LaNbarque
Abogados
CENTRADOS EN TUS INTERESES

ALEGACIONES A LAS DIRECTRICES 3/2025, DEL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, SOBRE LA INTERACCIÓN ENTRE LA LEY DE SERVICIOS DIGITALES Y EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

1. Entorno regulatorio y situación del mercado de servicios digitales.

El derecho a la protección de datos como derecho fundamental ha de ser interpretado de forma que se favorezca su mayor viabilidad. Por ello, sería indispensable que la interpretación del alcance del RGPD, en atención a la mayor optimización de sus mandatos de protección, y en relación con la Ley de Servicios Digitales, se efectuara teniendo en cuenta el entorno regulatorio sectorial y la situación fáctica de la repercusión del mercado en el derecho fundamental, a fin de conocer los elementos sistémicos que hayan de afrontarse para contribuir a la satisfacción del estándar de protección jurídica que es preciso proporcionar en garantía de la dignidad de las personas.

a) Nuevo entorno regulatorio de la protección de datos de carácter personal

Junto con el RGPD se han aprobado diversas normas que, aunque algunas de ellas, formalmente no afectan al RGPD, sin embargo, resulta obvio que inciden materialmente en la protección que el ordenamiento jurídico provee a los datos de carácter personal, pues en otro caso, se trataría de normas meramente retóricas que no tendría incidencia alguna en los contornos del derecho fundamental. A saber:

- Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)

- Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos)

- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por

el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 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)

- Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847

Aun cuando la interpretación de este haz de normas no corresponda al Comité Europeo de Protección de Datos no se puede desconocer la influencia que van a tener y, no en todo caso, en la dirección de mayor fortalecimiento de la autodeterminación informativa de las personas.

b) Repercusión de las actividades del mercado en el derecho fundamental

De acuerdo con el informe Comité Internacional de Bioética de la UNESCO, "Big Data y Salud":

> "La escala y la complejidad del procesamiento de datos personales en el área del Big Data hace prácticamente imposible que las personas realicen un seguimiento o tomen decisiones significativas sobre todos los usos de sus datos personales… Esto conduce a una pérdida de autonomía que, en consecuencia, significa una pérdida de control y a una pérdida de libertad frente a las decisiones tomadas por el entorno tecnológico y los procesos automatizados. La gobernanza tiene que compensar esta pérdida de control, garantizando que todas las dimensiones de la autonomía sean respetadas y apoyadas"[1].

La descripción que adopta este informe supone el fracaso de la protección jurídica de la autonomía informativa en el ámbito digital. En consecuencia, se debe aplicar una gobernanza que contribuya a compensar el declive de la efectividad del derecho fundamental a la protección de datos de carácter personal.

Asimismo, el exponencial desarrollo de tecnologías emergentes como la inteligencia artificial, "Internet de las cosas", robótica, nanotecnología, biotecnología o neurotecnología presentan nuevos retos que deben ser ponderados en las pautas de interpretación de las normas jurídicas.

Debe tenerse muy en cuenta el fenómeno de la denominada "economía de la atención". El Parlamento Europeo emitió la Resolución, de 12 de diciembre de 2023, sobre el diseño adictivo de los servicios en línea y la protección del consumidor en el mercado único de la Unión. Esta resolución considera que algunas empresas tecnológicas utilizan el diseño para

[1]Párrafo 48. SHS/SÍ/IBC-24/17/3 REV.2. París, 15 de septiembre de 2017.

aprovechar las vulnerabilidades de los usuarios, a fin de captar su atención y aumentar la cantidad de tiempo que pasan en las plataformas digitales, a fin de maximizar los datos recopilados, el tiempo y el beneficio. En consecuencia, se "insta a la Comisión a que promueva un diseño ético de los servicios en línea por defecto; cree firmemente que los proveedores deben alejarse de las características de plataforma que fomenten centrarse en monopolizar la atención de los usuarios"[2]

Existe una multitud de estudios empíricos sobre el impacto de las redes sociales en la salud mental de los menores. Aspecto al que las directrices dedica un apartado[3].

Asimismo, existe una creciente preocupación sobre el impacto de las redes sociales en la democracia. Antes de todo, procede advertir que no se puede caer en un planteamiento maniqueo. Los regímenes autoritarios interfieren el uso de las redes sociales pues es un instrumento a través de los cuales los ciudadanos ejercen sus derechos constitucionales y enriquecer la democracia. La importancia del acceso a Internet para la democracia se ha puesto manifiesto en sentencias del Tribunal Europeo de Derechos Humanos, como, por ejemplo, Aldeniz y Altiparmak c. Turquía, donde se acreditan restricciones arbitrarias del acceso a redes sociales. Por esta y otras razones, se postula el reconocimiento del acceso a Internet como derecho humano.

Sin embargo, no se puede desconocer las prácticas de los operadores más relevantes contrarias a los valores democrático. Por su cotidianeidad, mediante "burbujas de filtro" los algoritmos personalizan el contenido de acuerdo con el historial de navegación y actividad, aislando al usuario de los contenidos que puedan contradecir sus puntos de vista, lo cual habitualmente lleva al empobrecimiento intelectual y a la conformación de opiniones considerablemente polarizadas en una dialéctica de amigos o enemigos, creando "cámaras de resonancias" de autoafirmación de las posturas ideológicas impenetrables a cualquier tipo de matiz.

Asimismo, se pueden citar, incidencias puntuales y singularmente graves en el correcto funcionamiento de la democracia como el caso de *Cambridge Analytica*, entre otros.

Finalmente, apuntar que los principales operadores tecnológicos constituyen un oligopolio global de dimensiones sin precedentes que se residencia fundamentalmente en los Estados Unidos. Recientemente se ha adoptado por el Tribunal General de la Unión Europea la

[2] Resolución Parlamento Europeo, de 12 de diciembre de 2023, sobre el diseño adictivo de los servicios en línea y la protección del consumidor en el mercado único de la Unión (2023/2043(INI)). Asimismo, AEPD, "Patrones adictivos en el tratamiento de datos personales. Implicaciones para la protección de datos", julio 2024.

[3] Recientemente se ha publicado la Comunicación de la Comisión - Directrices sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28, apartado 4, del Reglamento (UE) 2022/2065 (DOUE núm. 5519, de 10 de octubre de 2025). Se debería afrontar la cuestión con la mayor sinergia institucional para lograr el mayor impacto.

sentencia 3 septiembre de 2025, Latombe vs Comisión (T-553/23) por la que se desestima el recurso interpuesto frente a la Decisión de Ejecución de la Comisión, de 10 de julio de 2023, mediante la que se constata un nivel de protección adecuado de los datos personales garantizado por los Estados Unidos. Tras la realización por los Estados Unidos en 2022 de una serie de reformas institucionales, la Comisión consideró mediante la decisión que se impugnó que garantizaba un nivel de protección de las libertades y de los derechos fundamentales sustancialmente equivalentes al garantizado por el derecho de la Unión Europea. Sin embargo, ha de tomarse buena nota de que se han desarrollado acontecimientos que pudieran ir en una dirección contraria y muy preocupante para la protección de los derechos fundamentales.

2. Métodos interpretativos con los que se debería afrontar la redacción de las directrices

La Unión Europea y los Estados miembros configuran un sistema constitucional multinivel. El artículo 8 de la Carta de derechos fundamentales de la Unión Europea prevé el derecho fundamental a la protección de datos. En consecuencia, debe adoptarse los criterios propios y específicos de interpretación del derecho constitucional y de los derechos fundamentales.

En coherencia con lo anterior, no parece del todo afortunada la referencia en el párrafo noveno, al final, al igual valor jerárquico de la Ley de Servicios Digitales y el RGPD, pues aun siendo cierto no pondera lo suficiente que, sin embargo, el derecho a la protección de datos es un derecho fundamental y que constituye derecho originario de la Unión Europea.

Este párrafo, sin embargo, parece matizado con lo que se declara en el número 11, donde se determina que la interpretación uniforme y coherente no debe llevar a una reducción del nivel de protección de los derechos fundamentales a la privacidad y la protección de datos. Sin embargo, este último párrafo no acaba de situar las categorías conceptuales en su lugar. Pues los derechos fundamentales han de ser interpretados en la forma más adecuada para la viabilidad de la optimización de sus mandatos de protección, lo cual se incardina perfectamente con el artículo 54 de la Carta de Derechos Fundamentales de la Unión Europea y el pluralismo constitucional que caracteriza al sistema. Que este derecho deba ser ponderado junto con otros no supone que deba ser rebajado a una categoría jurídica inferior a la de su posición como derecho fundamental.

Y en este sentido es donde alcanza sentido traer aquí a colación anteriormente el estado de la cuestión que refleja el informe de la UNESCO y demás elementos relativos a las prácticas en los mercados digitales. En consecuencia, no se puede efectuar una interpretación de los preceptos puramente en abstracto y carente de su basamento fundamental, máxime a la vista

de un derecho que, excesivamente ponderado por las dinámicas del mercado, ofrece actualmente una protección jurídica singularmente debilitada.

3. Protección de datos desde el diseño y por defecto*: las personas como núcleo de la transformación digital de la Unión Europea*

a) Protección de datos desde el diseño.

De conformidad con el artículo 2 del Tratado de la Unión Europea, la Unión es una «unión de valores» que se fundamenta en el respeto de la dignidad humana, la libertad, la democracia, la igualdad, el Estado de Derecho y el respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías. Además, de acuerdo con el artículo 1 de la Carta de los Derechos Fundamentales de la Unión Europea, la dignidad humana es inviolable. Será respetada y protegida.

En coherencia, con el sistema de democracia constitucional multinivel el Capítulo I de la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital, bajo la rúbrica "Una transformación digital centrada en las personas", presenta el siguiente tenor literal:

> *1. Las personas constituyen el núcleo de la transformación digital de la Unión Europea. La tecnología debe servir y beneficiar a todas las personas que viven en la UE y empoderarlas para que cumplan sus aspiraciones, en total seguridad y respetando plenamente sus derechos fundamentales. Nos comprometemos a:*
>
> *a) fortalecer el marco democrático para una transformación digital que beneficie a todas las personas y mejore las vidas de todas las personas que viven en la UE;*
>
> *b) adoptar las medidas necesarias para que los valores de la UE y los derechos de los ciudadanos reconocidos por el Derecho de la Unión se respeten tanto en línea como fuera de línea;*
>
> *c) fomentar y garantizar una acción responsable y diligente por parte de todos los agentes digitales, públicos y privados, en el entorno digital;*
>
> *d) promover activamente esta visión de la transformación digital, también en nuestras relaciones internacionales.*

De acuerdo con el contenido esencial del derecho a la protección de datos, el artículo 25 RGPD regula los elementos rectores del principio de privacidad desde el diseño y por defecto.

Con un carácter proactivo y preventivo se incorpora el mandato jurídico de optimizar la protección de datos desde las primeras fases del desarrollo informático y durante todo el ciclo de vida del proceso de prestación de servicios.

Entre los principios que se integran en el proceso de protección de datos desde el diseño se encuentra el nuclear de ***"respeto por la privacidad de los usuarios: mantener un enfoque centrado en el usuario"***. De acuerdo la "Guía de Privacidad desde el Diseño" de la Agencia Española de Protección de Datos:

> "Sin obviar los intereses legítimos que persigue la organización con el tratamiento de datos que realiza, el fin último debe ser garantizar los derechos y libertades de los usuarios cuyos datos son objeto de tratamiento, por lo que cualquier medida adoptada debe ir encaminada a garantizar su privacidad. Ello supone diseñar procesos, aplicaciones, productos y servicios "con el usuario en mente", anticipándose a sus necesidades"[4]

A partir de esta premisa, es cuando se puede proyectar el principio de equilibrio de intereses "todos ganan", esto es, minimizar riesgos y maximizar los beneficios mutuos. En otro caso, un defecto de ponderación del ámbito de protección del derecho fundamental es reducirlo a una retórica meramente retórica y burocrática. En otro caso, el equilibrio simplemente es satisfactorio para optimizar el beneficio empresarial.

Las directrices deberían incorporar un capítulo muy destacado sobre la implementación de la protección de datos desde el diseño y durante todo el ciclo de la vida del tratamiento de datos. Por otra parte, a la hora de abordar las directrices proyectadas en su apartado 2.3 "Patrones de diseño engañosos", de acuerdo con el artículo 25 de la Ley de Servicios Digitales, llama la atención que no se ponga en relación con el artículo 25 RGPD, pues de las sinergias de ambos preceptos, donde se tomen en serio los derechos fundamentales – en expresión de Ronald Dworkin- es donde se puede alcanzar un estándar de equilibrio que pueda ser constitucionalmente aceptable.

[4] AEPD, "Guía de Privacidad desde el Diseño", 2019p. 10

b) Protección de datos por defecto

La protección de datos por defecto permite a las personas la utilización del servicio con el menor tratamiento de datos técnicamente viable y, en todo caso, con garantía de sus derechos y libertades fundamentales.

De conformidad con este principio, la funcionalidad por defecto más restrictiva en el tratamiento de datos es la funcionalidad inicial que debe estar disponible sin necesidad de efectuar ningún cambio de configuración por el usuario. Sin embargo, si las opciones de uso se ofrecen como se determina en el párrafo 87, en el primer uso del servicio, el sistema no está configurado por defecto para su utilización, sino que, desde el inicio, simplemente se da la opción de diferentes parámetros de tratamiento de datos, lo cual es bien distinto.

A mayor abundamiento, el ofrecimiento de umbrales menos estrictos de protección en el primer uso abona el empleo de "patronos oscuros", pues se confunde ese proceso con la introducción de datos que puedan ser imprescindibles para comenzar a utilizar el servicio, lo cual no parece lo más aconsejable para que el consentimiento se pueda emitir válidamente.

4. Elaboración de perfiles: las "burbujas de filtro"

En relación con la elaboración de perfiles y la cuestión del consentimiento, y habida cuenta de los datos de la experiencia, se considera que se debería efectuar un énfasis mucho más intenso sobre los términos de prestación del consentimiento.

Como se afirma en la Sentencia del Tribunal Supremo de España, Sala de lo Civil, núm. 1111/2025, de 10 de julio (ECLI:ES:TS:2025:3613), en relación con el derecho fundamental a la propia imagen en el entorno de las redes sociales:

> "La autorización para el uso de la imagen contenida en las «condiciones de servicio» que necesariamente deben aceptar los usuarios para poder utilizar una red social, por sus características (lenguaje de difícil comprensión, «maraña de cláusulas contractuales contenidas en un prolijo y extenso documento alojadas en lugares del sitio web de difícil acceso para el usuario», activación por defecto del mayor grado de publicidad), difícilmente puede considerarse como un consentimiento basado en información fiable".

El consentimiento en las redes sociales debe revestir las características previstas en el artículo 7 RGPD y en la legislación de protección de consumidores de la Unión Europea. Debiendo realizarse un escrutinio estricto de las fórmulas utilizadas por las plataformas.

Por razón de las "burbujas de filtro" producen efectos no solo individuales, sino que afecta a la colectividad, al correcto desarrollo de las sociedades democráticas, las directrices deberían incluir un apartado que se refiera a esta problemática.

Estas burbujas se producen a través del perfilado de los usuarios y, concretamente, mediante la utilización de categorías especiales de datos como pueden ser lo relativos a las opiniones políticas, las convicciones religiosas o filosóficas -artículo 9 RGPD-. Sin perjuicio, de la cuestión central de la prestación del consentimiento para el tratamiento de estos datos, se suscitan otras cuestiones complejas.

De acuerdo con el artículo 5.1 a) RGPD: "Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)". "La lealtad es un principio general que exige que los datos personales no se procesen de una manera que sea perjudicial, discriminatoria, inesperada o engañosa para el titular de los datos"[5]

Habría que cuestionar si la programación algorítmica para producir el efecto de burbujas de filtro es contraria a esos principios en la medida que de acuerdo con la evidencia científica producen o pueden producir potencialmente unos daños que, efectivamente, no son informados.

De acuerdo con la información publicada en el *Wall Street Journal*, Facebook realizó un estudio para analizar la viabilidad de programar los algoritmos de manera que no se fomentara la radicalización del espacio público. Se comprobó que técnicamente era posible, sin embargo, no se implementó la nueva programación, pues supondría una pérdida de ingresos económicos[6]. Hay que traer aquí a colación el modelo de la "economía de la atención" y los patronos engaños, pues de lo que se trata es de que los usuarios estén conectado el máximo tiempo posible para maximizar los ingresos con independencia de cuáles sean medios. Asimismo, la idea de tomarse en serio los derechos fundamentales, lo cual, en este caso, supone la evaluación de riesgos y su prevención desde el diseño y durante todo el ciclo de vida del tratamiento teniendo a la persona, a su dignidad, en el centro.

Fdo Jorge Andrada Barquero.

Abogado. ICAC 1897.

Firmado por JORGE ANDRADA BARQUERO (SW) el día 30/10/2025
con un certificado emitido por ACA 1

[5] Directrices del CEPD 3/2022, citada en la nota al pie 76 del proyecto de directrices.
[6] BALAGUER CALLEJÓN, Francisco, "La Constitución del Algoritmo", Fundación Manuel Giménez Abad, Zaragoza, 2023, 2ª Ed, p, 58, nota al pie 53.