con los denominados «neuroderechos». Pero unos y otros, en un ámbito y en otro, no solo deben ser reconocidos sino también eficazmente protegidos en lo que algunos autores han denominado un nuevo «paradigma constitucional» y, por ende, la teoría constitucional debe ofrecer nuevos instrumentos para hacer frente a la transformación digital y a las nuevas tecnologías, para que, en definitiva, podamos seguir hablando de un verdadero Estado de Derecho y por eso también, hemos empezado a hablar de «constitucionalismo digital» y a preguntarnos cuál es el «alma constitucional» de la tecnología digital.

Este reto implica a instituciones públicas y privadas. Al mismo tiempo que se refuerza la intervención de las autoridades administrativas especializadas (Agencias de Protección de Datos, etc.) y de los órganos judiciales, no hay que olvidar que los actores privados están desarrollando funciones de control de contenidos en el mundo digital que, hasta ahora, correspondían únicamente a autoridades públicas, administrativas o judiciales y hay que garantizar también que ese control sea transparente y controlable a su vez en un Estado de Derecho.

Estos retos no son locales, sino globales y, por tanto, las medidas deberían ser globales. A pesar de las dificultades, en el ámbito del Consejo de Europa y de la Unión Europea se están dando importantes pasos en su regulación y además, de un modo bastante rápido y eficaz. Sin embargo, arbitrar soluciones jurídicas mundiales no es fácil, porque las perspectivas de las distintas culturas jurídicas y los intereses de los distintos países, empresas, etc., no siempre son coincidentes. Incluso dentro de la cultura jurídica occidental, las visiones no

siempre coinciden. Veamos un ejemplo muy ilustrativo: los Tribunales norteamericanos (y en particular, el Tribunal Supremo) están más preocupados en dar toda la amplitud posible a la Primera Enmienda de la Constitución norteamericana, entendiendo que la libertad de expresión debe extenderse al dominio digital, al que considera un nuevo canal para promover el libre intercambio de ideas, mientras que los Tribunales europeos están insistiendo cada vez más en un *superderecho* a la privacidad y a la protección de datos que predomina en determinados casos sobre la libertad de expresión. Y en este sentido, hay que tener cuidado con una cierta tentación eurocéntrica que tenemos en Europa, como si el mundo entero se moviese al compás jurídico europeo, y no olvidar nunca que estos asuntos tienen dimensión mundial y que los europeos solamente somos una parte y no la más importante ni poderosa en este *juego*. De ahí que algunos autores hayan hablado a este respecto de un «proceso de europeización» de Internet, que podría eventualmente conducir a una cierta fragmentación o «balcanización» de los instrumentos de protección frente a los retos globales que plantea Internet, lo que sería contraproducente.

Como en todo proceso, hay luces y sombras, y hablando de «luces» es de justicia destacar en el ámbito europeo la actividad militante de los Tribunales, que en algunos casos han ido por delante de los legisladores a la hora de resolver posibles conflictos en la protección de derechos frente a las nuevas tecnologías, hasta el extremo de que alguno de estos nuevos derechos como, por ejemplo, el *derecho al olvido* es de creación jurisprudencial y solo después de su creación jurisdiccional, se han regulado en extenso para regularlo y protegerlo. Además, se han ido aprobando toda una batería de normas de *soft law* que han tenido una gran influencia, pero dado que no tienen carácter vinculante, es necesario dar más pasos para convertir muchos de sus contenidos en auténtica normativa con carácter vinculante: en ello estamos ya con los nuevos instrumentos europeos de *hard law*, como el nuevo Reglamento Europeo (UE) 2024/1689, del Parlamento Europeo y del Consejo, de Inteligencia Artificial de 13 de junio de 2024 y con el Convenio Marco del Consejo de Europa nº 255 sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho, de 17 de mayo de 2024.

Por lo que respecta al caso español, la introducción de los nuevos derechos digitales en el ordenamiento jurídico se ha topado con algunas dificultades que han intentado ser superadas a través de mecanismos que no compaginan del todo bien con las categorías generales del sistema de fuentes del ordenamiento. En este momento, la única referencia constitucional a estos temas se encuentra en el artículo 18.4 de la Constitución de 1978. Este texto que, sin duda, fue un avance en el momento en que se aprobó la Constitución, resulta claramente insuficiente hoy, aunque introduce una cláusula bastante abierta que, como veremos, ha utilizado posteriormente el legislador, para ir más allá de la simple protección de datos. Probablemente, en pura técnica jurídica, la mejor solución sería reformar la Constitución española para incluir los nuevos derechos digitales, pero, como es bien conocido, la extraordinaria rigidez del procedimiento establecido en el artículo 168 de la Constitución para introducir cualquier modificación de la Constitución en el ámbito de los derechos fundamentales recogi-

dos en la sección primera del capítulo II de su Título I hace prácticamente inviable una modificación constitucional en este momento. Por ello, el legislador español ha utilizado una *vía discutible* para introducir esos derechos digitales en nuestro ordenamiento jurídico, pensando en que es mejor hacer algo que no hacer nada: el cauce de una Ley Orgánica, la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales, «adaptando», por decirlo de alguna manera, el 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 sus datos personales y a la libre circulación de estos datos.

Y digo *vía discutible* porque, en primer lugar, podríamos preguntarnos por qué hay que dictar una normativa de derecho interno para garantizar la aplicación de un Reglamento europeo que, por sí mismo, tiene eficacia directa en todos los países de la Unión Europea. Y, en segundo lugar, también resulta dudosa la técnica de incluir en el título X de la Ley Orgánica un elenco de derechos digitales. Esos derechos, deberían estar en la propia Constitución y no en una Ley Orgánica, por mucho que se quieran hacer «colgar» de la cláusula abierta del artículo 18.4 de la Constitución. La realidad es que se están creando derechos fundamentales nuevos no mediante una reforma constitucional, sino a través de una Ley Orgánica cuya cobertura jurídica en el artículo 18.4 de la Constitución es bastante discutible, y a través de otras leyes sectoriales específicas, en lo que parece un caso de «mutación constitucional», ya que, como hemos visto, en la práctica, no es posible en estos momentos reformar la Constitución siguiendo el procedimiento de reforma previsto en ella.

En todo caso, lo que nos debe preocupar ahora en este nuevo entorno digital es lo que nos ha preocupado siempre a los juristas que creemos en el Estado de Derecho y en la democracia: ¿cómo proteger eficazmente la libertad y los derechos fundamentales frente a las amenazas para ellos que han surgido en distintos momentos y coyunturas históricas? La lucha por el Estado de Derecho, sea liberal, social, social y democrático e incluso «ciberEstado de Derecho» no cesa a lo largo de los tiempos y es uno de los objetivos irrenunciables de un sistema constitucional y democrático, analógico o digital.

## **8. BIBLIOGRAFÍA**

- AGUILAR CALAHORRO, A. (2022): «Valores constitucionales y Sociedad digital». En: Revista da AJURIS. Porto Alegre: vol. 49, n° 152.
- ARCE JIMÉMEZ, C. (2022): «Desafíos para la ciudadanía y el sistema de derechos fundamentales en la era digital». En: *Derechos y Libertades*, n° 46. Época II.
- ANÓN ROIG, M<sup>a</sup> J. (2022): «Desigualdades algorítmicas: conductas de alto riesgo para los derechos humanos». En: *Derechos y Libertades*, n° 47, Época II.
- ARENAS RAMIRO, M. / ORTEGA GIMENO, A. (2019): *Protección de datos: Comentarios a la Ley Orgánica de protección de datos y garantía de derechos digitales (en relación con el RGPD)*. Las Rozas: Sepin.

- ARENAS RAMIRO, M. (2022): La igualdad a la luz de los derechos digitales. En: RECHE TELLO, N. / TUR AUSINA, R. (2022): *La teoría constitucional frente a la transformación digital y las nuevas tecnologías*. Cizur Menor: Aranzadi.
- BALAGUER CALLEJÓN, F. (2021 a): «La constitución del algoritmo. El difícil encaje de la constitución analógica en el mundo digital». En: GOMES, A.C. N./ ALBERGARIA, B. / CANOTILHO, M.R. *Direito Constitucional: diálogos em homenagem ao 80º aniversário de J.J. Gomes Canotilho*. Belo Horizonte: Forum.
- BALAGUER CALLEJÓN, F. (2021 b): «Inteligencia artificial, democracia y derechos». En: FILHO, W.S.G./ SANTAELLA, L. et al. *Direito e Inteligência Artificial: Fundamentos*. Río de Janeiro: Lumen Juris.
- BALAGUER CALLEJÓN, F. (2022). *La Constitución del algoritmo*. Zaragoza: Fundación Manuel Giménez Abad.
- BALAGUER CALLEJÓN, F. / COTINO HUESO, L. (coords.). (2023): *Derecho Público de la Inteligencia Artificial*. Zaragoza: Fundación Manuel Giménez Abad.
- BALAGUER CALLEJÓN, F. / SARLET, I. W. (2023): *Derechos fundamentales y democracia en el constitucionalismo digital*. Pamplona. Aranzadi.
- BARRIO ANDRÉS, M. (2021): «Génesis y desarrollo de los derechos digitales». En: *Revista de las Cortes Generales*, nº 110.
- BARRIO ANDRÉS, M. (2022): *Manual de Derecho Digital*. 2ª ed., Valencia: Tirant lo Blanch.
- BERROCAL LANZAROT, A I. (2020): *Comentarios a la nueva ley de protección de datos: Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*. Madrid: Dilex.
- COTINO HUESO, L. (ed.) (2022): *La Carta de Derechos Digitales*. Valencia: Tirant lo Blanch.
- COTINO HUESO, L. (2023 a): «Los requisitos del Tribunal Constitucional alemán para el análisis automatizado de datos o con inteligencia artificial, que no se cumplen en España». En *Revista catalana de dret públic. Blog*. <https://eapc-rcdp.blog.gencat.cat/2023/04/12/los-requisitos-del-tribunal-constitucional-aleman-para-el-analisis-automatizado-de-datos-o-con-inteligencia-artificial-que-no-se-cumplen-en-espana-lorenzo-cotino-hueso/> (última consulta, 15 de abril de 2023).
- COTINO HUESO, L. (2023 b): «Menos libertad de expresión en internet: el peligroso endurecimiento del TEDH sobre la responsabilidad de moderación de contenidos y discurso del odio». En *Revista de Derecho Digital e Innovación. Aranzadi. La Ley*, nº 16.
- DE GREGORIO, G. (2022): *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*. Cambridge: Cambridge University Press. [https://www.cambridge.org/core/services/aop-cambridge-core/content/view/A3F61C6368D17D953457234B8A59C502/9781316512777AR.pdf/Digital\\_Constitutionalism\\_in\\_Europe.pdf?event-type=FTLA](https://www.cambridge.org/core/services/aop-cambridge-core/content/view/A3F61C6368D17D953457234B8A59C502/9781316512777AR.pdf/Digital_Constitutionalism_in_Europe.pdf?event-type=FTLA) (última consulta, 24 de abril de 2023).
- FROSINI, T.E. (2022): «Transformación digital y constitucionalismo». En: RECHE TELLO, N. / TUR AUSINA, R. (2022). *La teoría constitucional frente a la transformación digital y las nuevas tecnologías*. Cizur Menor: Aranzadi.

- GARCÍA MAHAMUT, R. / TOMÁS MALLÉN, B. (2019): *El Reglamento General de Protección de Datos: un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y de garantía de los derechos digitales*. Valencia: Tirant lo Blanch.
- HERRÁN ORTIZ, A.I. (2023): «A vueltas con los neuroderechos. ¿Es tiempo de configurar nuevos derechos constitucionales en España?». En *Revista General de Derecho Constitucional*, nº 38.
- HOFFMANN-RIEM, W. (2022): *El derecho ante el reto de la transformación digital*. Cizur Menor: Aranzadi.
- LUCAS VERDÚ, P. (1975): *La lucha por el Estado de Derecho*. Bolonia: Real Colegio de España.
- LLANO ALONSO, F. H. / GARRIDO MARTÍN, J. (2021): *Inteligencia artificial y Derecho. El jurista ante los retos de la era digital*. Cizur Menor: Aranzadi.
- MADRID PARRA, A. (dir). (2022): *Derecho digital y nuevas tecnologías*. Cizur Menor: Aranzadi.
- MEDINA GUERRERO, M. (coord.) (2023). *Los derechos de la ciudadanía ante la Administración Digital*. Madrid: Centro de Estudios Políticos y Constitucionales.
- MOLINA MARTÍNEZ, L. (2022). «Honor y libertad de expresión en las redes sociales». En *Derecho Privado y Constitución*, nº 41.
- PEREA ORTEGA, R. (2020): *Estudios sobre Derecho digital*. Cizur Menor: Aranzadi.
- POLLICINO, O. (2021): *Judicial protection of fundamental rights on the internet: a road towards digital constitutionalism?* Oxford: Hart Publishing.
- PRESNO LINERA, M. A. (2023): *Derechos fundamentales e inteligencia artificial*. Madrid: Marcial Pons.
- QUADRA SALCEDO, T. DE LA / PIÑAR MAÑAS, J. L. (dirs.) (2018): *Sociedad Digital y Derecho*. Madrid: Boletín Oficial del Estado.
- QUERALT JIMÉNEZ, A. (2021): «Una Constitución analógica ante el fenómeno digital». En GONZÁLEZ GARCÍA, I. Y GARCÍA ROCHA, M<sup>a</sup> P. *Estado de Derecho y Reforma Constitucional*. Valencia: Tirant lo Blanch.
- RALLO LOMBARTE, A. (2017): «De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018)». En *Revista de Derecho Político*, nº 100.
- RALLO LOMBARTE, A. (2020): Una nueva generación de derechos digitales. En *Revista de Estudios Políticos*, nº 187.
- REBOLLO DELGADO, L. (2023): *Inteligencia artificial y derechos fundamentales*. Madrid: Dykinson.
- RECHE TELLO, N. / TUR AUSINA, R. (2022): *La teoría constitucional frente a la transformación digital y las nuevas tecnologías*. Cizur Menor: Aranzadi.
- RODRÍGUEZ AYUSO, J.F. (2022): *Nuevos retos en materia de derechos digitales en un contexto de pandemia*. Cizur Menor: Aranzadi.
- SÁNCHEZ BARRILAO, J.F. (2016): «El Derecho Constitucional ante la era de Ultrón: la informática y la inteligencia artificial como objeto constitucional». En *Estudios de Deusto*, vol. 64, nº 2.

- SÁNCHEZ NAVARRO, A. / FERNÁNDEZ RIVEIRA, R. (eds.) (2023): *Reflections for quality democracy in a technological era*. Cizur Menor: Aranzadi.
- SARRIÓN ESTEVE, J. (2023): *El reconocimiento y protección de los derechos y libertades en un mundo en transformación. ¿Hacia un nuevo paradigma constitucional?* Cizur Menor: Aranzadi.
- SIMÓN CASTELLANO, P. (2023): «Taxonomía de las garantías jurídicas en el empleo de los sistemas de inteligencia artificial». En *Revista de Estudios Políticos*, nº 117.
- TRONCOSO REIGADA, A. (dir.). (2021): *Comentario al Reglamento general de protección de datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales*. Cizur Menor, Civitas.
- VALLS PRIETO, J. (2018). *Retos jurídicos por la sociedad digital*. Cizur Menor: Thomson Reuters / Aranzadi.
- VV.AA. (2022). Número monográfico sobre «Derecho e Inteligencia Artificial». En: *El Cronista del Estado Social y democrático de Derecho*, nº 100.
- VALPUESTA GASTAMINZA, E. / HERNÁNDEZ PEÑA, J.C. (coord.): (2021). *Tratado de Derecho Digital*. Barcelona: La Ley.