



Universidad de Oviedo
FACULTAD DE DERECHO

GRADO EN DERECHO

TRABAJO FIN DE GRADO

CIUDADANÍA DIGITAL Y LA NUEVA DIMENSIÓN
DE LOS DERECHOS FUNDAMENTALES

Estudiante: Belinda Pascual López

Convocatoria: junio-julio 2024

DECLARACIÓN DE ACUERDO CON EL ARTÍCULO 8.3 DEL REGLAMENTO SOBRE LA ASIGNATURA TRABAJO FIN DE GRADO

Yo, Belinda Pascual López,

DECLARO

que el TFG titulado “Ciudadanía digital y la nueva dimensión de los derechos fundamentales” es una obra original, de mi propia autoría y que he referenciado debidamente todas las fuentes utilizadas, no habiendo recurrido al plagio, a la realización del trabajo por persona distinta del propio estudiante ni a ningún otro medio fraudulento de elaboración, incluidos los basados en sistemas de inteligencia artificial.

A 1 de julio de 2024.

RESUMEN

La era digital ha impactado en nuestras vidas de forma decisiva y con miras a su permanencia y evolución. Ha modificado el concepto de ciudadanía que hasta entonces conocíamos enfocado desde la perspectiva tradicional de la persona física, desplazándose ahora hacia una "ciudadanía digital". También nos ha llevado necesariamente a reinterpretar los derechos fundamentales bajo su nuevo prisma para poder hacer frente a nuevos retos, lo que, a su vez, implica constantes reformas en la regulación. En este trabajo se analizará, uno por uno, esa incidencia tecnológica y sus consecuencias. Siendo la consecuencia principal el surgimiento de nuevos derechos especialmente vinculados, arraigados al escenario digital, que encuentran ya cierto grado de regulación. Pero, asimismo, el surgimiento de posibles derechos emergentes, derivados de este ámbito pero independientes del resto, que puedan y deban ser calificados como fundamentales para asegurar una adaptación igualitaria de las sociedades a este nuevo contexto, garantizando siempre el pleno respeto de nuestros derechos humanos.

ABSTRACT

The digital era has had a profound impact on our lives and is here to stay and evolve. It has transformed the concept of citizenship as we knew it, which was focused on the traditional perspective of the physical person, and has shifted towards a "digital citizenship". It has also led us to necessarily reinterpret fundamental rights through a new lens in order to face new challenges, which in turn implies constant reforms in regulation. This paper will analyze, one by one, this technological impact and its consequences. The main consequence is the emergence of new rights, especially linked to and rooted in the digital sphere, which already have a certain degree of regulation. However, the emergence of possible new emerging rights, derived from this sphere but independent of the rest, which can and should be classified as fundamental to ensure an equal adaptation of societies to this new context, always guaranteeing full respect for our human rights.

ABREVIATURAS Y ACRÓNIMOS

AEPD.....	Agencia Española de Protección de Datos
Art.....	Artículo
CDFUE.....	Carta de los Derechos Fundamentales de la Unión Europea
CE.....	Constitución Española de 1978
CEPDHLF.....	Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales
DUDH.....	Declaración Universal de Derechos Humanos
FJ.....	Fundamento Jurídico
IA.....	Inteligencia Artificial
INE.....	Instituto Nacional de Estadística
LO.....	Ley Orgánica
LOPDGDD.....	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales
OCU.....	Organización de Consumidores y Usuarios
RGPD.....	Reglamento general de protección de datos
STC.....	Sentencia del Tribunal Constitucional
STS.....	Sentencia del Tribunal Supremo
TFUE.....	Tratado de Funcionamiento de la Unión Europea
UE.....	Unión Europea

ÍNDICE

INTRODUCCIÓN	2
1.- EL NUEVO CONCEPTO DE “CIUDADANÍA”	3
2.- REGULACIÓN ACTUAL DE LOS DERECHOS DIGITALES	5
2.1.- Marco europeo	5
2.2.- Marco nacional	6
3.- DERECHOS FUNDAMENTALES EN CONFLICTO	7
3.1.- Existentes	7
3.1.1.- Honor, intimidad y propia imagen.....	7
3.1.1.1.- Honor.....	7
3.1.1.2.- Intimidad	9
3.1.1.3.- Propia imagen.....	12
3.1.2.- Libertad de expresión e información	15
3.1.3.- Secreto de las comunicaciones	17
3.1.4.- Igualdad	18
3.2.- Emergentes	21
3.2.1.- Protección de datos personales y derecho al olvido.....	21
3.2.2.- Acceso a internet.....	25
3.2.3.- Desconexión digital.....	27
3.2.4.- Identidad digital.....	29
CONCLUSIONES	32
BIBLIOGRAFÍA Y DOCUMENTACIÓN	35
OTRAS FUENTES	39
NORMATIVA CITADA	40
JURISPRUDENCIA Y DOCTRINA JUDICIAL	42

INTRODUCCIÓN

El mundo real va quedando desplazado por uno digital.

La persona física se transforma cada vez más en un ente incorpóreo, un espectro que navega en internet, formado a partir de las páginas visitadas, búsquedas, cuentas, juegos, likes, interacciones... pasando a ser una “persona” digital.

Lo que crea múltiples interrogantes: ¿se crea una personalidad nueva?, ¿se amoldan los resultados a la persona, o la persona a los resultados hasta crearse un “perfil”?, ¿se podrá salir de ese “perfil” establecido cada vez más delimitado?, ¿se es consciente de los datos que se van almacenando?, ¿y qué pasa con esos datos, a quién le pertenecen?, etc.

Pero la principal cuestión aquí será: ¿protegen los derechos fundamentales el ámbito de esta nueva dimensión?

La respuesta estará en la adaptación al cambio, en la nueva normativa y jurisprudencia que los reinterprete. Pero la transformación es tan rápida que tampoco deja claro de qué manera hacerlo.

En esta investigación se examinará la nueva dimensión que conlleva para cada uno de los derechos fundamentales más afectados y que tan solo pensaban en una persona física o jurídica, pero no en “personas” difusas en la red. Comentando también otros de más reciente creación, más estrictamente vinculados al mundo digital, se entiendan ya como derechos fundamentales o que debieran serlo.

1.- EL NUEVO CONCEPTO DE “CIUDADANÍA”

La ciudadanía podría definirse como aquel concepto utilizado para englobar a personas pertenecientes a un mismo *pueblo* o *estado* (organizado), y en base a dicha inclusión se le reconocen unos determinados derechos y deberes derivados de su ordenamiento jurídico.

Este concepto se abre a otros debates relacionados con el término “pueblo”, ampliamente desarrollado en obras como la de Luigi Ferrajoli en su *Principia Iuris*, o “ciudadanía social”, originario de la obra *Ciudadanía y clase social* de Thomas H. Marshall, entre otras muchas concepciones que se ven interrelacionadas para dar una *exactamente* correcta definición; pero todo este debate es más propio de la filosofía política¹. Lo que aquí y ahora nos interesa es la evolución y nueva delimitación que se le ha conferido a la “ciudadanía” con el progresivo desarrollo de las tecnologías.

En relación con este tema puede mencionarse la obra “*Digital Citizenship: The Internet, Society, and Participation*” de Karen Mossberger en la que se define a los ciudadanos digitales como “aquellos que utilizan Internet de forma regular y efectiva”², lo que en la actualidad se extiende a casi el total de la población (según el INE, el 90% de la población entre 16 y 74 años utiliza Internet diariamente, y se encuentra en continuo crecimiento con el paso de los años³), o al menos esa es la idea, pues más adelante, en el análisis de los derechos en conflicto, se analizará la situación existente. Todos estos cambios tecnológicos originaron la aparición de la “brecha digital”, es decir, desigualdades en el acceso a internet y dispositivos electrónicos.

Se ha pasado de un “yo analógico” a un “yo digital”, y por ello será necesario adaptar el ordenamiento jurídico para proteger efectivamente estos nuevos espacios, puesto que “los instrumentos que jurisprudencial, normativa y doctrinalmente se han ido construyendo al servicio del ‘yo analógico’, tradicional titular de la ciudadanía, se revelan como inadecuados.”⁴

¹ DE LUCAS MARTÍN, J., “Ciudadanía: concepto y contexto. Algunas observaciones desde Principia Iuris de L. Ferrajoli”, *Anuario de filosofía del derecho*, núm. 29, 2013, pp.101-124.

² MOSSBERGER, K., TOLBERT, C.J., AND MCNEAL, R.S., *Digital Citizenship: The Internet, Society, and Participation*, MIT Press, 2007, p. 140.

³ Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares, del Instituto Nacional de Estadística, de 28 noviembre de 2023, p.2.

⁴ ARCE JIMÉNEZ, C., *¿Una nueva ciudadanía para la era digital?*, Dykinson, Madrid, 2022, p.15.

En resumen, el concepto de ciudadanía inicial como persona física ha quedado desfasado y desplazado por una predominante ciudadanía digital. Centrada ahora en la identidad personal creada a partir de nuestra actividad en la red.⁵ Lo que hace necesario un mayor control respecto a su gestión y desarrollo para que nuestra personalidad digital se cree de manera consciente, y sobre todo, de manera voluntaria.

Estaríamos hablando ahora, más que de una delimitación o división, de la creación de un nuevo concepto de ciudadanía, englobando necesariamente el mundo digital. Y a raíz de esto, van surgiendo nuevos problemas que deberemos abordar en el momento para continuar protegiendo los derechos fundamentales básicos de toda persona.

⁵ MORENTE PARRA, V., "Big data o el arte de analizar datos masivos: Una reflexión crítica desde los derechos fundamentales", *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 41, 2019, p. 247, pp. 225-260.

2.- REGULACIÓN ACTUAL DE LOS DERECHOS DIGITALES

2.1.- MARCO EUROPEO

Respecto a la legislación internacional, no encontramos en sus normas básicas referencias expresas al ámbito digital de los derechos humanos, ni en la Declaración Universal de Derechos Humanos, ni en el Convenio Europeo de Derechos Humanos, ni en la Carta de los Derechos Fundamentales de la Unión Europea, ni en el Tratado de Funcionamiento de la Unión Europea, entre otras; puesto que el mundo del internet se trata de un fenómeno de reciente y rápida expansión.

Igualmente, se podrá hacer uso de esta normativa como importante referencia básica a la protección de los principales derechos humanos, enunciados de manera genérica. Respecto al contexto digital, en particular, un derecho muy afectado que sí se recoge en estas normas sería la protección de datos, en el artículo 8 de la CDFUE o el 16 del TFUE, aunque no se haga mención expresa al contexto digital.

Ante ello, teniendo en cuenta su rápido desarrollo, ha tenido la Unión Europea que adaptarse a los cambios tecnológicos. Es voluntad de la UE el establecimiento de unos principios éticos que sirvan de base respecto a la transformación digital, garantizando el pleno respeto de derechos fundamentales como la protección de datos o la igualdad y no discriminación, derechos que en el próximo apartado se analizarán en detalle.

Dicha voluntad se manifiesta en la aprobación de la reciente Declaración Europea de 2023 sobre los Derechos y Principios Digitales para la Década Digital; sin embargo, como en su considerando número 10 establece, esta tiene únicamente carácter declarativo, sin afectar al contenido ni aplicación de las normas jurídicas. Dejando así un amplio margen de discrecionalidad para su seguimiento o no.

Ya con carácter normativo, existe alguna regulación anterior con mayor incidencia en la materia pero sobre ámbitos más concretos, como el Reglamento UE 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que incluye menciones a cuestiones tales como el derecho al olvido o el derecho a la información y al acceso de esos datos personales.

Y como regulación más reciente, también sobre una materia específica, se encontraría el Reglamento Europeo de 2024, aplicable al ámbito de los sistemas de aprendizaje autónomo, a los proveedores y usuarios que explotan sistemas de Inteligencia Artificial.

Este Reglamento será importante a lo largo del trabajo para puntualizar determinados derechos. Se aplica a materias del derecho de la UE como la protección de los datos personales, la intimidad o la confidencialidad de las comunicaciones respecto de datos personales tratados en relación con los derechos y obligaciones establecidos en este Reglamento; pero sin afectar a la aplicación de otras normas como el anterior Reglamento de 2016 mencionado (art. 2.7). Se encarga de regular el uso de los sistemas de IA y también de establecer límites y obligaciones, todo ello “para limitar los riesgos que de ellos se derivan”⁶. Es decir, se trata de una regulación basada en el riesgo que se pueda causar a la sociedad y sus derechos fundamentales, a más riesgo más restrictivas serán sus normas, que serán máximas en los sistemas IA de alto riesgo. Habrá que tener en cuenta además, las especialidades sobre la entrada en vigor de sus distintos capítulos, recogidas en el artículo 113.

2.2.- MARCO NACIONAL

En cuanto a la legislación española en materia digital, en gran parte por influencia del ámbito comunitario, destaca la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, a la cual haremos referencia frecuentemente en el desarrollo del trabajo. Concretamente su Título X, que recoge las garantías de los derechos digitales, perfilando los derechos fundamentales en el contexto digital. Esta ley supone un gran avance al reconocer ya ciertos derechos digitales.

Otra norma que resaltar, centrada ya en el ámbito laboral, es la Ley 10/2021, de 9 de julio, de trabajo a distancia, que recoge un derecho muy importante en esta materia como es la desconexión digital, también analizado próximamente.

Asimismo, es de mencionar la Carta de Derechos Digitales de 2021 que trata de adaptar los derechos ante los nuevos conflictos originados por el cambiante ecosistema digital; pero careciendo de fuerza normativa, con un carácter meramente descriptivo, prospectivo y asertivo. Se recuerda en sus consideraciones previas que esta Carta “no trata de crear nuevos derechos fundamentales sino de perfilar los más relevantes en el entorno y los espacios digitales o describir derechos instrumentales o auxiliares de los primeros”. Dejándola básicamente carente de funcionalidad.

⁶ *El Reglamento Europeo de IA, en resumen*, del Ministerio de Asuntos Económicos y Transformación Digital, p.1.

3.- DERECHOS FUNDAMENTALES EN CONFLICTO

3.1.- EXISTENTES

Se trata de derechos fundamentales ampliamente presentes en todas las situaciones que adquieren una nueva dimensión para adaptarse al espacio digital.

3.1.1.- HONOR, INTIMIDAD Y PROPIA IMAGEN

El uso de la informática afecta a estos derechos y ello puede verse ya reflejado en el apartado 4 del artículo 18 de la CE, según el cual, por ley deberá limitarse su uso para que estos puedan ser plenamente garantizados y ejercidos, disposición recogida cuando aún ni siquiera existía tal impacto tecnológico como el actual. Este artículo fue matizado en cuanto a su alcance por la sentencia del Tribunal Constitucional 254/1993, permitiendo interpretar estos derechos desde una perspectiva distinta a como históricamente se hacía, entendiendo como una nueva garantía la autodeterminación informativa⁷. Esta sentencia supuso un gran hito, principalmente por reconocer como derecho fundamental la protección de los datos personales, tanto el acceso a estos como su rectificación, cancelación o supresión. Además de establecer la obligación de las Administraciones Públicas a suministrar información que sobre los propios datos se solicite por los ciudadanos. Como refuerzo de sus conclusiones, el tribunal hace mención en su resolución de la LO 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal⁸, norma que quedará derogada por la LO 15/1999 de Protección de Datos de Carácter Personal (disposición derogatoria única), quedando ésta posteriormente derogada en su casi totalidad por la actual LO 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (disposición derogatoria única 1).

3.1.1.1.- Honor

Derecho fundamental reconocido en el art. 18.1 CE. Se trata de un concepto jurídico indeterminado vinculado a la dignidad de la persona, fama, propia estima, prestigio profesional y el merecimiento de la consideración ajena. Según la doctrina constitucional, “expresa de modo inmediato la dignidad constitucional inherente a toda persona”, lo cual

⁷ MURILLO DE LA CUEVA, P.L., “La construcción del derecho a la autodeterminación informativa”, *Revista de estudios políticos*, núm. 104, 1999, pp. 35-60.

⁸ STC 254/1993, de 20 de julio, FJ 9: “No es ocioso advertir que la reciente aprobación de la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal (L.O. 5/1992, de 29 octubre), no hace más que reforzar las conclusiones alcanzadas con anterioridad. La creación del Registro General de Protección de Datos, y el establecimiento de la Agencia de Protección de Datos, facilitarán y garantizarán el ejercicio de los derechos de información y acceso de los ciudadanos a los ficheros de titularidad pública, y además extienden su alcance a los ficheros de titularidad privada”.

variará en función de los valores e ideas sociales vigentes en cada momento, teniendo por tanto que ser concretado por el órgano judicial⁹. Su carácter es personalista, referido a la persona individualmente considerada, lo que no implica que su lesión se lleve a cabo únicamente mediante un ataque dirigido a una persona concreta, sino que puede tratarse también de ataques dirigidos a determinados colectivos de personas, trascendiendo a sus miembros, siempre que sus individuos sean identificables¹⁰.

Con las nuevas tecnologías este derecho está sufriendo un cambio hacia una interpretación de forma más amplia, siendo además más difícilmente delimitable los delitos de injurias y calumnias frente a la cada vez mayor cantidad de opiniones vertidas en la red sin ningún tipo de filtro e incluso bajo identidad oculta¹¹. En su protección ante intromisiones ilegítimas destaca la LO 1/1982, modificada posteriormente por la LO 3/1985. Pero sobre él incide innumerable cantidad de normativa, lo que complica su aplicación a la realidad social que regula, y por ello existe también numerosa jurisprudencia que trata de delimitar y clarificar los conceptos, supuestos y requisitos de estas normas¹².

Se tendrá que delimitar caso por caso el derecho a las libertades de información y opinión frente al derecho al honor, ponderando los derechos fundamentales en conflicto. En esa valoración, para ejercer el derecho de información, se hace referencia a su veracidad¹³, y en tal caso prevalecerá este frente al honor. Esto ha sido confirmado por sucesivas sentencias del TC, en las que se entiende la “veracidad” como un “deber de diligencia en la comprobación razonable de su veracidad”¹⁴.

Con el nuevo contexto digital, la LO 3/2018 introduce la colaboración por los responsables de las redes sociales y de servicios equivalentes para adoptar protocolos adecuados para el ejercicio del derecho de rectificación ante los usuarios de internet que atenten contra el derecho al honor (art. 85.2). Derecho que, según la STC 99/2011 de 20 de julio, ya en el marco legislativo anterior, entiende que constituye “un medio del que dispone la persona aludida para prevenir o evitar el perjuicio que una determinada información pueda irrogarle en su honor” (FJ 3), asociado indisolublemente a su dignidad, autoestima o reconocimiento

⁹ STC 46/2002, de 25 de febrero, FJ 6.

¹⁰ STC 214/1991, de 11 de noviembre, FJ 6 b).

¹¹ De la citada STC 46/2002, de 25 de febrero, FJ 6: “cuando de imputaciones de hechos se trata, cobra especial relieve el requisito de la veracidad: ninguna información que afecte al honor de una persona puede difundirse de modo constitucionalmente legítimo si es inveraz”.

¹² RÓDENAS CORTÉS, P., “Protección jurisdiccional al honor: polémica sobre prevalencia de derechos constitucionalmente protegidos; delimitación de competencias”, *Anuario de la Facultad de Derecho*, vol. XXIX, 2011, p.288.

¹³ STC 223/1992, de 14 de diciembre, FJ 2: “«mientras los hechos por su materialidad son susceptibles de prueba, los pensamientos, ideas, opiniones o juicios de valor no se prestan, por su naturaleza abstracta, a una demostración de su exactitud» (STC 107/1988). Tal diferencia conlleva que la libertad de expresión carezca del límite intrínseco que constitucionalmente se marca al derecho de información, consistente en la veracidad.”

¹⁴ STC 171/1990, de 12 de noviembre, FJ 8.

social (más destacado en el mundo digital). En la mencionada sentencia también se proclama que la rectificación del caso concreto, de una información que quién ejerció dicho derecho consideró inexacta y lesiva de sus intereses, no menoscaba el derecho fundamental del art. 20.1 d) CE a la libertad de información, incluso aunque la versión contenida en la rectificación pudiese considerarse incierta a posteriori puesto que esta no lleva aparejada la declaración de su veracidad (FJ 7).

Otro ejemplo más reciente, relacionado con la responsabilidad de una entidad prestadora de un servicio de intermediación de internet, es la STC 83/2023 de 4 de julio. Para la ponderación de los derechos al honor y libertad de expresión, se recuerda la doctrina para estos casos en la que se da especial relevancia a los caracteres del uso de internet y las redes, y el nivel de difusión que estos hacen alcanzar al mensaje. Resolviendo la prevalencia del derecho al honor frente a las expresiones excesivamente ofensivas e innecesarias para expresar el desacuerdo con la conducta a que la noticia hacía referencia. Y añade como refuerzo intensificador: la utilización del medio tecnológico (*“con especial potencialidad lesiva del honor individual, que no agota sus efectos en el contexto pasajero de una conversación oral, sino que permanece como contenido público fácilmente accesible”*) y el anonimato del autor (*“que intensifica el elemento de pura vejación, pues el destinatario del insulto queda particularmente indefenso”*) (FJ 6 c).

Cuestión especial son las intromisiones respecto a menores de edad¹⁵, cuestión que se desarrollará en el derecho a la propia imagen. Tendrá consideración de intromisión ilegítima “cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales”¹⁶. En esta nueva era digital habrá que prestarles gran atención puesto que se trata de sujetos de especial protección, debiendo atender siempre al superior interés del niño. Interés consagrado en el artículo 3 de la Convención sobre los Derechos del Niño, a tomar en cuenta por todas las instituciones, públicas o privadas, tribunales, autoridades administrativas y órganos legislativos.

3.1.1.2.- Intimidad

Este es definido como el “derecho a estar solo” o “a ser dejado en paz”¹⁷, estableciendo un

¹⁵ Protegido, entre otras normas que se irán mencionando, en el art. 4 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor; o art. 7 de la LO 3/2018.

¹⁶ Artículo 4.3 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

¹⁷ WARREN S.D. and BRANDEIS L.D., “The Right to Privacy”, *Harvard Law Review*, vol. IV, núm. 5, december 15, 1890, p.1.

espacio propio, íntimo, al que solo se puede tener acceso con autorización del titular. Esta protección frente a injerencias tanto de terceros como de los poderes públicos se reitera ya por el TC en sucesivas sentencias, como la importante 114/1984 FJ 7, o la más reciente 119/2022 FJ 4: *“implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana”*.

En cuanto a la intimidad, la mutación del derecho es clara, principalmente con las redes sociales, “es una realidad social el aumento de la difusión en todo tipo de redes sociales de fotografías tanto personales como de familiares o amigos que van pasando directamente de unos a otros a través de distintos procedimientos e incluso sin su consentimiento”¹⁸. Desconociendo, pero sin importarnos mucho, su destino final; simplemente dejándonos llevar por la tendencia, compartiendo todos los aspectos “privados” de nuestra vida. En cuanto a la IA, el nuevo Reglamento Europeo entiende que debe garantizarse, tanto el derecho a la intimidad como la protección de datos personales, “a lo largo de todo el ciclo de vida del sistema de IA” (considerando 69).

La intromisión digital en la vida privada ha llevado a modificar la función de este derecho fundamental, “pasando de ser un instrumento de exclusión, de impedimento de las intromisiones en el ámbito íntimo, a constituir un principio activo que faculte para decidir y controlar el destino de los propios aspectos personales y de la información que le afecte directamente”¹⁹. Es decir, ya no se trata tanto de proteger las intromisiones, sino partiendo de la base de que tales intromisiones van a suceder, buscar la manera de que cada persona sea la propietaria real de su vida y pueda decidir el uso que se le dé a su información personal (un ejemplo sería una verdadera decisión a aceptar o no las *cookies*). Esta visión activa del derecho ha sido respaldada por jurisprudencia del Tribunal Constitucional, como la sentencia 254/1993, de 20 de julio en su FJ 7: “la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada “libertad informática” es, así, también derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*)”; o alguna más reciente como la STC 292/2000, de 30 de noviembre (analizada posteriormente). Esta visión activa del TC podría llevarnos a pensar, indirectamente, en un derecho a la propia identidad digital.

¹⁸ SAP de Navarra 116/2020, de 26 febrero, FJ 4, JUR/202/299802.

¹⁹ MARTÍNEZ DE PISÓN CAVERO, J.M., “Vida privada sin intimidad. Una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo”, *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 37, 2017, p. 62.

En el ámbito laboral, la Ley Orgánica de Protección de Datos reformó el Estatuto de los Trabajadores con el artículo 20 bis, introduciendo una cuestión que la Carta de Derechos Digitales (XIX.2.b) también recoge, la protección a los trabajadores del derecho a la intimidad personal en el uso de dispositivos digitales, de videovigilancia, grabación de sonido o monitoreo. Tiene su razón de ser en los dispositivos de videovigilancia y geolocalización, para cuyo uso el empleador deberá respetar “en todo caso”²⁰ unos estándares mínimos de protección de la intimidad, y tener autorización para el acceso con fines privados a su contenido. Además de límites en la colocación, “en ningún caso”²¹ se admitirán en lugares de descanso de los trabajadores como vestuarios, aseos, comedores o similares; y límites en su consulta e información al trabajador, en su carácter como intervención mínima, en la proporcionalidad de la medida para la grabación de sonidos, ante riesgos para la seguridad de las instalaciones, bienes y personas en el centro de trabajo, etc.

Acerca de la grabación por videovigilancia, es destacable la sentencia del TEDH asunto *López Ribalda y Otros v. España*²² que admite el sistema de control por videovigilancia cuando el trabajador conoce de su instalación. El Tribunal parte de la reiteración de que el concepto “vida privada” del art. 8 del CEDH debe interpretarse de forma amplia. En este caso, existían cámaras de vigilancia encubiertas, de las que los trabajadores no fueron informados, por razón de sospechas de robo. Los tribunales nacionales consideraban la medida justificada al ser necesaria, proporcionada y perseguir un fin legítimo. Sin embargo, el TEDH determinó lo contrario, la legislación vigente de protección de datos exigía la previa información a los afectados de estos dispositivos, además, la sospecha previa no se dirigía específicamente contra alguna persona sino contra todo el personal indistintamente y sin ningún límite de tiempo, por consiguiente, no considera cumplida la proporcionalidad en las medidas adoptadas por el empresario, estimando vulneración del derecho a la vida privada. También en relación con las videocámaras, el nuevo Reglamento de IA aborda los sistemas de identificación biométrica, cuestión analizada en el apartado de protección de datos.

Respecto a esa exigencia del test de proporcionalidad en la grabación de las conversaciones destaca la STC 98/2000, caso *Casino de la Toja*, donde se plantea una intromisión en el derecho de intimidad personal, procediendo a analizar si existen “razones de necesidad estricta debidamente justificadas por el empresario”. Se concluyendo finalmente que la instalación de micrófonos para grabar conversaciones de trabajadores y

²⁰ Artículo 87.3 Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

²¹ Artículo 89.2 Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

²² STEDH, asunto López Ribalda y Otros v. España, de 9 enero de 2018, § 41-70.

clientes en determinadas zonas del casino no se ajustaba a las exigencias del respeto a la intimidad puesto que la empresa los instaló como simple complemento del sistema de seguridad que ya disponían, no siendo indispensable, y por ello, no conforme a los principios de proporcionalidad e intervención mínima.

Sobre el control empresarial por GPS, la STS 766/2020 de 15 septiembre terminó por rechazar cualquier lesión a derechos fundamentales en el despido de una trabajadora por usar el coche de empresa fuera de la jornada laboral y para fines ajenos, conocido esto a través del dispositivo GPS del vehículo, el cual era conocido previamente por la empleada, además que la carta de despido no contenía ninguna circunstancia personal sino únicamente dicho incumplimiento, justificando la decisión de la empresa en la constatación de señales de movimiento en tiempos no justificados.

3.1.1.3.- Propia imagen

El derecho a la propia imagen está ampliamente difuminado en el contexto actual, con las redes sociales parece que subir fotos a tu perfil permite que estas puedan ser comentadas y usadas por cualquiera. Es este el derecho que más problemática ocasiona y necesita de protección entre los tres analizados.

Su configuración se establece en diversa jurisprudencia del Tribunal Constitucional, definiéndolo la doctrina como: “un derecho de la personalidad, que atribuye a su titular la facultad de disponer de la representación de su aspecto físico que permita su identificación, lo que conlleva tanto el derecho a determinar la información gráfica generada por los rasgos físicos que le hagan reconocible que puede ser captada o tener difusión pública, como el derecho a impedir la obtención, reproducción o publicación de su propia imagen por un tercero no autorizado”²³.

No haciendo referencia este derecho fundamental únicamente a la estricta imagen física, sino también a otros atributos como la voz o el nombre, todo aquello propio y característico de la persona física. Se salvaguarda su ámbito de intimidad, perteneciendo a la propia persona el poder de decisión sobre los fines a los que aplicar su imagen. Constituye un “ámbito exento capaz de impedir o limitar la intervención de terceros contra la voluntad del titular”²⁴, salvo los casos de imágenes captadas en público, especialmente de personajes públicos por su confrontación con la libertad de información del art. 20.1.d) CE. Es decir, ante su choque con el derecho a la libertad de información, prevalece la relevancia del

²³ SSTC 81/2001, de 26 de marzo, FJ 2; 72/2007, de 16 de abril, FJ 3.

²⁴ STC 117/1994, de 25 abril, FJ 3.

debate público (y a más protección de la libertad de información, decrece la propia imagen).

Un aspecto conflictivo que resulta relevante en la nueva era es el caso de los menores, sujetos de especial protección. La Ley Orgánica 1/1982 no fija una edad límite para el consentimiento, haciendo referencia a “menores” (art. 3), lo que sí recoge en el art. 7 es una lista de situaciones con consideración de intromisiones ilegítimas que pueden comprender el uso de medios tecnológicos. El Reglamento de la LO 15/1999 de protección de datos sí fija la edad en 14 años (art. 13), igual que hace la LOPDGDD (art. 7). Los problemas surgen por diversos frentes, además del hecho de que se abran perfiles de redes sociales por debajo de la edad mínima requerida compartiendo información de forma irreflexiva, también cada vez más los padres suben vídeos y fotos de estos como principales exponentes de su vida familiar. Esta práctica, conocida como “sharenting”, requiere de gran regulación para su mejor protección puesto que se estaría creando una identidad digital prematura y sin consentimiento del menor²⁵. Además, si los progenitores en las plataformas obtienen ingresos económicos ¿no se trataría de una explotación de menores? Cuestión prohibida en el artículo 32 de la Convención sobre los Derechos del Niño, exigiendo a los Estados Parte la adopción de medidas legislativas, administrativas, sociales y educativas para garantizar su protección.

Este problema se limita de cierta manera en supuestos de patria potestad compartida, pues se requiere el consentimiento de ambos progenitores. Un ejemplo es la sentencia núm.116/2020, de 26 de febrero, de la Audiencia Provincial, en la que el tribunal entendió vulnerado el derecho a la propia imagen del hijo menor por la publicación de una fotografía por el padre ante la negativa de la madre, “aun cuando el hecho de que se trate de fotografías que en sí mismas no revisten ningún perjuicio para el menor” (FJ 4).

También existen supuestos de choque con otros derechos fundamentales, como la STC 158/2009 de 29 junio. En ella se cuestiona la publicación de una fotografía de un menor de edad en un periódico sin consentimiento ni justificación legal. El tribunal, tras ponderar los intereses enfrentados en la colisión de derechos, termina por considerar prevalente la propia imagen de un menor frente a la libertad de información, puesto que se carecía de consentimiento y no existe interés público en la captación o difusión de la fotografía que pueda estar por encima del superior interés por preservar la captación o difusión de las imágenes del menor (FJ 6).

²⁵ GARCÍA GARCÍA, A., “La protección digital del menor: el fenómeno del *sharenting* a examen”, *Revista de Derecho UNED*, núm. 27, 2021, p.463.

Parece que toda la normativa, tanto a nivel internacional y europeo como nacional, realiza una gran protección activa del menor, sin embargo, podemos ver que en el mundo digital se deja mucha libertad a la regulación interna por las propias plataformas en cuanto a los límites de edad, formas de uso de las plataformas o vías para resolver intromisiones, entre otras cuestiones.

Son especialmente numerosos los pleitos relativos a intromisiones ilegítimas en el nuevo contexto digital. Destaca la STC 27/2020 de 24 febrero en la que se plantea la ilicitud en el uso, por un reportaje periodístico, de la imagen de la víctima cogida de Facebook sin consentimiento del titular. El tribunal llega a varias reflexiones importantes²⁶. Por un lado, aclara que “los usuarios continúan siendo titulares de derechos fundamentales” (FJ 3), establece que las redes sociales no constituyen un lugar abierto al público, porque “el hecho de que circulen datos privados por las redes sociales en Internet no significa [...] que lo privado se haya tornado público, puesto que el entorno digital no es equiparable al concepto de «lugar público» del que habla la Ley Orgánica 1/1982” (FJ 3). Con ello resuelve un gran interrogante de esta “era digital”, pese a formar parte de internet, seguimos siendo los propietarios de nuestro perfil y teniendo los mismos derechos fundamentales a nuestro favor, interpretados ya desde este nuevo punto de vista. Otra cuestión está en que subir una foto a una red social no conlleva ninguna especie de consentimiento tácito que autorice a terceros libremente el uso de nuestras imágenes, ni aunque se tratase de un perfil público, sino que “tan sólo consiente en ser observado en el lugar que él ha elegido (perfil, muro, etc.)” (FJ 4). Ello tiene su razón puesto que el art. 2.2 de la LO 1/1982 exige un consentimiento “expreso” del titular para que no se considere como intromisión ilegítima. Y resuelve una cuestión respecto a la excepción del art. 8.2 c) LO 1/1982, al considerar que la imagen no tenía contenido informativo puesto que carecía de interés real para la transmisión de la información, ni era accesoria porque se trataba del partícipe principal del hecho noticiable (ante lo que solo podría estar con su consentimiento).

Fuertemente relacionado con estas ideas, aunque también con la intimidad o la protección de datos que más tarde se analizará, son los nuevos términos para la IA en Meta que modifican la política de privacidad de aplicaciones como Instagram, Facebook o WhatsApp de manera poco transparente e *inconsentida*. Si consigues enterarte, encontrarlos y leerlos, te indican que usarán todas las publicaciones personales, imágenes privadas/familiares o datos de seguimiento en línea de nuestros perfiles en redes para “entrenar” a esa IA

²⁶ AGÜERO ORTIZ, A., “Derecho a la propia imagen y divulgación en prensa de fotos obtenidas de Facebook”, *Derecho Privado y Constitución*, núm. 38, 2021, pp. 134-145.

generativa. Está formada por modelos informáticos, una forma de inteligencia artificial para la que parece que ya hemos “consentido”. NOYB presentó denuncias en 11 países europeos solicitando poner en marcha procedimientos de urgencia para detener ese cambio antes de su entrada en vigor. También la Organización de Consumidores y Usuarios lo denunció ante la Agencia Española de Protección de Datos en mayo de 2024, esperando una respuesta por la protección de los derechos de los usuarios a la mayor brevedad puesto que estas nuevas medidas estaban previstas para su entrada en vigor a partir del 26 de junio de 2024. Finalmente, días después de que la Comisión de Protección de Datos de Irlanda (DPC) solicitara la suspensión en nombre de varias autoridades de protección de datos europeas, parece que se consiguió, al menos por el momento, Meta no podrá usar información de usuarios europeos para “entrenar” su herramienta de Inteligencia Artificial²⁷.

3.1.2.- LIBERTAD DE EXPRESIÓN E INFORMACIÓN

Estas libertades del artículo 20 de la Constitución actúan como límite, con posición preferente en la mayoría de los casos, ante los derechos al honor, intimidad y propia imagen. Continúan estando vigentes en el nuevo mundo digital, se prevén en la normativa nacional, en el general art. 79 LO 3/2018, y el particular art. 85 para la libertad de expresión, además del capítulo XIV de la Carta de Derechos Digitales; y a nivel declarativo internacional, en el capítulo IV de la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01).

La libertad de expresión, de acuerdo con la doctrina jurisprudencial²⁸, constituye «uno de los pilares de una sociedad libre y democrática», y es por ello que goza de un amplio margen de protección, asegurando el libre intercambio de ideas y opiniones. Comprendiendo tanto aquellas opiniones más favorablemente acogidas como aquellas con menos apoyo, admitiendo incluso aquellas expresiones que puedan molestar, inquietar o disgustar a quien se dirigen. Se refuerza así la libertad de expresión en su dimensión colectiva, permitiendo manifestaciones que puedan incluso “tensionar los propios principios democráticos y los valores ético-morales mayoritarios de la sociedad”²⁹. Sin embargo, existe un límite, no se encuentran protegidas las expresiones que en el caso concreto tengan únicamente un

²⁷ Prensa: ORGANIZACIÓN DE CONSUMIDORES Y USUARIOS, *Inteligencia Artificial: OCU denuncia a Meta ante la Agencia de Protección de Datos*, de 31 de mayo de 2024; OCU, *Meta quiere tus datos para “entrenar” su IA... pero tendrá que cambiar de planes*, de 17 de junio de 2024; NOYB, *Noyb insta a 11 APD a detener inmediatamente el uso indebido de datos personales para la IA por parte de Meta*, de 6 de junio de 2024.

²⁸ SSTC 235/2007, de 7 noviembre, FJ 4; 159/1986, de 16 diciembre, FJ 6; o, STEDH, caso Castells c. España, de 23 abril 1992, § 42.

²⁹ ARCE JIMENEZ, C., *Una lucha contra el “odio digital” con pleno respeto a los derechos fundamentales*, Atelier, Barcelona, 2024, p.26.

carácter injurioso u ofensivo, sin guardar relación con las ideas u opiniones que se estén exponiendo. Incluso el Tribunal Europeo de Derechos Humanos ha afirmado que el respeto a la dignidad de todos los seres humanos también es fundamental en la sociedad democrática, y de ello resulta que se pueda considerar necesario sancionar e incluso prevenir en determinados casos las formas de expresión³⁰.

En el contexto digital el competente para establecer y aplicar estas restricciones parece cambiar, ya que la Carta transmite potestades a los prestadores de servicios intermediarios para establecer “restricciones en el uso de los servicios, incluyendo la existencia de políticas y herramientas de moderación de contenidos o de códigos de conducta y autorregulación, o de sistemas para comunicación y reclamación por dichos contenidos o de mecanismos y herramientas de alerta y detección”. Y ello con el simple requisito de informe previo a los usuarios y destinatarios finales. Es decir, se les daría a empresas privadas poder de decisión en materia de derechos fundamentales, funciones que el ámbito internacional no se les atribuye³¹. Algunas de estas prácticas son el filtrado y bloqueo de contenidos potencialmente ilícitos, en ocasiones muy cercanos a simples censuras³². Cuestión que en sentido inverso recoge esa Declaración Europea, comprometiéndose a adoptar medidas proporcionadas para combatir los contenidos ilegales “sin establecer ninguna obligación general de supervisión o censura”.

Respecto a la libertad de información, con menos alusión en la normativa nacional, los cambios principales que sufre están presentes en el espacio y el tiempo³³. El espacio está totalmente distorsionado con la posibilidad de un alcance global, incluso inintencionado, con la “viralización”; y el tiempo es detenido al quedarse la información en la red de forma permanente, pero a la vez rápidamente cambiante hasta que otra cuestión llame la atención de los usuarios y sea dejado de lado, teniendo también en cuenta el limitado alcance del derecho al olvido. Además, la calidad de la información pasa a un segundo plano, opacada por la inmediatez, se quieren conocer los sucesos en el momento en que acontecen, pudiendo esto interferir en la protección por la desinformación a la que la Declaración europea hace referencia. Aún más amenazada con el periodismo de calle realizado por los ciudadanos. Y todo ello poniendo en grave riesgo la protección constitucional a recibir “información veraz” del art. 20.1 d) CE.

³⁰ STEDH, caso Féret c. Bélgica, de 16 de julio de 2009, § 64.

³¹ “Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión” David Kaye, Consejo de Derechos Humanos, 32º período de sesiones, 11/05/2016, pp. 7-9.

³² ARCE JIMÉNEZ, C., “Desafíos para la ciudadanía y el sistema de derechos fundamentales en la era digital”, *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 46, 2022, p. 259.

³³ Reflexiones a partir de las ideas extraídas del citado artículo de D.Carlos Arce Jiménez.

3.1.3.- SECRETO DE LAS COMUNICACIONES

Reconocido en el art. 18.3 CE, se encuentra ampliamente relacionado con el derecho a la intimidad, libertad a comunicar y recibir información del art. 20.1 d) CE, y vinculado con la protección de datos personales. En la Declaración europea de 2023, se recogió en el punto 18 el derecho a la confidencialidad de las comunicaciones e informaciones contenidas en los dispositivos electrónicos, a proteger contra el acceso de terceros no autorizados.

La doctrina jurisprudencial del Tribunal Constitucional en esta materia es abundante³⁴, reconociendo la vertiente positiva de este derecho, implícitamente como la libertad de las comunicaciones, y explícitamente en su reserva; cubriendo bajo “secreto”, tanto al mensaje como la identidad de los interlocutores e incluso a los terceros ajenos.

En el nuevo contexto digital habría que cuestionarse si toda la información que vertemos en los chats de las aplicaciones o redes sociales están plenamente protegidos, o son simples conversaciones en manos de empresas privadas. En el ámbito laboral, la doctrina contenida en sentencias como la STS de 26 de septiembre de 2007 establecen límites en el registro de ordenadores empresariales para proteger una “expectativa razonable de intimidad” del trabajador. En aplicación de esta doctrina, la STC 170/2013 de 7 octubre resuelve un caso en el que entiende “no podía existir una expectativa fundada y razonable de confidencialidad” respecto al uso de la cuenta de correo proporcionada por la empresa puesto que había una expresa prohibición convencional de su uso extralaboral y la implícita facultad de la empresa para controlar su utilización, por lo que tal conducta quedaría fuera de la protección del art. 18.3 CE (FJ 4). En resumen, a lo que este concepto particularmente indeterminado hace referencia es al marco jurídico en que se produce, no en la tecnología concreta utilizada. Por ejemplo, no podría derivar de él un secreto de las comunicaciones en el contexto de un foro de internet abierto o una red social con cientos de seguidores o en un correo electrónico para cientos de personas; en cambio, sí existiría cierta expectativa razonable en un sistema de mensajería privada de una red social o una conversación mantenida con un único contacto³⁵.

Pero en lo que respecta al resto de casos, la regla general, y como ha afirmado la doctrina constitucional, es que la protección del 18.3 CE abarca “sea cual sea el ámbito objetivo del concepto de ‘comunicación’”, extendiéndose así a todas las formas de expresión, “no solo el

³⁴ Por ejemplo, SSTC 114/1984, de 29 de noviembre, FJ 7.7; 34/1996, de 11 de marzo, FJ 4.4; 99/2021, de 10 de mayo, FJ 3.3.

³⁵ COTINO HUESO, L., “Las obligaciones del Estado: el nuevo derecho fundamental de acceso a internet y las garantías a partir de la redefinición de las clásicas libertades informativas”, en VVAA, *La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC)*, 2015, p. 75.

mensaje plasmado en papel escrito, «sino también en otros soportes que los incorporan –cintas de cassette o de video, CD's o CVD's, etc»³⁶. Por lo tanto, deberían quedar amparados todos los nuevos modos de comunicación de la era digital, aunque igual necesitaría de mayor precisión normativa para garantizar un secreto de las comunicaciones por encima de los intereses particulares. Todo ello sin perjuicio de resolución judicial que autorice la injerencia justificadamente en ley.

Hay que mencionar también aquí al Reglamento Europeo de Inteligencia Artificial, que en su artículo 78 recoge la confidencialidad de la información y los datos obtenidos por la Comisión, las autoridades y organismos en el ejercicio de sus funciones. Se trataría de una protección de los datos frente a las intromisiones que estas autoridades puedan ejercer, debiendo estas solicitar únicamente aquellos datos que sean “estrictamente necesarios” para la evaluación del riesgo que presentan los sistemas de IA. Sin embargo, se deja margen al intercambio de información con autoridades de terceros países con las que se celebren acuerdos de confidencialidad bilaterales o multilaterales que garanticen un “nivel de confidencialidad adecuado”.

3.1.4.- IGUALDAD

Inicialmente recogida en el art. 14 CE, extendida a todos los ámbitos y desarrollada por normas como la Ley 15/2022 para la igualdad de trato y la no discriminación. La igualdad es una cuestión en la que se va avanzando, pero por la que aún se continúa luchando a nivel universal.

En el contexto del desarrollo tecnológico se hace referencia a la “brecha digital”, a las diferencias existentes desde distintos ámbitos, incluidos de género, acceso material a los recursos necesarios (económico) o generacional. Siendo de gran importancia evitar la “exclusión digital” de ciertos colectivos y realidades sociales, dado el potencial efecto discriminatorio que puede generar sobre grupos desprotegidos³⁷. Trae consecuencia de desigualdades existentes previas que se trasladan al plano digital, no solo desde la perspectiva tecnológica sino sobre todo socioeconómica, continuando con ellas y acrecentándolas³⁸.

³⁶ MARTÍNEZ DE PISÓN CAVERO, J.M., “El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional”, *Anuario de filosofía del derecho*, núm. 32, 2016, p. 429. En relación con STC 281/2006, de 9 de octubre, FJ 3.

³⁷ ARCE JIMÉNEZ, C., “Desafíos para la ciudadanía y el sistema de derechos fundamentales en la era digital”, *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 46, 2022, p. 266.

³⁸ OLARTE ENCABO, S., “Brecha digital, pobreza y exclusión social”, *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 138, 2017, pp. 291 y 292.

En la examinada Declaración de la UE (capítulo II) ya se hizo mención del compromiso de inclusión, en la busca del equilibrio de “género”, de las “personas de edad avanzada”, de las “personas que viven en zonas rurales”, y de las “personas con discapacidad o marginadas”; además de “limitar la explotación de las vulnerabilidades y los sesgos” (15.f).

En el ámbito nacional es mencionable el artículo 81 de la LO 3/2018 donde se garantiza el derecho universal a Internet, independientemente de su condición personal, social, económica o geográfica, proponiendo la superación de la “brecha de género”, y la “brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores”. También en la Carta de Derechos Digitales se incluye el derecho a la igualdad y no discriminación en el entorno digital, buscando garantizar el acceso de todos los colectivos.

Respecto a un tema muy reciente como es la IA, la Ley de igualdad 15/2022 incluyó en su artículo 23 la minimización de sesgos en los algoritmos de sistemas de Inteligencia Artificial, debiendo promover tanto las administraciones públicas como las empresas su uso ética, confiable y respetuosamente con los derechos fundamentales, y con respeto de las recomendaciones de la UE. Cuestión que también se recoge en el artículo 10.2 letras f) y g) del recientemente aprobado Reglamento Europeo de Inteligencia Artificial, según el cual se deberán tomar medidas adecuadas para detectar, prevenir y mitigar posibles sesgos que “puedan afectar a derechos fundamentales” o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión.

Con todo ello se busca la igualdad de trato de los usuarios, sin establecer diferencias económicas según el contenido, lo que parece bastante controvertido con la suscripción a páginas con la promesa de contenido exclusivo o mayor velocidad, o simplemente para poder leer completa una noticia. Es otro ejemplo la problemática actual con las *cookies* que más tarde se comentará. Y si todo ello continúa así, parece llevarnos hacia una privatización del internet, al tener “acceso” pero no poder visualizar ningún contenido sin pago previo.

Un asunto más concreto es el uso de las tecnologías en nuestra relación con las Administraciones Públicas. Se incrementó considerablemente como medidas ante la situación de la pandemia COVID-19, pero tras un tiempo prudencial debimos volver a adaptarnos contando con todas las situaciones posibles. Entra en juego, principalmente, la brecha generacional por todas aquellas personas mayores a las que, indirectamente, se les estaría dificultando el acceso a servicios públicos si todo se vuelve en formato informático.

Tema que en la Carta de Derechos Digitales se recogía como un derecho a la igualdad en el “acceso a los servicios públicos y en las relaciones digitales con las Administraciones públicas”.

Una gran apreciación a este respecto está en el fin de la cita previa obligatoria para interactuar con la Administración a través de un cambio normativo en el artículo 14 de la Ley de Procedimiento Administrativo Común de las Administraciones Públicas, ello “para que el acceso de los ciudadanos a los servicios públicos sea por el canal que cada uno elija y que piense que es el más adecuado”, pues si es útil como canal adicional pero no como sustituto a la presencialidad³⁹. Es decir, no se trataría de frenar el avance de la sociedad sino de garantizar una situación igualitaria, sin impedir (discriminar) el acceso a servicios públicos por el hecho de no hacer uso de estos medios tecnológicos, ya sea por voluntad o desconocimiento.

Por tanto, para la superación de estas brechas debe continuarse haciendo uso de medidas específicas frente a cada una de ellas, al desconocimiento en el manejo de las tecnologías, al acceso universal a los instrumentos necesarios (relacionado con problemas de conectividad o acceso a internet en países menos desarrollados), y a la limitación de sesgos en los sistemas. Limitación que puede resultar ampliamente controvertida en relación con la “caja negra” de la Inteligencia Artificial, definida como la incapacidad para comprender totalmente cómo esta toma las decisiones⁴⁰. Esta “caja negra” puede explicarse fácilmente mediante un símil entre la IA y la red neuronal del cerebro humano, de hecho, una IA es una red neuronal profunda⁴¹. A medida que aumenta su complejidad se vuelve cada vez más difícil entender cómo funciona y cómo toma sus decisiones. Estos problemas de *explicabilidad* son los que continuarán repercutiendo graves consecuencias de inseguridad jurídica al hacer difícil su regulación, no solo por la propia confusión sino también por su dinamismo.

³⁹ Diario de sesiones del Congreso de Diputados, Hacienda y Función Pública, comparecencia Ministro para la Transformación Digital y de la Función Pública (José Luis Escrivá Belmonte), núm. 46, de 31 de enero de 2024, p.22.

⁴⁰ GUTIERREZ DAVID, M.E., “Administraciones inteligentes y acceso al código fuente y los algoritmos públicos. Conjurando riesgos de cajas negras decisionales”, *Derecom*, núm. 31, 2021, p.41.

⁴¹ IBM, *¿Qué son las redes neuronales?*

3.2.- EMERGENTES

El concepto de derecho emergente alude a aquellos derechos que surgen específicamente con ocasión de la era digital, requiriendo de un carácter fundamental para su plena garantía.

3.2.1.- PROTECCIÓN DE DATOS PERSONALES Y DERECHO AL OLVIDO

La protección de datos personales fue el primer derecho fundamental que surgió con la introducción de la tecnología en nuestras vidas, pero se consolidó cuando éstas aún no estaban tan desarrolladas como actualmente, antes de la digitación. Es un derecho que surgió por el uso y sistematización de bases de datos. Se establece por el TC en la sentencia comentada al inicio de los derechos al honor, intimidad y propia imagen, en base al artículo 18.4 CE, con la limitación del uso de la informática. Debiendo tener en cuenta las sucesivas derogaciones en la normativa de datos hasta la actual LO 3/2018 de Protección de Datos Personales. Pero en este caso lo analizaremos como emergente, desde la nueva dimensión que el impacto de la actual era digital le ha ocasionado. Recogido en el art. 8 de la CDFUE y art. 16 TFUE, con desarrollo en el Reglamento UE 2016/679 y, a nivel nacional, la Ley Orgánica 3/2018, y también la Carta de Derechos Digitales recogió el derecho a ser informada sobre la recogida de los datos, su destino y usos, y a acceder, rectificar, oponerse, cancelar, o suprimirlos (III.4).

Datos que según la Carta deben tratarse “sobre la base del consentimiento de la persona afectada”, consentimiento que según la LO 3/2018 debe ser fruto de una “voluntad libre, específica, informada e inequívoca”, “ya sea mediante una declaración o una clara acción afirmativa” (art.6). ¿Características que se cumplen con el actual “consentimiento” de las cookies? Además, dar todo el control de los datos a la autonomía individual resulta muy manejable por los agentes privados que cuentan con mayor conocimiento e intereses. Debe partirse de la dificultad para comprender y valorar correctamente la magnitud de los riesgos que se generan cuando compartimos nuestros datos personales, por lo que en la mayoría de los casos tomamos decisiones que resultan perjudiciales sin darnos cuenta, de hecho, en la mayoría de los casos esa “decisión” tan solo es una “ilusión de control” sobre nuestra información personal⁴². Un ejemplo problemático demostrativo que sucedió es el caso de reconocimiento del iris ocular a cambio de criptomonedas, datos personales que resultan más desprotegidos con el incremento de tecnologías IA que recogen sistemas de identificación biométricos, riesgo previsto en el reciente Reglamento Europeo de Inteligencia Artificial.

⁴² SORIANO ARNANZ, A., “Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos”, *Revista de Derecho Público: Teoría y Método*, vol. 3, 2021, p. 109.

Dicho Reglamento de IA recoge entre las prácticas prohibidas del artículo 5, la introducción en el mercado, puesta en servicio o uso de sistemas de categorización biométrica que “clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual”. Sin embargo, existen salvedades: “no abarca el etiquetado o filtrado de conjuntos de datos biométricos adquiridos legalmente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la aplicación de la ley” (apartado g). Permittedose también el uso de estos sistemas en tiempo real en los espacios públicos para la búsqueda de víctimas de determinados delitos, de personas desaparecidas, para la prevención de amenazas específicas, o para la persecución de sospechosos de determinados delitos (apartado h). Este uso en los espacios de acceso público se encuentra muy limitado, solo para situaciones excepcionales, dado su carácter invasor de derechos y libertades de las personas, afectando a su vida privada al provocar la sensación de estar bajo una vigilancia constante, y disuadir así indirectamente a los ciudadanos de ejercer su libertad de reunión y otros derechos fundamentales. Además de la probabilidad de resultados sesgados con efectos discriminatorios, riesgo que se acrecienta en los sistemas “en tiempo real” debido a su inmediatez⁴³ (considerando 32 y 33).

A la protección de datos se le ha otorgado una dimensión activa, como en el derecho a la intimidad se mencionó, pues este se justifica en un control sobre los datos personales. Control que Morente ya calificó como “*apriorístico*”, “*aparente*” y “*anecdótico*” (conocidos como “*déficit de triple A*”), puesto que en cuanto se manifiesta el consentimiento inicial ya se pierde el control efectivo, una vez publicada la información en la red ésta se pierde en el ciberespacio, y así el control se reduce a unos pocos datos gestionados de forma meramente superficial⁴⁴.

Aquella sentencia del TC 292/2000 mencionada, recoge algunos importantes planteamientos: lo que este derecho fundamental debe hacer es limitar el uso de la informática con el objetivo de asegurar un verdadero poder a la persona sobre el uso y destino de sus datos, extendiéndose la garantía constitucional del art. 18.4 a la protección de cualquiera de los derechos de la persona “sean o no derechos constitucionales y sean o

⁴³ Reglamento de IA, considerando 17: “Los sistemas «en tiempo real» implican el uso de materiales «en directo» o «casi en directo», como grabaciones de vídeo, generados por una cámara u otro dispositivo con funciones similares.”

⁴⁴ MORENTE PARRA, V., “La libertad de los modernos en la sociedad digital: El control de los datos os hará libres”, *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 45, 2021, pp. 223 y 224.

no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado” (FJ 6); y no reduciéndose el objeto únicamente a datos íntimos, sino a cualquier tipo de dato personal, incluso los públicos. También hace alusión a las facultades mencionadas sobre acceso, rectificación, cancelación, oposición (derechos ARCO) (FJ 7).

Otra cuestión bastante controvertida tiene que ver con los informes médicos, datos personales que terminan en almacenamientos de sistemas informatizados de empresas o administraciones sin mediar consentimiento de los afectados⁴⁵. El tratamiento de datos sin consentimiento del afectado sólo es lícito en las condiciones excepcionales contempladas de manera genérica en el art. 6.1 del RGPD. Para este supuesto, el apartado d) hace referencia al “tratamiento necesario para proteger intereses vitales del interesado o de otra persona física”, lo que se aplicó en el caso COVID-19 por el interés general de la sanidad pública. Una resolución destacada sobre informes médicos es la STC 202/1999⁴⁶, donde se cuestionaba la tenencia de datos médicos por una entidad crediticia sin consentimiento expreso ni alegación de interés contractual suficiente, la negativa a la denegación de esos datos solicitada, y el acceso a ellos por otro personal no facultativo. El TC finalmente determinó que “el tratamiento y conservación del diagnóstico médico en la mencionada base de datos sin mediar consentimiento expreso del afectado incumple la garantía que para la protección de los derechos fundamentales se contiene en el art. 53 C.E.” (FJ 5).

Por tanto, la nueva cuestión en la actualidad está en cómo conseguir una protección efectiva de nuestros datos para cada caso concreto, no solo respecto a la gestión de los datos cedidos voluntariamente, sino también de los meramente contenidos en los dispositivos y aplicaciones que son tratados sin consentimiento del usuario. Y teniendo en cuenta la especial protección del tratamiento de los datos de menores en razón al interés superior del menor (art. 92 LOPDGDD).

En cuanto al derecho al olvido, la STC 58/2018 de 4 de junio lo entendió como “facultad inherente al derecho a la protección de datos personales” (FJ 6), y por ello, como derecho fundamental. Por tanto, cabe el derecho al olvido en el espacio virtual, pero ¿de qué manera?, ¿hasta dónde llega?, ¿es posible un derecho al olvido absoluto?

⁴⁵ MARTÍNEZ DE PISÓN CAVERO, J.M., “El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional”, *Anuario de filosofía del derecho*, núm. 32, 2016, p.425.

⁴⁶ STC núm. 202/1999, de 8 noviembre.

La respuesta es no, como todo derecho fundamental, “no es ilimitado, y encuentra sus límites en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos”⁴⁷, sobre todo en los derechos de libertad de expresión (art. 20.1 a CE) y de información (art. 20.1 d CE).

La sentencia del Tribunal de Justicia de la Unión Europea de 2014 del caso Google contra AEPD y Mario Costeja González⁴⁸, al igual que la jurisprudencia del TC, determinó la prevalencia del derecho al olvido frente al interés general en la libertad de información en motores de búsqueda de Internet, salvo que la injerencia en sus derechos fundamentales estuviese justificada por un interés público. Además, para la eliminación de datos, se refiere a que la búsqueda sea hecha a partir del nombre de la persona; acorde al contenido que se ha recogido en el artículo 93 de la LO 3/2018. El apartado segundo del mencionado artículo resolvería la duda acerca de un derecho al olvido absoluto, pues esta eliminación de información personal “no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho”, cuestión que no se contempla en el artículo 17 del Reglamento 2016/679 de la UE sobre protección de datos. Esto podría llevarnos a interpretarlo no como un derecho al “olvido” sino más bien un derecho a la “ocultación”, pues “las fuentes permanecen inalteradas y el resultado se seguirá mostrando cuando la búsqueda se realice por cualquier otra palabra o término distinta al nombre del afectado.”⁴⁹

Otro aspecto, más común actualmente, estaría en el artículo 94 de esta LO 3/2018, el derecho al olvido en el contexto de las redes sociales. Permite la supresión de datos personales facilitados tanto por él, con su simple solicitud, como por terceros. Y en el caso de datos sobre menores deberá procederse directamente a la supresión por la simple solicitud del afectado. Es decir, y teniendo en cuenta el art. 7 sobre su consentimiento, ¿siendo menores de catorce años podrán los titulares de su patria potestad o tutela publicar datos de estos, y solo cuando sean mayores podrán como afectados solicitar este derecho a la supresión de dichos datos? Parece suponer una protección tardía del menor, ampliamente cuestionada y limitada con su derecho al honor. Es cierto que se protegen las intromisiones ilegítimas en sus derechos fundamentales (art. 84 LO 3/2018), pero aquí vuelve a entrar la cuestión de hasta dónde llega esa protección, pues como hemos visto anteriormente los límites se han difuminado (lo que resulta más preocupante aún en este caso de menores desprotegidos).

⁴⁷ STC núm. 89/2022, de 29 junio, FJ 4.

⁴⁸ STJUE (13-05-2014), Google vs. AEPD y Costeja González, C-131/12, FJ 82, 97, 98 y 99.

⁴⁹ Agencia Española de Protección de Datos, “Derecho de supresión (“al olvido”): buscadores de internet”.

Esto demuestra que la era digital continúa afectando a derechos, incluso a los ya reconocidos en la materia, obligando a los tribunales a una “constante labor de actualización de su doctrina para adecuarla a la cambiante realidad social” (STC 58/2018, FJ 4).

3.2.2.- ACCESO A INTERNET

Ya meramente enunciado al hablar del derecho a la igualdad, aquí procederemos a desarrollarlo. Recordemos que la LO 3/2018 incluye en su art. 81 el derecho al acceso universal a Internet, específicamente orientado a la lucha contra la discriminación en lo que a él respecta (cuando parece lógico que lo que primeramente debería garantizarse es el efectivo acceso universal a internet, y como segundo plano ocuparse de que no existan desigualdades dentro de él). Debiendo mencionar también el derecho a la neutralidad de Internet del art. 80 de esta misma ley, el cual impone a los proveedores de servicios de Internet proporcionar una oferta transparente de servicios sin discriminación “por motivos técnico o económicos”. Este derecho al acceso a internet está ampliamente relacionado con el derecho a la igualdad además de otros derechos fundamentales, pero podría desgajarse de ellos como derecho fundamental independiente. Sin embargo, esta Ley nacional, en su disposición final primera, excluye expresamente ambos artículos de la consideración de ley orgánica, lo que impide atribuirles calificación de fundamental.

Sería posible interpretarlo como “una manifestación del mandato de promover la igualdad material del art. 9.2 CE, o como parte de la dimensión objetiva y prestacional de derechos fundamentales para los que se ha constituido en herramienta esencial”⁵⁰. Esto se explica porque en el contexto actual el acceso a internet es clave para garantizar unas condiciones de igualdad y participación en la mayoría (aunque podría decirse todos) de los aspectos de la vida, y su falta supondría un gran obstáculo. Como indiqué anteriormente, la ciudadanía ha pasado a un plano digital, la persona es ahora recogida como una persona digital, se recopilan tus datos de forma informatizada para la elaboración de tu perfil⁵¹, como que si no tuvieses un perfil no existirías (y no solo en las redes sociales); además del necesario acceso a la información que se encuentra en internet, de la tramitación de servicios públicos de forma electrónica (la administración digital), etc. Por lo tanto, ¿sin acceso a internet soy

⁵⁰ ARCE JIMÉNEZ, C., “Desafíos para la ciudadanía y el sistema de derechos fundamentales en la era digital”, *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 46, 2022, p.268. Y COTINO HUESO, L., “Las obligaciones del Estado: el nuevo derecho fundamental de acceso a internet y las garantías a partir de la redefinición de las clásicas libertades informativas”, en VVAA, *La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC)*, 2015, p. 59.

⁵¹ Ver definición recogida en artículo 4.4 del RGPD.

ciudadano digital?, y, ¿si no soy ciudadano digital, sigo siendo ciudadano?

Es mandato constitucional (art. 9.2) que los poderes públicos promuevan las condiciones necesarias para que esa igualdad y participación en la vida sea posible, para que puedan ser disfrutados en su plenitud (cuestión bastante difícil, por no decir imposible, sin internet). La “Declaración conjunta sobre libertad de expresión e Internet” de 2011 de ámbito europeo entendió una obligación positiva a facilitar el acceso a Internet (apartado 6 e) para garantizar la igualdad material, siendo por ello necesaria más intervención estatal en este contexto tan protagonizado por el sector privado a la autorregulación. Esto es exactamente lo que sucede con el acceso a internet desde su visión positiva, y desde la negativa su falta supondría restricciones para el disfrute efectivo y pleno de derechos fundamentales.

Esta visión positiva se extiende al contexto internacional, europeo y nacional, entendiéndolo como derecho fundamental al sustentar el acceso a internet en el derecho a la libertad de expresión e información reconocidos en el art. 20.1 a) y d) CE, como parte de esa “dimensión objetiva y prestacional del derecho fundamental” al que hacía referencia. En el ámbito nacional, un ejemplo está en los conflictos surgidos con la libertad de comunicaciones, como “salvaguarda del pluralismo de los medios de comunicación social y, por tanto, la preservación de la formación de una opinión pública libre”⁵², contando con diversa jurisprudencia constitucional al respecto. Como la STC núm. 73/2014, de 8 mayo, en la que se hace referencia a un derecho a crear medios de comunicación como instrumentos para difundir ideas y opiniones (lo que es jurisprudencia reiterada), permitiendo su configuración por parte del legislador (a través de una autorización) puesto que no se entiende que sea decisión esencial la ordenación de las condiciones. Frente a estas ideas, se formula un voto particular⁵³, con la opinión de la existencia de una verdadera limitación en el contenido material del derecho por la necesidad de concesión administrativa, contrario a la jurisprudencia reiterada de considerarlo contenido esencial de estos derechos. Algo similar ocurre con el acceso a internet desde la perspectiva de herramienta básica para ejercer derechos fundamentales en el contexto actual de globalización tecnológica, para que nuestros derechos puedan ejercerse plenamente.

En el ámbito internacional destacan los números 3 y 24 a 28 de la Declaración de Ginebra de 2003⁵⁴, en relación con el art. 19 de la DUDH, según los cuales “todas las personas, en

⁵² STC núm. 73/2014 de 8 mayo, RTC 2014\73.

⁵³ Voto particular formulado por el Magistrado don Juan Antonio Xiol Ríos a la Sentencia dictada en la cuestión de inconstitucionalidad núm. 2155-2004.

⁵⁴ Declaración de Principios de Ginebra de 12 de diciembre de 2003 para *Construir la Sociedad de la Información: un desafío global para el nuevo milenio*, adoptada en la Cumbre Mundial sobre la Sociedad de la Información, organizada por la Unión Internacional de Telecomunicaciones y las Naciones Unidas.

todas partes, deben tener la oportunidad de participar” en la Sociedad de la Información, haciendo uso de estos derechos; y para ello será necesaria la “capacidad universal de acceder”, como “elemento indispensable”. Junto a ellas, posteriores Declaraciones de Naciones Unidas y Directivas europeas lo recogieron.

Por otro lado, otra perspectiva que se plantea es vincular el acceso a internet con el derecho fundamental a la educación⁵⁵. En tal caso, cuestiones como la disponibilidad de ordenadores, sería considerada simple medida adicional, como se dispuso en la STC 140/2002, de 3 de junio, FJ 5: *“Desde luego, no puede desconocerse la relevancia que la utilización de medios informáticos tiene hoy en el ámbito educativo, pero esto no autoriza a alterar las reglas de la ‘vida del establecimiento’ y que tienen por finalidad mantener el buen orden y adecuado desarrollo de aquélla, en lo que ahora importa, en materia de ordenadores, [...], no se le ha privado al demandante de amparo de la posibilidad de utilizar el ordenador, sino que meramente se le ha limitado, puesto que, si no en su celda, puede usarlo en el local señalado para tal fin”*.

La adopción de tales medidas por los Estados Miembros responde al llamamiento realizado por el Consejo Europeo de Lisboa de 23 y 24 de marzo de 2000 para “garantizar que todos los centros de enseñanza dispongan de acceso a Internet y a los recursos multimedia”. Medidas adicionales que, como indica el considerando 46 de la Directiva 2002/22/CE del Parlamento Europeo y del Consejo, los Estados Miembros pueden adoptar de conformidad con el Derecho comunitario.

Ya a nivel declarativo, la Declaración de la UE de 2023 sobre los Derechos y Principios Digitales para la Década Digital (capítulo II) hace referencia al “acceso a una conectividad digital asequible y de alta velocidad”, velando por un acceso a internet con alcance europeo, incluso para aquellas personas con menores ingresos. Y a nivel nacional, la Carta de Derechos Digitales de 2021 añade por igual un derecho de acceso a internet universal, asequible y no discriminatorio, promovido e impulsado por los poderes públicos.

3.2.3.- DESCONEJIÓN DIGITAL

Compete de manera especial al mundo laboral puesto que la digitalización crea un efecto de “borrado” de las clásicas fronteras de tiempo y lugar del trabajo, y así, entre los tiempos de

⁵⁵ COTINO HUESO, L., “Las obligaciones del Estado: el nuevo derecho fundamental de acceso a internet y las garantías a partir de la redefinición de las clásicas libertades informativas”, en VVAA, *La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC)*, 2015, p. 60 y 61.

trabajo y ocio/cuidado⁵⁶, creando una sobreexplotación tecnológica que da origen a nuevas enfermedades profesionales⁵⁷.

En el considerando 4 del preámbulo de la Declaración de la UE de 2023 se menciona que el Parlamento Europeo, en distintas resoluciones e iniciativas, ha pedido que se refuerce la protección de “derechos” de los usuarios en el entorno digital como el derecho a la desconexión, entre otros; cuestión destacable es que lo menciona de manera separada a los “derechos fundamentales” que cita anteriormente. En el resto del artículo declarativo no vuelve a mencionarlo, aunque sí podría extraerse cierta interpretación del punto 6, según el cual *“Las organizaciones sindicales y patronales desempeñan un papel importante en la transformación digital, en particular en lo relativo a la definición de unas condiciones de trabajo justas y equitativas, también en lo que respecta al empleo de herramientas digitales en el trabajo”*.

En España, a nivel normativo, se incluyó la desconexión digital entre los derechos del ámbito laboral en diversas disposiciones que a continuación se analizarán; de la misma manera que, a nivel declarativo, lo incluyó la Carta de Derechos Digitales (XIX). El artículo 20 bis del Estatuto de los Trabajadores reconoce el derecho a la desconexión digital de los trabajadores, pero ello “frente al uso de dispositivos de videovigilancia y geolocalización”, no lo incluye en el primer supuesto que se apunta frente al “uso de los dispositivos digitales puestos a su disposición por el empleador”; de la misma manera es introducido por reforma de la LOPDGDD en el Estatuto Básico del Empleado Público (art. 14 apartado j bis). El art. 18 de la Ley de trabajo a distancia ya se refiere a limitar el uso de los “medios tecnológicos de comunicación empresarial y de trabajo” durante los periodos de descanso, respetando en concreto la duración máxima de la jornada; que se entenderá “en los términos establecidos en el artículo 88 de la Ley Orgánica 3/2018”. Este art. 88 lo concreta en el respeto al tiempo de descanso fuera del tiempo de trabajo, y la conciliación de la actividad laboral y la vida personal y familiar; añadiendo, además, que se “elaborará” una política interna por el empleador para determinar las modalidades del ejercicio de este derecho. Es decir, se va concretando más, pero dejando aún el mayor margen interno a las empresas para su regulación y establecimiento de las medidas necesarias.

⁵⁶ RODRÍGUEZ FERNÁNDEZ, M.L. Y PÉREZ DEL PRADO, D., *Economía digital: su impacto sobre las condiciones de trabajo y empleo. Estudio de caso sobre dos empresas de base tecnológica*, Fundación para el Diálogo Social, 2017, p. 21. En relación con WEBSTER J. AND RANDLE K., *Virtual Workers and the Global Labour Market*, London: Palgrave Macmillan, 2016, p. 13-14.

⁵⁷ COTERILLO LASO, R., “Hacia la recuperación del poder perdido de la Representación Legal de los Trabajadores en la nueva era digital. Una visión comparada en el nuevo marco europeo”, del *Congreso Internacional: El derecho digital en un escenario jurídico cambiante*, organizado por el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, mayo de 2024.

Para esa negociación colectiva de regulación del derecho, los firmantes del Acuerdo para el Empleo y la Negociación Colectiva para los años 2023, 2024 y 2025, deben tener en cuenta ciertos criterios como su ámbito (“todos los dispositivos y herramientas susceptibles de mantener la jornada laboral más allá de los límites”), la no obligación a responder llamadas o comunicados fuera de la jornada laboral, la prohibición de tratos diferenciados o sanciones por hacer uso de este derecho, etc. Destacando como buena práctica el uso del “envío retardado” para que las comunicaciones al trabajador sólo se realicen dentro del horario laboral.

Cuestiones que en la teoría son muy favorables pero que en la mayoría de los casos de la práctica si se hace uso de ello puede verse con malos ojos, existiendo cierta “coacción” interna o social. Sin embargo, cada vez más se le está dando visibilidad, en protección de la salud mental y buscando la conciliación entre la vida laboral y personal/familiar.

Por su actual y continuo desarrollo legislativo y práctico (jurisprudencial), parece que podría llegar a constituirse como un derecho fundamental originario de la era digital.

3.2.4.- IDENTIDAD DIGITAL

De todo lo expuesto en los derechos precedentes parece derivarse un derecho a la propia identidad digital, similar al derecho a la autodeterminación informativa. Resultaría de la confluencia de derechos fundamentales como la igualdad, intimidad, propia imagen, y sobre todo la protección de datos personales, entre otros. Todos ellos unidos dando lugar a una nueva dimensión de la identidad, desde la perspectiva concreta de la identidad digital (al igual que sucedía con la ciudadanía).

En el contexto europeo, a nivel normativo hay que hacer referencia al Reglamento UE 2016/679, especialmente a sus artículos 7, respecto a las condiciones para un consentimiento válido del tratamiento de nuestros datos, 9, para el tratamiento de datos personales especiales (equivalente al art. 9 de la LOPDGDD), y 22, que garantiza el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado como la elaboración de perfiles. Y a nivel no normativo, la Declaración de 2023 sobre Derechos y Principios Digitales a la que hemos estado haciendo referencia recoge en el punto 7 la posibilidad de una identidad digital accesible y voluntaria pero orientada al acceso de servicios públicos de la UE; según el punto 10, todos deberíamos poder “elegir”

efectivamente y de manera “libre” los servicios digitales y la información de la que estas hacen uso; y en el punto 15 f), perteneciente al capítulo IV de participación en el espacio público digital, alude a la capacitación de las personas para que puedan “tomar decisiones” concretas “con libertad”, y limitando la explotación de las vulnerabilidades y sesgos, “en particular a través de la publicidad personalizada”.

En el contexto nacional, la LOPDGDD, al igual que la normativa europea, entiende el consentimiento como la “manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta” (art. 6.1); y la Carta de Derechos Digitales la enuncia directamente como el “derecho a la identidad en el entorno digital”, sin poder ser controlada, manipulada ni suplantada por terceros, y el derecho de la persona a no ser perfilada.

Por lo tanto, el aspecto esencial que caracteriza el surgimiento de este derecho es la libertad de consentimiento, de creación y gestión de nuestros propios datos; lo que a *contrario sensu* implica la prohibición de que sean otros quienes los gestionen, y menos aún, que nos creen una identidad. Es decir, es la “persona digital” quien decide qué datos verter en la red y de qué manera, que incluso pueden ser falsos resultado de la presión a una mejor integración en la sociedad. Pero el problema además es que la red no solo toma los datos propios, sino también todo tipo de interacciones e historiales en todas las webs, redes y aplicaciones a las que accedemos, conocido como “huella digital”; o incluso por datos proporcionados por terceros con los que pudiste interactuar a través de simples “me gusta”, comentarios o etiquetas de tu persona en perfiles de familiares, amigos o incluso por personas ajenas sin ningún tipo de consentimiento.

Datos cuyo “consentimiento” es muy cuestionable. “Libre” es el concepto en que la normativa incide cuando se refiere al consentimiento, lo que en la actualidad resulta más bien condicionado, ni siquiera de forma indirecta, con las *cookies* a aceptarlas frente a rechazarlas que implicaría suscribirte obligatoriamente y con pago en algunas ocasiones a la página respectiva. Por lo que ese “consentimiento libre” se reduce ahora a aceptar ceder tus preferencias para diversos fines (los cuales no se leen al completo, o incluso ni al principio) a cambio de una compensación económica o creación de tu identidad digital por otros. Dejando así de tener el control de nuestra propia identidad. Lo que en consecuencia genera un bucle al estar los resultados cada vez más acotados según las preferencias, ya ni siquiera se estaría teniendo libertad en las búsquedas y contenidos que se muestran por estar siendo totalmente orientados. Es un algoritmo quién nos dice qué es lo que nos gusta y necesitamos, “corrige nuestras búsquedas en Google, nos dice cuáles son nuestros amigos potenciales en las redes sociales, nos indica cuáles son las películas, los libros o la

música que se adaptan mejor a nuestros gustos”⁵⁸. Esto fue denominado por los autores Neil M. Richards y Jonathan H. King como “The Identity Paradox”⁵⁹, la paradoja de la identidad, pues el “yo soy” y “me gusta” pasaría a convertirse en “tú eres” y “te gustará”, perdiendo así nuestra auténtica identidad.

Esto se agrava con la cada vez mayor “publicidad” de aspectos de nuestra vida, que deja de ser privada, en distintas redes sociales o blogs, aspectos que permanecen en la red de manera prácticamente infinita (no sabemos exactamente lo que sucede cuando por ejemplo se borra una publicación, a dónde ésta se dirige). De manera que en la actualidad, “en el contexto de las nuevas tecnologías lo privado, y por ende la intimidad, se configura en el espacio público”⁶⁰.

Aunque no esté reconocido como tal derecho fundamental, será necesario que el derecho intervenga para redireccionar estas prácticas hacia un verdadero cumplimiento de los derechos fundamentales, como es garantizar la libertad de determinación de la propia identidad en el mundo digital.

⁵⁸ GARRIGA DOMÍNGUEZ, A., “La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el reglamento general de protección de datos de la Unión Europea”, *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 38, 2018, p. 127.

⁵⁹ NEIL M. RICHARDS & JONATHAN H. KING, “Three Paradoxes of Big Data”, *Stanford law review online*, vol. 66:41, 2013, pp. 43-44.

⁶⁰ ARCE JIMÉNEZ, C., *¿Una nueva ciudadanía para la era digital?*, Dykinson, Madrid, 2022, p. 16.

CONCLUSIONES

- Esta nueva era de globalización del internet supone un proceso dinámico, el entorno digital se encuentra en constante evolución, lo que obliga a nuestra regulación y jurisprudencia también a que lo sea. Resulta difícil predecir las consecuencias que pueden producir en nuestra sociedad, pero será cuestión de resolver de la mejor manera el supuesto tratando simplemente de proteger la máxima dimensión de los derechos con los que ya contamos, tratando de evitar su vulneración.
- Principalmente habrá que compatibilizar la regulación legislativa con el ámbito de discrecionalidad que se les está dejando a los agentes privados de las plataformas, poniendo el foco en que se trata de la regulación de derechos fundamentales, no podemos dejarlos al libre arbitrio de estos sujetos si verdaderamente buscamos garantizar los derechos de las personas en los entornos digitales. Como por ejemplo la vida privada, gran perjudicada por los avances tecnológicos, pero incluso en este nuevo espacio continúa siendo un derecho esencial para garantizar la individualidad y libertad de las personas; frente al “dataísmo” o ideología del dato, donde parece que este trata de sustituir a la realidad material por una transparencia absoluta, lo que podría generar una tendencia a la uniformidad y en contra de la diversidad⁶¹.
- Es también trabajo por parte de todos conocer el uso que se le está dando a nuestra información y las consecuencias de la exposición de toda nuestra vida, desdibujando los límites entre lo privado y lo público, facilitando la constante vulneración de nuestra intimidad.
- Se requiere por ello una protección de los datos personales más fuerte, en particular en el caso de los menores que nacen en pleno desarrollo tecnológico y sus vidas pasan a ser retransmitidas en *live*. En la actualidad los datos cuentan con un indudable valor comercial, se habla ya de la “Economía del Dato”, se han convertido en la principal fuente de riqueza, como principal fuente económica (pensar que las mayores empresas hoy día son las tecnológicas). La información cada vez es más valiosa, desplazando así a las tradicionales mercancías materiales⁶². Estudian todas nuestras imágenes e interacciones para finalmente conocer datos relacionados con la salud, ideología, religión, política... incluso por lo que el internauta ha “tirado a la basura”; llegando a conocernos más que nosotros mismos, y perdiendo así el control de nuestros propios datos.

⁶¹ FERNÁNDEZ BARBUDO, C., “El nuevo concepto de privacidad: la transformación estructural de la visibilidad”, *Revista de Estudios Políticos*, núm. 185, 2019, p.161 y 162.

⁶² FERNÁNDEZ LACASA, J.M., en la jornada “El impacto de la IA en el ejercicio de las profesiones jurídicas” del *Aula TalentiUS*, Universidad de Oviedo.

- Especialmente para el acceso a internet, el principal reto estará en superar la brecha de diferencias entre países más y menos desarrollados, en la brecha económica, necesario para garantizar el pleno ejercicio de derechos fundamentales puesto que, con independencia a estar más o menos de acuerdo con el creciente uso de las tecnologías, en la actualidad podría hacerse una analogía con la interdicción del derecho altomedieval en la que como condena ante delitos graves no se les aplicaba la muerte civil directamente sino que se les expulsaba de la comunidad, lo que en muchos casos impedía en la práctica que tuviesen los requisitos necesarios para adquirir la capacidad jurídica. En nuestro caso, “expulsarnos de la comunidad” lo constituiría el no acceso a internet, impidiendo el acceso a información y servicios, negándose así indirectamente la ciudadanía digital, la ciudadanía.
- Pero esa necesaria igualdad no sólo está presente en el acceso a internet sino en todos los planos, debería ser la base de cualquier sociedad y es importante trasladarla y ajustarla al mundo digital para evitar continuar perpetuando las desigualdades. Debemos asegurarnos siempre de que ésta se dé desde la perspectiva legal formal hasta su práctica efectiva. Tanto en el acceso a internet en sí como en el acceso a conocimientos para su uso, y sin olvidar a los colectivos más vulnerables. Fenómeno que se viene conociendo como la democratización de la tecnología.

En resumen, la transformación derivada de las nuevas formas de comunicación y su uso generalizado “no produce un vaciamiento de la protección constitucional de los derechos fundamentales y tampoco [...] modifica el contenido y alcance de los derechos fundamentales que deben ser ponderados cuando se invoca una vulneración”⁶³. Sobre todo, en este contexto, ya el TEDH ha anunciado que “el riesgo de perjuicio que suponen los contenidos y las comunicaciones en internet para el ejercicio y disfrute de los derechos humanos y las libertades, en particular el derecho al respeto de la vida privada, es ciertamente mayor que el que plantea la prensa [escrita]”⁶⁴. Las tecnologías son buenas para nuestro avance como sociedad, además que sería imposible plantearnos una teoría involucionista, por lo que la cuestión esencial está en que haya cierto control sobre ellas. Control que debe ser urgente, acorde al rápido desarrollo digital. Coincido completamente con el juez Eloy Velasco cuando plantea como solución la “humanización” de la tecnología⁶⁵. Consistiría en lo que se viene dando a entender a lo largo de todo el trabajo, en englobar

⁶³ STC 93/2021, de 10 de mayo, FJ 2.

⁶⁴ STEDH, Consejo Editorial de Pravoye Delo y Shtekel c. Ucrania, de 5 de mayo de 2011, § 63.

⁶⁵ VELASCO, ELOY, “Derechos fundamentales en la era digital”, charla TED [vídeo], 2017: «En definitiva, para que cuando en el día de mañana me pregunten ¿cuál es el precio que estás pagando por el teléfono móvil? diga exclusivamente la tarifa y NO mis derechos humanos».

la humanidad, el derecho, en su regulación. Debemos pensar que con estos nuevos “productos”, como son los datos, no estamos ante una nueva mercancía sino ante los derechos fundamentales de las personas, no hablamos ya de objetos físicos sino de la esencia de las personas, y no podemos dejar que se pierda en la red y en las manos privadas.

BIBLIOGRAFÍA Y DOCUMENTACIÓN (enlaces actualizados a junio 2024)

- AGÜERO ORTIZ, A., “Derecho a la propia imagen y divulgación en prensa de fotos obtenidas de Facebook”, *Derecho Privado y Constitución*, núm. 38, 2021, pp. 119-155. Disponible en: <https://doi.org/10.18042/cepc/dpc.38.04>.
- Apuntes de la asignatura “Derechos Fundamentales y Libertades Públicas”, por BASTIDA FREIJEDO, F.J., Universidad de Oviedo.
- Apuntes de la asignatura “Historia del Derecho Público y Privado”, por PÉREZ-CASTRO PÉREZ, R., Universidad de Oviedo.
- ARCE JIMÉNEZ, C., “Desafíos para la ciudadanía y el sistema de derechos fundamentales en la era digital”, *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 46, 2022, pp. 241-272. Disponible en: <https://doi.org/10.20318/dyl.2022.6520>.
- ARCE JIMENEZ, C., *Una lucha contra el “odio digital” con pleno respeto a los derechos fundamentales*, Atelier, Barcelona, 2024.
- ARCE JIMÉNEZ, C., *¿Una nueva ciudadanía para la era digital?*, Dykinson, Madrid, 2022.
- COTERILLO LASO, R., “Hacia la recuperación del poder perdido de la Representación Legal de los Trabajadores en la nueva era digital. Una visión comparada en el nuevo marco europeo”, del *Congreso Internacional: El derecho digital en un escenario jurídico cambiante*, organizado por el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, mayo de 2024.
- COTINO HUESO, L., “Las obligaciones del Estado: el nuevo derecho fundamental de acceso a internet y las garantías a partir de la redefinición de las clásicas libertades informativas”, en VVAA, *La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC)*, 2015, pp. 51-93. Disponible en: <https://hdl.handle.net/10983/23002>.
- DE LUCAS MARTÍN, J., “Ciudadanía: concepto y contexto. Algunas observaciones desde Principia iuris de L. Ferrajoli”, *Anuario de filosofía del derecho*, núm. 29, 2013, pp. 101-124. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=4550447>.
- Diario de sesiones del Congreso de Diputados, Hacienda y Función Pública, comparecencia Ministro para la Transformación Digital y de la Función Pública (José Luis Escrivá Belmonte), núm. 46, de 31 de enero de 2024. Disponible en: https://www.congreso.es/public_oficiales/L15/CONG/DS/CO/DSCD-15-CO-46.PDF.

- FERNÁNDEZ BARBUDO, C., “El nuevo concepto de privacidad: la transformación estructural de la visibilidad”, *Revista de Estudios Políticos*, núm. 185, 2019, pp. 139-167. Disponible en: <https://doi.org/10.18042/cepc/rep.185.05>.
- FERNÁNDEZ LACASA, J.M., en la jornada “El impacto de la IA en el ejercicio de las profesiones jurídicas” del *Aula TalentiUS*, Universidad de Oviedo.
- GARCÍA GARCÍA, A., “La protección digital del menor: el fenómeno del *sharenting* a examen”, *Revista de Derecho UNED*, núm. 27, 2021, pp.455-492. Disponible en: <https://doi.org/10.5944/rduned.27.2021.31094>.
- GARRIGA DOMÍNGUEZ, A., “La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el reglamento general de protección de datos de la Unión Europea”, *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 38, 2018, pp. 107-139. Disponible en: <https://hdl.handle.net/10016/28000>.
- GUTIERREZ DAVID, M.E., “Administraciones inteligentes y acceso al código fuente y los algoritmos públicos. Conjurando riesgos de cajas negras decisionales”, *Derecom*, núm. 31, 2021, pp.19-105. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=8193102>.
- INSTITUTO NACIONAL DE ESTADÍSTICA (INE), *Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares*, de 28 noviembre de 2023. Disponible en: https://www.ine.es/prensa/tich_2023.pdf.
- MARTÍN VALVERDE, A. Y GARCÍA MURCIA, J., *Manual Derecho del trabajo*, Tecnos, edición 2023.
- MARTÍNEZ DE PISÓN CAVERO, J.M., “El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional”, *Anuario de filosofía del derecho*, núm. 32, 2016, pp. 409-430. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=5712518>.
- MARTÍNEZ DE PISÓN CAVERO, J.M., “Vida privada sin intimidad. Una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo”, *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 37, 2017, pp. 51-84. Disponible en: <https://doi.org/10.14679/1047>.
- MORENTE PARRA, V., “Big data o el arte de analizar datos masivos: Una reflexión crítica desde los derechos fundamentales”, *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 41, 2019, pp. 225-260. Disponible en: <https://hdl.handle.net/10016/30630>.
- MORENTE PARRA, V., “La libertad de los modernos en la sociedad digital: El control de los datos os hará libres”, *Derechos y libertades: Revista de Filosofía del Derecho y*

- derechos humanos*, núm. 45, 2021, pp. 199-231. Disponible en: <https://doi.org/10.20318/dyl.2021.6106>.
- MOSSBERGER, K., TOLBERT, C.J., AND MCNEAL, R.S., *Digital Citizenship: The Internet, Society, and Participation*, MIT Press, 2007. Limited part available in: https://books.google.es/books?id=LgJw8U9Z0w0C&printsec=frontcover&redir_esc=y#v=onepage&q&f=false.
 - MURILLO DE LA CUEVA, P.L., “La construcción del derecho a la autodeterminación informativa”, *Revista de estudios políticos*, núm. 104, 1999, pp. 35-60. Disponible en: <http://hdl.handle.net/10396/2238>.
 - NEIL M. RICHARDS & JONATHAN H. KING, “Three Paradoxes of Big Data”, *Stanford law review online*, vol. 66:41, 2013, pp. 41-46. Available at SSRN: <https://ssrn.com/abstract=2325537>.
 - OLARTE ENCABO, S., “Brecha digital, pobreza y exclusión social”, *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 138, 2017, pp. 285-313. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=6552396>.
 - RÓDENAS CORTÉS, P., “Protección jurisdiccional al honor: polémica sobre prevalencia de derechos constitucionalmente protegidos; delimitación de competencias”, *Anuario de la Facultad de Derecho*, vol. XXIX, 2011, pp. 285-299. Disponible en: <http://hdl.handle.net/10662/11611>.
 - RODRÍGUEZ FERNÁNDEZ, M.L. Y PÉREZ DEL PRADO, D., *Economía digital: su impacto sobre las condiciones de trabajo y empleo. Estudio de caso sobre dos empresas de base tecnológica*, Fundación para el Diálogo Social, 2017. Disponible en: http://fdialogosocial.org/public/upload/2/23_FdS_Economia-digital-impacto-condiciones-trabajo-y-empleo_2017_final.pdf.
 - SORIANO ARNANZ, A., “Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos”, *Revista de Derecho Público: Teoría y Método*, vol. 3, 2021, pp. 85-127. Disponible en: https://doi.org/10.37417/RPD/vol_3_2021_535.
 - VELASCO, ELOY, *Derechos fundamentales en la era digital*, charla TED [vídeo], 2017. Disponible en: https://www.ted.com/talks/eloy_velasco_derechos_fundamentales_en_la_era_digital?utm_campaign=tedsread&utm_medium=referral&utm_source=tedcomshare.
 - WARREN S.D. and BRANDEIS L.D., “The Right to Privacy”, *Harvard Law Review*, vol.IV, núm. 5, december 15, 1890. Available at: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

- WEBSTER J. AND RANDLE K., *Virtual Workers and the Global Labour Market*, London: Palgrave Macmillan, 2016. Available at: <http://ndl.ethernet.edu.et/bitstream/123456789/21815/1/38.pdf>.

OTRAS FUENTES (enlaces actualizados a junio 2024)

- Agencia Española de Protección de Datos, “Derecho de supresión (“al olvido”): buscadores de internet”. Disponible en: <https://www.aepd.es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido>.
- *El Reglamento Europeo de IA, en resumen*, del Ministerio de Asuntos Económicos y Transformación Digital. Disponible en: https://portal.mineco.gob.es/es-es/digitalizacionIA/sandbox-IA/Documents/20220919_Resumen_detallado_Reglamento_IA.pdf.
- IBM, *¿Qué son las redes neuronales?* Disponible en: <https://www.ibm.com/es-es/topics/neural-networks>.
- NOYB, *Noyb insta a 11 APD a detener inmediatamente el uso indebido de datos personales para la IA por parte de Meta*, de 6 de junio de 2024. Disponible en: <https://noyb.eu/es/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai>.
- ORGANIZACIÓN DE CONSUMIDORES Y USUARIOS, *Inteligencia Artificial: OCU denuncia a Meta ante la Agencia de Protección de Datos*, de 31 de mayo de 2024. Disponible en: [Inteligencia Artificial: OCU denuncia a Meta ante la Agencia de Protección de Datos](#).
- ORGANIZACIÓN DE CONSUMIDORES Y USUARIOS, *Meta quiere tus datos para “entrenar” su IA... pero tendrá que cambiar de planes*, de 17 de junio de 2024. Disponible en: <https://www.ocu.org/consumo-familia/derechos-consumidor/noticias/meta-privacidad-ocu>.

NORMATIVA CITADA

Legislación internacional y europea:

- Declaración Universal de Derechos Humanos de 1948.
- Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950.
- Convención sobre los Derechos del Niño de 1989, Asamblea General de las Naciones Unidas.
- Carta de los Derechos Fundamentales de la Unión Europea del 2000.
- Tratado de Funcionamiento de la Unión Europea de 2010.
- 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 (Reglamento general de protección de datos).
- Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 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), de 14 de mayo de 2024.
- Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas.

Soft law:

- Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye, Consejo de Derechos Humanos, 32º período de sesiones, 11/05/2016.
- Declaración de Principios de Ginebra de 12 de diciembre de 2003 para *Construir la Sociedad de la Información: un desafío global para el nuevo milenio*, adoptada en la Cumbre Mundial sobre la Sociedad de la Información, organizada por la Unión Internacional de Telecomunicaciones y las Naciones Unidas.
- Declaración Conjunta sobre Libertad de Expresión e Internet de 2011.
- Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01), del Parlamento Europeo, Consejo y Comisión Europea.
- Conclusiones de la Sesión del Consejo Europeo de Lisboa del 23 y 24 de marzo de

2000.

Legislación estatal:

- Constitución Española de 1978.
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Ley Orgánica 3/1985, de 29 de mayo, sobre modificación de la Ley orgánica 1/1982, de 5 de mayo, sobre protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
- Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 10/2021, de 9 de julio, de trabajo a distancia.
- Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Resolución de 19 de mayo de 2023, de la Dirección General de Trabajo, por la que se registra y publica el V Acuerdo para el Empleo y la Negociación Colectiva.

Soft law:

- Carta de Derechos Digitales de 2021.

JURISPRUDENCIA Y DOCTRINA JUDICIAL

Jurisprudencia del TEDH:

- Sentencia Tribunal Europeo de Derechos Humanos, Castells c. España, de 23 abril 1992.
- Sentencia Tribunal Europeo de Derechos Humanos, Féret c. Bélgica (demanda nº38098/02), de 16 de julio de 2009.
- Sentencia Tribunal Europeo de Derechos Humanos, Consejo Editorial de Pravoye Delo y Shtekel c. Ucrania, de 5 de mayo de 2011.
- Sentencia Tribunal Europeo de Derechos Humanos, López Ribalda y otros c. España (demandas nº 1874/13 y 8567/13), de 9 de enero de 2018.

Jurisprudencia del TJUE:

- Sentencia Tribunal de Justicia de la Unión Europea, Google c. AEPD y Costeja González, C-131/12, de 13 mayo de 2014.

Jurisprudencia del TC:

- Sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre.
- Sentencia del Tribunal Constitucional 159/1986, de 16 de diciembre.
- Sentencia del Tribunal Constitucional 171/1990, de 12 de noviembre.
- Sentencia del Tribunal Constitucional 214/1991, de 11 de noviembre.
- Sentencia del Tribunal Constitucional 223/1992, de 14 de diciembre.
- Sentencia del Tribunal Constitucional 254/1993 de 20 de julio.
- Sentencia del Tribunal Constitucional 117/1994, de 25 de abril.
- Sentencia del Tribunal Constitucional 34/1996, de 11 de marzo.
- Sentencia del Tribunal Constitucional 202/1999, de 8 de noviembre.
- Sentencia del Tribunal Constitucional 98/2000, de 10 de abril.
- Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.
- Sentencia del Tribunal Constitucional 81/2001, de 26 de marzo.
- Sentencia del Tribunal Constitucional 46/2002, de 25 de febrero.
- Sentencia del Tribunal Constitucional 140/2002, de 3 de junio.
- Sentencia del Tribunal Constitucional 281/2006, de 9 de octubre.
- Sentencia del Tribunal Constitucional 72/2007, de 16 de abril.
- Sentencia del Tribunal Constitucional 235/2007, de 7 de noviembre.
- Sentencia del Tribunal Constitucional 158/2009 de 29 de junio.
- Sentencia del Tribunal Constitucional 99/2011, de 20 de junio.
- Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre.

- Sentencia del Tribunal Constitucional 73/2014, de 8 de mayo.
- Sentencia del Tribunal Constitucional 58/2018, de 4 de junio
- Sentencia del Tribunal Constitucional 27/2020, de 24 de febrero.
- Sentencia del Tribunal Constitucional 93/2021, de 10 de mayo.
- Sentencia del Tribunal Constitucional 99/2021, de 10 de mayo.
- Sentencia del Tribunal Constitucional 89/2022, de 29 de junio.
- Sentencia del Tribunal Constitucional 119/2022, de 29 de septiembre.
- Sentencia del Tribunal Constitucional 83/2023, de 4 de julio.

Jurisprudencia del TS:

- Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (rec. 5444/2000).
- Sentencia del Tribunal Supremo 766/2020 de 15 septiembre.

Jurisprudencia de AP:

- Sentencia de la Audiencia Provincial de Navarra (Sección 3ª) 116/2020, de 26 febrero, JUR/202/299802.