

## RETOS Y AMENAZAS DE LA REVOLUCIÓN TECNOLÓGICA EN EL ÁMBITO DE LOS DERECHOS HUMANOS

### Challenges and threats of the technological revolution in the field of Human Rights

**María Belén Cardona Rubert**

Catedrática de Derecho del Trabajo y de la Seguridad Social  
Universidad de Valencia  
maria,b,cardona@uv.es

Recibido: 22/10/2022 – Aceptado: 22/10/2022

*Conferencia pronunciada por la madrina de la promoción anual de la Facultad de  
Derecho el día 22 de junio de 2022 en la festividad de  
San Raimundo de Peñafort*

### Resumen

Las tecnologías digitales abren nuevos escenarios para la vida en sociedad, para la economía y las relaciones interpersonales. Son muchos los retos y desafíos frente a los que nos sitúan la revolución tecnológica como sociedad. Las tecnologías abren nuevos horizontes al papel regulador del Derecho y a la labor de los profesionales del Derecho, llamados a encontrar el equilibrio entre la utilización de las tecnologías y el respeto a los derechos y libertades del individuo.

Estamos ante desafíos globales, un cambio de paradigma y de época. Nuevos retos para los que hay que hallar soluciones aterrizadas en la realidad concreta y desde la perspectiva garantista de los derechos. El gran reto es proteger y garantizar el derecho fundamental a la protección de datos en un contexto público-privado de aceleración de la innovación, transformación digital, de fomento de la economía de datos y de generalización de aplicación de la inteligencia artificial, desde una visión holística de la sociedad y la economía y con una perspectiva inclusiva, ética y garante de los derechos humanos.

#### ■ Palabras clave:

Sociedad digital; Derechos humanos; Protección de datos; Tecnologías digitales; Inteligencia artificial; Algoritmos; Transformación digital; Economía del dato; Ciberseguridad; Brecha digital; Discriminación; Género; Acoso sexual; Prejuicios sexistas; Contrato de trabajo; Teletrabajo

## Abstract

### ■ Keywords:

Digital society; Human rights; Data protection; Digital technologies; Artificial intelligence; Algorithms; Digital transformation; Data economy; Cybersecurity; Digital divide; Discrimination; Gender; Sexual harassment; Gender bias; Employment contract; Teleworking

Digital technologies open up new scenarios for life in society, for the economy and for interpersonal relationships. There are many challenges facing us as a society as a result of the technological revolution.

Technologies open up new horizons for the regulatory role of law and the work of legal professionals, who are called upon to strike a balance between the use of technologies and respect for the rights and freedoms of the individual.

We are facing global challenges, a change of paradigm and of era. New challenges for which solutions must be found that are grounded in concrete reality and from the perspective of guaranteeing rights. The great challenge is to protect and guarantee the fundamental right to data protection in a public-private context of accelerating innovation, digital transformation, the promotion of the data economy and the widespread application of artificial intelligence, from a holistic vision of society and the economy and with an inclusive, ethical and human rights-guaranteeing perspective.

Me gustaría iniciar mi intervención, agradeciendo a la Facultad de Derecho de la Universidad de León y a su decano, Salvador Tarodo Soria, la invitación para participar en este acto como madrina de las promociones del Máster Universitario en Abogacía, del Máster en Derecho de la Ciberseguridad y Entorno Digital y del Grado de Derecho. Me siento honrada por impartir la conferencia de clausura en esta ceremonia en un día tan feliz.

El acto de hoy está cargado de significado para todos los aquí presentes o representados. En primer lugar, para la propia Universidad de León que ha acompañado a los egresados durante su proceso formativo, en segundo lugar, para la sociedad de León, representada hoy en todos sus estamentos y para los padres, familiares y amigos que nos acompañan y que sienten el orgullo y la satisfacción por la culminación de los egresados de una etapa de esfuerzo, de anhelos y desvelos que, sin duda, habrán sentido como propios y que hoy se ve jalonada con éxito.

Pero, sin duda, es para vosotros, los egresados para los que este momento es especial. El momento de mirar con cariño a la etapa que hoy culmina, de sentirse orgullosos de lo conseguido y de dirigir la mirada hacia delante y emprender la etapa siguiente con ilusión y paso firme. Es también el momento en el que os enfrentáis a las incertidumbres que todo cambio conlleva, a la elección de un camino profesional, que va a ser un elemento fundamental en vuestras vidas. Esta elección es un acto de madurez, que tiene un importante componente de decisión consciente, al tiempo que es un acto de fe y de expresión de autoconfianza importante que confirma que la decisión adoptada es la correcta.

Centrándome ya en el tema del que me corresponde hablar: “Retos y amenazas de la revolución tecnológica en el ámbito de los derechos humanos”.

En la actualidad, conceptos como las tecnologías de la información y la comunicación, el ciberespacio, la ciberdelincuencia, las redes sociales, el internet de las cosas, la sociedad digital o el metaverso, han tomado carta de naturaleza en nuestra vida cotidiana. Conceptos que nos resultan familiares, que utilizamos con naturalidad, sin extrañeza, de manera habitual.

La digitalización ha transformado de manera radical nuestra forma de comunicarnos y relacionarnos, nuestra forma de trabajar y de crear valor.

Las tecnologías digitales abren nuevos escenarios para la vida en sociedad, para la economía y las relaciones interpersonales. La vida ordinaria y profesional de las personas, la actividad productiva, los negocios, la educación, etc., se han visto enormemente facilitadas y agilizadas por la utilización de estas nuevas técnicas.

Lo digital se ha instalado definitivamente en las instituciones públicas y privadas y en la economía. Se ha generalizado un modelo de empresa basado en la digitalización, del que las plataformas digitales son el ejemplo paradigmático.

La emergencia sanitaria mundial ha naturalizado definitivamente lo digital en las relaciones económicas y sociales. El impacto de la pandemia ha acelerado la necesidad de transformación digital de empresas e instituciones. Un tránsito obligado por la necesidad de mantener el negocio, la economía. Al tiempo que ha puesto de manifiesto que las legislaciones, tanto en el plano de la Unión Europea como en el interno requieren un impulso y sobre todo una interpretación y una aplicación que no desconozca el potencial lesivo de las tecnologías disruptivas para la esfera de los derechos de las personas.

Por otro lado, la conocida como economía del dato traza un escenario de oportunidades de negocio y profesionales, basado en la analítica de todo tipo de dato en el contexto de la Estrategia Digital Europea.

La economía del dato tiene cada vez mayor relevancia en los ecosistemas europeos. Así mismo, los datos abiertos habilitan el desarrollo de nuevos productos, servicios y soluciones de alto valor socioeconómico. La Estrategia Europea de Datos busca convertir la UE en líder de una sociedad libre impulsada por los datos y aspira a impulsar la creación de un mercado digital único de datos, garantizando el desarrollo de la tecnología capaz de armonizarse con la garantía de los derechos fundamentales.

En dicha línea el Plan España Digital 2025 y las líneas estratégicas del Gobierno de España para ejecutar el Plan europeo de Recuperación, Transformación y Resiliencia, apuesta por la digitalización y generación de servicios públicos y negocios privados basados en datos, siguiendo el modelo europeo, es decir, con respeto al derecho a la protección de datos.

Sectores en expansión creciente, como el de la ciberseguridad necesitan urgentemente la incorporación de talento, de especialistas que blinden a los ciudadanos, a las empresas y a los estados de ciberataques y que garanticen la supervivencia ya no del propio sector sino de la propia economía, de las administraciones y de la soberanía nacional. La Estrategia de Seguridad Nacional española 2021, incardinada en la política exterior y de seguridad común de la Unión Europea, incluye entre sus prioridades el avance en la gestión de crisis, en el favorecimiento de la dimensión de las capacidades tecnológicas y de sectores estratégicos, así como de las capacidades de prevención, disuasión, detección y respuesta de España frente a estrategias híbridas. Tristemente el escenario bélico de Ucrania permite entender como hasta los perfiles de la guerra se han transformado por mor de la tecnología. Las guerras convencionales han dado paso a las guerras híbridas, en las que la desinformación, las noticias falsas y los ciberataques a infraestructuras críticas se combinan con las más tradicionales manifestaciones de la guerra como la invasión y los bombardeos.

Por otra parte, a nivel de cuotas de calidad democrática, la tecnología indudablemente ha contribuido a reforzar democráticamente a las sociedades.

Nunca tuvimos mayor acceso y más rápido a la información, ni de una manera socialmente más transversal. Nunca la tecnología nos acercó más. Nunca nos sentimos más libres, nunca fuimos más capaces de ejercer nuestra libertad de expresión, ni el derecho de información. Estos rasgos y otros se sitúan entre los aspectos positivos de las tecnologías de la información y la comunicación pero estas indudables ventajas tienen su reverso.

Se trata de tecnologías que, evidentemente, con innegables bondades pero también una nada despreciable potencialidad lesiva para la esfera de los derechos fundamentales, que hacen que su implantación genere numerosas dudas e incertidumbres. La dignidad, el derecho a la intimidad, la protección de datos, la libertad de expresión e información, la integridad física y moral, la libertad ideológica, la igualdad y no discriminación o los derechos a la libertad sindical y a la huelga, pueden verse comprometidos por aquellas.

Nuestros tiempos nos obligan a realizar una reflexión profunda y a plantearnos si esta sociedad digital, de la que todos nos consideramos parte, que está en constante evolución, ha tomado en consideración los valores y principios que inspiran las sociedades democráticas e igualitarias o si sólo los ha adoptado desde un punto de vista meramente formal y no material. En definitiva, nos obliga a cuestionarnos sobre cómo las tecnologías afectan a los derechos, puesto que su implantación nos enfrenta a importantes paradojas como sociedad y a retos que sólo desde el Derecho es posible resolver.

Uno de los retos y primeras paradojas de la digitalización de la sociedad y de la economía es que esta se produce de manera desigual y no afecta de manera equilibrada ni si quiera similar a todas las personas, es más, sirve para acentuar inequidades precedentes, surgiendo la que se conoce como brecha digital.

La brecha digital hace referencia, en definitiva, a la desigualdad entre las personas que pueden tener acceso o conocimiento en relación a las nuevas tecnologías y las que no. La brecha digital no es única si no que admite su clasificación en diversas modalidades. Así es posible hablar de brecha digital por género, por razón de edad, formativa (analfabetismo digital), de índole funcional (diversidad funcional física o psíquica), por renta o económica, de índole geográfica o territorial, urbano-rural, etc., guardando muchas de ellas estrecha relación con las otras, es el caso del género con la edad, de la funcional con el género, de la formativa con el género, etc. Se produce así la paradoja de que las tecnologías de la información y la comunicación lejos de desempeñar un papel vertebrador de la sociedad, en estos casos se constituye en un factor coadyuvante de la desigualdad.

Casos particularmente significativos son los vinculados a la brecha digital de índole geográfica o territorial y la brecha digital urbano-rural, que visualizan como el lugar de residencia de las personas puede ser determinante para la exclusión digital. Por ello, están llamadas a desempeñar un papel crucial las políticas públicas que faciliten de manera transversal la implantación de la digitalización en la sociedad y la economía superando la brecha digital en sus diversas manifestaciones.

Pero si hay que señalar una característica de las tecnologías de la información y de la comunicación que ha proyectado la transformación de la sociedad y de las relaciones de todo tipo hacia esferas hasta ahora desconocidas es, sin duda, su capacidad generadora de flujos de grandes cantidades de datos relativos a las personas y sus conductas que permiten la construcción de perfiles, susceptibles de ser valorados con las finalidades más diversas: estrategias de consumo, evaluación del desempeño del trabajo, finalidades políticas, de control fiscal, etc.

Estamos hablando de un imparable caudal de información de gran precisión y calidad y que con la incorporación de la técnica de los algoritmos permite, incluso, la previsión de comportamientos futuros y la adopción de decisiones por sistemas expertos basadas en dichas informaciones. Es decir, permite la adopción de decisiones automatizadas, la adopción de decisiones algorítmicas basadas en el manejo de *big data*.

El conocimiento ordenado de datos personales puede dibujar un determinado perfil de la persona o configurar una determinada reputación o fama que es, en definitiva, expresión del honor.

La información sensible crea vulnerabilidad en el sujeto titular de los datos pero también en toda la sociedad. La privacidad es una cuestión individual con implicaciones en lo colectivo, en toda la sociedad. La pérdida de privacidad está erosionando la igualdad.

Nos tratan con base en nuestros datos: según la tiranía del algoritmo, según lo que compramos, nuestro género, nuestra salud, nuestra orientación sexual, nuestra edad o todos estos factores combinados, las posibilidades son casi ilimitadas... todo ello contribuye a la polarización de la sociedad. Todo ello desde la paradoja de que se produce una entre comillas “renuncia libre” del titular de los datos a su privacidad.

Cada vez que realizamos una publicación en Instagram, cada vez que manifestamos nuestras opiniones en redes o simplemente cada vez que solicitamos o compramos un bien de consumo en plataformas digitales, como Amazon u otras, estamos renunciando a una parcela de nuestra privacidad. Parece ser que en nuestra sociedad existe una tendencia a la aceptación de que nuestra esfera privada se encoja cada vez más y eso es peligroso en términos democráticos.

El filósofo surcoreano BYUNG-CHUL HAN en su obra “No-Cosas” nos advierte de esos peligros cuando señala a las plataformas digitales, como Facebook o Google, como los nuevos señores feudales. “Incansables, labramos sus tierras y producimos datos valiosos de los que ellos luego sacan provecho. Nos sentimos libres, pero estamos completamente explotados, vigilados y controlados. En un sistema que explota la libertad no se crea ninguna resistencia (...). Somos demasiado dependientes de la droga digital y vivimos aturdidos por la fiebre de la comunicación, de modo que no hay ningún basta, ninguna voz de resistencia”. El sujeto sometido se imagina que es libre<sup>1</sup>.

Si analizamos de cerca cómo se producen las interacciones que proporciona la tecnología, es sencillo alcanzar la conclusión de que los algoritmos analizan nuestro comportamiento en la red y la forma de interactuar, lo que lleva a que se nos ofrezca información sobre aquello en lo que estamos interesadas y se nos aleje de la que nos genera rechazo. Lógicamente, esta segregación y selección en los mensajes que recibimos impide que se difunda el discurso discrepante, el discurso del otro. Por lo tanto, al final esa pretendida función de expansión del conocimiento y de la información tampoco resulta tan real. De hecho, el juego de los algoritmos contribuye a la segregación de la sociedad en grupos cada vez más segmentados y alejados unos de los otros y a la polarización de los discursos.

Otra de las evidencias que puede proyectar sombras sobre las conocidas como TICS y que, de nuevo, nos sitúa frente a paradojas es que su utilización puede no ser neutra desde el punto de vista del género. Un espacio como el virtual que, en teoría, propiciaría la construcción de relaciones horizontales y, por lo tanto, facilitaría un modelo de relaciones democráticas e igualitarias, ofrece la paradoja de que constituye un entorno en el que los idearios y estereotipos machistas se trasladan y difunden con suma facilidad. Las mismas redes que han permitido difundir y favorecer el movimiento Me Too o globalizar las reivindicaciones de mujeres, como las afganas o, recientemente, las protestas de las mujeres iraníes, contribuyendo a su viralización y adhesión solidaria; no están libres, sin embargo, de prejuicios sexistas y de manifestaciones de roles de género, pudiendo, en estos casos, la inteligencia artificial contribuir a su perpetuación.

Por otro lado, aparecen formas de violencia de género y de acoso sexual más sofisticadas, perversas y crueles puesto que su potencialidad lesiva se redimensiona y mediante la viralidad y la permanencia someten a tortura psicológica, emocional y social a sus destinatarias, conduciendo a la revictimización continua. No son estos rasgos exclusivos de la violencia o el acoso ejercido sobre las mujeres si no que se

---

<sup>1</sup> BYUNG-CHUL HAN, No-Cosas. Ed. Taurus, Barcelona, 2021, págs. 40-41.

reproducen con la misma virulencia en el ciberacoso ejercido sobre otros vectores de la población y en cualquier ámbito de las relaciones sociales, laborales, educativas, deportivas, culturales, etc.

Actualmente para hablar de enfermedad mental y/o emocional, hay que mencionar el entorno digital, la sobreexposición en este medio voluntaria o indeseada es habitual que acabe generando, en las personas sometidas a ella, efectos devastadores sobre su salud, constituyendo un problema social y de salud pública de primer orden.

En la misma línea una de las caras más oscuras de la inteligencia artificial es que puede contribuir a generar una honda expansiva de las causas de discriminación prohibidas, vulnerabilizando adicionalmente a las personas por sus características personales, físicas, psíquicas, de edad, raza, origen nacional, orientación o condición sexual. Por lo que en este contexto es importante reivindicar que los derechos fundamentales se erigen en instrumentos para la plena realización de la dignidad humana, cuyo fin último es el libre desarrollo de la personalidad y desde esa perspectiva constituye un umbral inquebrantable que no admite renunciadas ni claudicaciones en el entorno virtual.

En dicha línea, hay que situar, en el ámbito de la Unión Europea, la propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Dicha norma pretende afrontar además la opacidad, la complejidad, el sesgo, cierto grado de imprevisibilidad y un comportamiento parcialmente autónomo de ciertos sistemas de IA, para garantizar su compatibilidad con los derechos fundamentales y facilitar la aplicación de las normas jurídicas, sin que ello implique, en ningún caso, obstaculizar el desarrollo tecnológico y ni aumentar de manera desproporcionada el coste de introducir soluciones de inteligencia artificial en el mercado<sup>2</sup>.

Pero si hay un entorno en que estas tecnologías ha impactado, definitivamente, es en el de las relaciones de trabajo y el mundo empresarial, hasta el punto de hablarse de Cuarta Revolución Industrial, de la Industria y Sociedad 4.0, de una nueva era, para referirse a los cambios que la digitalización de la economía y la robotización están ocasionando.

Esta transformación se ha operado paulatinamente, pero de forma contundente y nos ha situado en un escenario de no retorno que obliga, ineludiblemente, al futuro Estatuto de los Trabajadores, propio de las relaciones laborales del siglo XXI, a

---

<sup>2</sup> <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206&from=ES>

Dicha propuesta culminaría un proceso precedido por el Libro Blanco de la Inteligencia Artificial, de 19 de febrero de 2020 ([https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020\\_es.pdf](https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf)) y la Guía de directrices éticas para una inteligencia artificial fiable (<https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>).

considerar la perspectiva digital y los derechos digitales como uno de los retos más importantes que regular.

Las tecnologías digitales abren nuevos escenarios para la organización del trabajo y la ejecución de la prestación laboral.

Estas tecnologías diluyen los tradicionales rasgos distintivos y configuradores del ámbito en el que se desarrolla la prestación de trabajo, el centro de trabajo y el tiempo de trabajo. Y lo hacen en favor de una hiperconectividad, permanente e independientemente del lugar en el que se halla el trabajador, puesto que la ejecución de la prestación de trabajo hace tiempo que dejó de estar constreñida a aquellos estrictos límites. El teletrabajo ha venido para quedarse.

El debate surgió con fuerza de la mano de la pandemia que trazó un escenario propiciatorio para comprobar lo que comporta la adopción global de modalidades de trabajo a distancia, para dar continuidad a la actividad económica, ya sea bajo la modalidad de teletrabajo doméstico o teletrabajo en alternancia. Más allá de las recomendaciones de las autoridades sanitarias indicando la conveniencia de promover estas modalidades de trabajo para retener la expansión de la pandemia, estas modalidades han venido para quedarse, también, en el escenario post COVID-19. El gigantesco laboratorio social proporcionado por la emergencia sanitaria mundial ha servido para evidenciar los claros y sombras de los ordenamientos jurídicos.

Su vertiente positiva, a parte de los beneficios medioambientales o de disminución de costes económicos de la empresa es, sin duda, la flexibilidad en la ejecución de la prestación laboral y el favorecimiento idealmente de la conciliación de la vida personal y familiar con la laboral, a través de la autodeterminación en la gestión del tiempo y autoorganización del trabajo. Pero, al mismo tiempo, es imposible desconocer los aspectos negativos o por así decirlo los riesgos asociados al trabajo vinculado a la utilización de estas tecnologías: invasión de espacios vinculados a la intimidad personal y familiar, la indefinición de los límites entre estos y los estrictamente laborales, el daño para la salud de los trabajadores, el perjuicio efectivo para la conciliación de la vida personal y laboral y la contribución a consagrar roles de género y particularmente las tareas de cuidado a las mujeres. Emergiendo en este ámbito la necesidad de reforzar el derecho a la desconexión digital como derecho de autodeterminación del trabajador que le permita preservar espacios privados y tiempos de descanso para el desarrollo de su personalidad y la tutela de la intimidad personal y familiar.

En otro orden de cosas, la introducción de los algoritmos en la gestión del personal ha revolucionado absolutamente los sistemas de trabajo y los modelos organizativos de la empresa. Su utilización permite extraer conclusiones que van más allá de la verificación de la correcta ejecución de la prestación laboral y ofrecer conclusiones sobre la personalidad del trabajador y obtener perfiles completos del trabajador. Perfiles susceptibles luego de ser valorados, favorable o desfavorablemente, a efectos laborales.



En los últimos años la forma de acceder y recopilar la información se ha abaratado drásticamente y eso ha facilitado que cada vez un mayor número de empresas tenga la capacidad de procesar esos datos y de adoptar decisiones usando la inteligencia artificial, reduciendo la intervención del ser humano hasta un escenario de. Decisiones sobre promociones profesionales, modificaciones de las condiciones de trabajo o despidos pueden adoptarse a través de algoritmos que no requieren la voluntad humana inmediata (*machine learning*).

La inteligencia artificial puede propiciar, por ejemplo, que la combinación de factores como las opiniones vertidas por los clientes, la medición de los tiempos de descanso o del tiempo de desempeño de los encargos, motive la adopción de decisiones empresariales sobre sus trabajadores. Pero, además, los algoritmos pueden albergar sesgos y producir discriminaciones de todo tipo, entre ellas sexistas. Puede suceder, por ejemplo, que se retribuyan más las tareas que requieran mayor esfuerzo físico o que se incluya algún criterio que favorezca a los trabajadores varones, o que la decisión automática produzca un perjuicio a las personas que disfruten de permisos de conciliación familiar, mayoritariamente disfrutados por mujeres.

La progresiva automatización en la toma de decisiones relativas al ejercicio de los poderes empresariales obliga a identificar los mecanismos de protección de los derechos de los trabajadores en este contexto. Dicha protección se construye a partir de la aproximación de reglas sobre las relaciones entre la gestión algorítmica de las decisiones empresariales y el derecho a la privacidad y el adecuado tratamiento de datos personales. No es un equilibrio fácil, pues las decisiones automáticas pueden proyectarse sobre datos que afectan a la vida íntima de las personas y que revelan informaciones tan privadas como sus relaciones personales, su religión o sus convicciones o su orientación sexual, entre otros muchos.

Las herramientas jurídicas de las que disponemos para compaginar estos dos aspectos son pocas. La protección más importante proviene de la normativa en protección de datos, el Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD). Y, en concreto, de la prohibición general sobre las decisiones basadas, únicamente, en un tratamiento automatizado de sus datos de carácter personal, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar y su derecho a oponerse a ella (art. 22 RGPD).

A esta altura de la exposición y sin ánimo de agotar todos los retos singulares que se plantean, se puede extraer ya una conclusión general y es que la aplicación de la informática y de tecnologías afines somete a duro examen la capacidad del ordenamiento jurídico para responder a los nuevos interrogantes que se plantean.

Y cual ha sido la respuesta del Derecho hasta el momento. Pues bien la regulación del derecho de protección de datos cuenta con una dilatada trayectoria. A nivel internacional el Convenio nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal,

de 28 de enero de 1981, se remite a los propios Estados firmantes para que desarrollen leyes y adopten medidas en cumplimiento de los principios enunciados en su texto.

A nivel de la Unión Europea, es la Directiva 95/46/CE, del Parlamento y del Consejo de la Unión Europea, de 24 de octubre de 1995, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la que introduce el concepto e impone a los Estados miembros su transposición a sus respectivos ordenamientos nacionales.

Con posterioridad otras normas comunitarias han ido incidiendo sobre la regulación del derecho de protección de datos a la par que los nuevos retos tecnológicos y sociales exigían su adaptación a las nuevas realidades. Las Directivas 97/66/CE, de 15 de diciembre de 1997 y 2002/58/CE, de 12 de julio son buena muestra de esto.

El respaldo definitivo a la consideración internacional del derecho a la protección de datos como un derecho independiente respecto al derecho al respeto a la vida privada se obtiene en la Carta de Derechos Fundamentales de la Unión Europea en la que se consagra el derecho fundamental de toda persona a la protección de datos de carácter personal que la conciernen (art. 8).

Por su parte, la mayoría de los Estados han llevado a cabo la constitucionalización del derecho a la autodeterminación informativa y, entre ellos, el nuestro, en el art. 18.4 de nuestra Carta Magna. Aunque existe acuerdo en considerar a este precepto como el fundamento constitucional del derecho, en puridad el artículo se limita a introducir un mandato para el legislador para que garantice los derechos fundamentales frente al uso de la informática. En el año 1992 se produce la primera respuesta legislativa al mandato constitucional a través de la Ley Orgánica 5/1992, de 29 de octubre, de regulación de tratamiento automatizado de los datos de carácter personal (LORTAD) que será sustituida por exigencias de adaptación a la Directiva 95/46/CE, por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (LOPD).

El punto de inflexión a nivel europeo llega de la mano del Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD), que deroga la Directiva 95/46/CE. El RGPD es directamente aplicable en todos los Estados miembro y obligatorio en todos sus elementos, sin necesidad de norma de transposición. Eso sí, a los Estados nacionales se les exige proceder a la depuración de sus ordenamientos, derogaciones de normas incompatibles, cuando proceda; al tiempo que se les incita a completar su regulación y adaptarla a las tradiciones jurídicas propias y al contexto nacional. En el caso español, estas exigencias conducen a la promulgación de una nueva norma de protección de datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD), que junto al RGPD, constituyen el nuevo marco normativo de la protección de datos.

Precisamente, este año se cumplen 30 años de la primera norma que en el ámbito nacional, dio cumplimiento al mandato constitucional del art. 18.4 CE e introdujo la regulación legal en materia de protección de datos. Tres décadas desde que la LORTAD se promulgó y los que entonces vaticinaban escenarios que en aquel

momento parecían propios del ámbito de la ciencia ficción, hoy se ven sobrepasados por una realidad tecnológica-digital que ha superado con creces cualquier previsión y que ni mucho menos ha escrito su última página.

Y en este entorno digital, absolutamente cambiante a medida que se transforma la tecnología, la pregunta que necesariamente debe plantearse es si sigue teniendo vigencia el derecho a la protección de datos y la arquitectura legal que le da soporte y contenido o es necesaria una normativa nueva.

Existe una tendencia, en algunos ámbitos a entender que cada evolución tecnológica requiere una nueva regulación. En mi opinión, resulta excesivo pretender que el Derecho se regule a golpe de innovación, en un escenario caracterizado por la transformación continua, además de que dicha pretensión estaría abocada sin remedio a un estrepitoso fracaso. No todas las innovaciones requieren normativa ad hoc, ni la normativa de protección de datos ha perdido vigencia, ya que la misma tiene vocación de permanencia y ofrece un sistema de principios rectores y reglas suficientes. Ahora bien, ello no excluye que sea aconsejable e, incluso, imprescindible proceder a la interpretación y adaptación del ordenamiento jurídico a la realidad cambiante, cuando los cambios y transformaciones de la tecnología sean suficientemente relevantes y, sobre todo, tengan potencialidad de incidir sobre la esfera de los derechos fundamentales de la persona.

En definitiva son muchos los retos y desafíos frente a los que nos sitúan la revolución tecnológica como sociedad.

Las tecnologías disruptivas abren nuevos horizontes al papel regulador del Derecho y a la labor de los profesionales del Derecho, llamados a encontrar el equilibrio entre la utilización de las tecnologías y el respeto a los derechos y libertades del individuo.

Estamos ante desafíos globales, un cambio de paradigma y de época. Nuevos retos para los que hay que hallar soluciones aterrizadas en la realidad concreta y desde la perspectiva garantista de los derechos. El gran reto es proteger y garantizar el derecho fundamental a la protección de datos en un contexto público-privado de aceleración de la innovación, transformación digital, de fomento de la economía de datos y de generalización de aplicación de la inteligencia artificial, desde una visión holística de la sociedad y la economía y con una perspectiva inclusiva, ética y garante de los derechos humanos.