



Liderar  
Defender  
Impulsar  
Promover



**Digitalización, Innovación,  
Comercio e Infraestructuras**

# **Comentarios sobre la propuesta de Carta de Derechos Digitales**

## **COMENTARIOS GENERALES A LA CONSULTA PÚBLICA PARA LA ELABORACIÓN DE UNA CARTA DE DERECHOS DIGITALES.**

Esta Carta de Derechos Digitales es un instrumento que, si bien parece destinado a establecer un conjunto de principios y derechos que inspiren las futuras leyes y reglamentos españoles, se considera que, en la práctica, excede tal objetivo. La Carta de Derechos Digitales (en adelante la Carta) establece un conjunto de normas que, bien por estar redactadas en un lenguaje y forma de requisitos obligatorios, o bien por reelaborar derechos ya existentes y en vigor en España y en la Unión Europea, pueden crear conflictos legales y generar un entorno jurídico inseguro y confuso para la innovación.

Muchos de los derechos establecidos en la Carta se solapan con derechos preexistentes en España, que tienen su propio contexto y ecosistema jurídico, y que son ignorados. Además, la Carta incluye disposiciones que se refieren a temas que actualmente se están debatiendo y considerando activamente para su regulación a nivel europeo; por lo tanto, también podría introducir más incertidumbre y ser perjudicial para la futura armonización.

Aunque la Carta está redactada en un lenguaje obligatorio, sigue sin estar clara la cuestión de si alguno de esos derechos es exigible. La exigibilidad de muchos de estos derechos estaría ciertamente abierta a discusión, considerando que dicha exigibilidad entraría en contradicción con las leyes existentes (como las contenidas en el Reglamento (UE) 2016/679 679, 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 (en adelante, "Reglamento General de Protección de Datos" o "RGPD") y los procedimientos (como la ventanilla única establecida en el Artículo 60 RGPD).

## COMENTARIOS DETALLADOS SOBRE LA CARTA Y SU CONTENIDO:

El establecimiento de un catálogo de derechos digitales a través de esta Carta confunde y se superpone con otras regulaciones aplicables:

- En algunos casos, la inclusión de determinados derechos en este catálogo es innecesaria, ya que tales derechos ya están consagrados en otras leyes relevantes, como el derecho a la igualdad, regulado en artículo 14 de la Constitución Española o el derecho a la protección de datos, regulado en la Constitución Española como derecho fundamental, en el Convenio 108, en el Reglamento General de Protección de Datos y la Ley 3/2018, de 5 de diciembre, de Protección de Datos y Garantías de los Derechos Digitales ("en adelante Ley 3/2018 o LOPDGDD"), así como el artículo 18, apartado 4 de la Constitución Española y el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.
- En otros casos, la Carta contradice la legislación vigente, como en lo que respecta al uso de datos de geolocalización precisos, regulado por la normativa de telecomunicaciones; el "derecho" de sucesión, regulado en el Código Civil y en una disposición ya confusa de la Ley 3/2018, concretamente en su artículo 3; y el uso de perfiles o el uso de datos personales para la investigación científica, ya regulado en el RGPD.

Además, la Carta compromete la armonización de futuras leyes que se están debatiendo actualmente en el ámbito de la Unión Europea, como el uso de sistemas de Inteligencia Artificial (en adelante IA); contenidos personalizados y la aplicación de las neurotecnologías.

### El papel pasivo de los individuos

- Todos estos derechos se redactan unilateralmente; sin embargo, la efectividad de tales derechos requiere un papel activo por parte de los particulares. Por ejemplo, el derecho a la identidad nunca puede ser una realidad si los individuos mienten, el derecho a la seguridad no puede abordarse si los individuos no instalan actualizaciones de seguridad o comparten negligentemente sus contraseñas, la protección de los menores no puede abordarse sin la responsabilidad activa de los padres o tutores legales (por ejemplo, los padres que hacen caso omiso de las actividades de sus hijos cuando están en línea o los usuarios adultos que no tienen en cuenta que los menores podrían ser incluidos en los destinatarios de contenidos generados por los

usuarios inapropiados que generan y/o comparten). No se puede llevar a cabo una lucha eficaz contra el material de explotación infantil sin utilizar perfiles, sin geolocalización o con malos actores "autorizados" a utilizar seudónimos, etc. El texto actual de la Carta pasa por alto estas cuestiones críticas.

Además, la Carta se refiere a la ciudadanía digital como el estatus de "derechos y deberes" de una persona. Sin embargo, la Carta no menciona ni una sola obligación que deba esperarse de los individuos en relación con el respeto mutuo de los derechos y libertades fundamentales de los demás, el respeto de las medidas destinadas a proteger la seguridad digital, los deberes parentales en relación con la protección de los menores, el respeto de los derechos de propiedad intelectual e industrial y los secretos comerciales de los demás, etc.

#### Aplicación y principio de ventanilla única

- No está claro contra quién pueden ejercerse estos derechos o quién debe defenderlos o hacerlos valer. Esto es particularmente peligroso, ya que los derechos están enmarcados de manera absoluta e ilimitada. La aplicación de la mayoría de estos derechos coexistirá y puede entrar en conflicto con la aplicación de los derechos de protección de datos y otros derechos fundamentales, creando conflictos legales y jurisdiccionales. Uno de los principales impulsores del proceso de reforma de la protección de datos en Europa fue el deseo de lograr una mayor claridad y coherencia tanto de la reglamentación como de la aplicación de la protección de datos en toda Europa; por este motivo, el RGPD establece normas de ventanilla única. Estas normas no son respetadas por la presente Carta (véanse nuestros comentarios sobre el artículo XXV).

## COMENTARIOS SOBRE EL ARTICULADO

### 1. Punto I. Derechos y libertades en el entorno digital (en relación también con el punto XV Derecho a la educación digital).

Entre los principios que deben guiar los procesos de transformación digital y el uso de la tecnología digital, así como la educación digital, cabe mencionar: i) las libertades fundamentales (y no sólo los derechos fundamentales); y ii) la necesidad de abordar un equilibrio adecuado entre los derechos y las libertades fundamentales, que requerirá una necesaria ponderación (ya que ningún derecho o libertad fundamental es absoluto y algunos de ellos pueden entrar en conflicto, como sucede a menudo en el mundo off line).

### 2. Punto II. Derecho a la protección de datos

El derecho a la protección de datos es un derecho fundamental regulado en la Constitución Española, en su artículo 18, apartado 4, en el Reglamento General de Protección de Datos (directamente aplicable en España desde el 25 de mayo de 2018) y en la Ley 3/2018 que ya incluye la regulación de los "derechos digitales". Por lo tanto, es innecesario y confuso regular otra vez un derecho de protección de datos. Si se considera oportuno incluir este derecho en la Carta, sería conveniente limitarse a confirmar que los derechos de protección de datos deben ser respetados en el contexto de los entornos digitales, pero siempre de acuerdo con la regulación actual de dichos derechos de protección de datos.

En lo que respecta al apartado 2, para ser coherente con el RGPD, el consentimiento no debería presentarse como la base legitimadora para el tratamiento de los datos personales establecidos en la ley. El RGPD, en su artículo 6 establece una serie de bases jurídicas para el tratamiento de los datos personales sin ningún orden de jerarquía entre ellas. Al referirse explícitamente de forma prevalente al "consentimiento" en el párrafo 2, este artículo sugiere que el "consentimiento" es la única base legitimadora, por tanto, sería necesario incluir las otras bases legitimadoras reguladas en el RGPD para tratar datos personales.

En este sentido se propone la siguiente redacción alternativa:

*1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada **cualquiera de las bases legitimadoras reguladas en el artículo 6 del Reglamento General de Protección de Datos** o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a ~~acceder a los datos recogidos que le conciernen y a obtener su rectificación~~ **ejercitar sus derechos sobre sus datos personales, de conformidad con lo dispuesto en la normativa de protección de datos.**
3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

Por último, este punto II reconoce expresamente los derechos de "acceso" y "rectificación"; sin embargo, la normativa de protección de datos regula una lista más extensa de derechos de protección de datos (todos ellos aplicables en entornos digitales). De nuevo, podría deducirse que la Carta considera que estos derechos de acceso y rectificación tienen mayor importancia que otros derechos, cuando no lo tienen en el derecho comunitario y español. Por ello, se propone que se realice la referencia completa de todos los derechos, de acuerdo con lo establecido en los artículos 15 a 22 del RGPD.

### 3. Punto III. Derecho a la identidad en el entorno digital

La redacción de este derecho resulta demasiado genérica y puede derivar e incluso fomentar un tratamiento diferente de la identidad en el plano digital y analógico.

Tampoco consideramos que debería permitirse como un derecho a disponer una identidad distinta en el plano digital, lo cual plantearía sus propios inconvenientes jurídicos e incluso a nivel de seguridad de la información.

En definitiva, se propone la eliminación de este apartado puesto que se considera innecesario articular derechos específicos sobre la identidad en este plano, cuando la identidad es algo que trasciende el plano digital y debe aplicar a cualquier contexto, sin generar rupturas innecesarias entre los planos analógico y digital.

#### **4. Punto IV. Derecho al pseudonimato**

La actual redacción de este derecho provoca incongruencias y dudas interpretativas.

En primer lugar, este derecho viene a generar problemas interpretativos con las medidas de salvaguarda en materia de pseudonimización previstas en la propia normativa de protección de datos, dado que una cosa es tener la posibilidad de utilizar un servicio en un entorno digital de forma pseudónima y otra distinta que el tratamiento de datos se realice de forma pseudónima.

En este sentido, sería conveniente matizar qué se entiende por pseudonimato. Asimismo, en caso de que la persona desee acceder a un servicio en condiciones de pseudonimidad, la carga de la pseudonimización de sus propios datos debería recaer en la persona y no suponer la implantación de procedimientos extra por parte del responsable del tratamiento / titular del servicio digital al que la persona quiere acceder de modo pseudonimizado.

En segundo lugar, este derecho también viene a generar incongruencias con otras normas, las cuales exigen una identificación directa de las personas (no sólo tener la posibilidad de reidentificar, tal y como se prevé en el apartado IV.2 de la Carta). La identidad real es indispensable para garantizar la aplicación de las cláusulas contractuales o las acciones legales contra las personas que cometen infracciones contractuales y/o legales, incluidos los delitos civiles y penales y los comportamientos perjudiciales. Entre estas normas se incluye la de prevención del blanqueo de capitales, la ley de conservación de datos (la cual exige a los operadores de telecomunicaciones llevar un libro registro para clientes prepago) e incluso, la propia normativa de protección de datos exige a los responsables del tratamiento actuar y poder demostrar una diligencia debida, de conformidad con el principio de responsabilidad proactiva, en diversos ámbitos que pueden impactar a este derecho (medidas de seguridad en mecanismos de autenticación, calidad y exactitud de los datos, carga de la prueba a la hora de demostrar la obtención del consentimiento, identificación expresa para el ejercicio de derechos, etc.)

Es más, son múltiples las sanciones de las autoridades de protección de datos en donde se ha considerado la realización de un tratamiento ilícito de protección de datos porque el responsable no ha sido lo suficientemente diligente a la hora de identificar al interesado.

En tercer lugar, este derecho viene a generar incluso otras incongruencias con otros derechos previstos en la propia Carta, como es el derecho a la libertad

de empresa en el ámbito digital, ya que el punto IV.1 de la Carta preestablece cómo las empresas deben configurar sus servicios en el entorno digital para permitir un acceso pseudónimo a los mismos, suponiendo, en todo caso una carga adicional para los responsables del tratamiento / titulares del servicio digital, al suponer “duplicar” sistemas para permitir acceder el acceso identificado / pseudónimo.

Es decir, este derecho presume que el uso pseudónimo debe ser la opción por defecto y condena, en cierto modo, el uso habitual en condiciones de identificación directa, todo ello de forma innecesaria, condicionando la libertad de empresa sin basarse en una norma y generando múltiples problemas interpretativos a nivel jurídico.

No obstante, la realidad jurídica es que el uso de servicios digitales mediante identificación directa es legal, recomendable e incluso exigida por la normativa en algunos casos, aspectos que hacen innecesario determinar un derecho al pseudonimato en el plano digital. Por ejemplo, determinados servicios que requieren identificación (formalización de contratos, suscripción de servicios, etc.) no podrían estar disponibles para su formalización de modo pseudonimizado (inseguridad jurídica en relación con la parte contratante).

La promoción de una identidad digital anonimizada o pseudonimizada puede también generar mayores riesgos en las interacciones en redes sociales, fake news o desinformación, etc.

Finalmente, la promoción de una identidad digital anonimizada o pseudonimizada, supone riesgos de Seguridad informática en la forma de introducción de información falsa o sesgada dentro de los sistemas informacionales de una compañía, efecto conocido como “*poisoning data*”, con el fin de sesgar resultados, alterar algoritmos con fines perversos y en contra de determinados colectivos de la población.

En conclusión, todo lo anterior hace necesario resolver las incongruencias y dudas interpretativas generadas por la redacción de este derecho.

## **5. Punto V. Derecho a no ser localizado y perfilado**

En primer lugar, se ha de indicar que la localización y la elaboración de perfiles son conceptos no relacionados entre sí que no deben abordarse conjuntamente.



**Localización.** Es preciso definir el término datos de localización, ya que puede referirse a diferentes niveles de precisión. Teniendo en cuenta el título de este artículo V ("el derecho a no ser localizado"), se podría pensar que sólo se aplica a la geolocalización precisa de un dispositivo. En tal caso, este tipo de datos de geolocalización ya están regulados en la normativa de telecomunicaciones y de privacidad electrónica, en la que no se impone una prohibición de su uso, sino que somete su uso a condiciones específicas que esta Carta no contempla. Además, la nueva Ley General de Telecomunicaciones española (que regula el uso de estos datos) está actualmente en discusión.

**Perfiles.** El propio término es subjetivo y se entiende que significa cosas diferentes para públicos diferentes. Algunos utilizan el término para referirse a la personalización de cualquier producto, mientras que otros pueden utilizarlo para referirse más específicamente al *targeting* de la publicidad online. También algunos utilizan el término para referirse a una segmentación que va más allá de la edad, el sexo y la ubicación y se centra en elementos de la personalidad de un individuo y otros se refieren a cualquier tipo de segmentación. En este sentido, es importante aclarar que, a efectos de normativa de protección de datos, la diferencia entre perfilado y segmentación es importante. Segmentar puede implicar solo agrupar clientes según características, mientras que perfilar habitualmente implica un tratamiento más intensivo de los datos. Los requisitos / exigencias normativas para realizar una u otra actividad son distintos. Y también los efectos jurídicos que el tratamiento basado en una u otra podría provocar.

Dicho lo anterior, se considera que este es un derecho que, tal y como está redactado, viene a modificar y extender injustificadamente la regulación ya prevista en la normativa, en concreto en la normativa de protección de datos. Esto hace que sea especialmente alarmante, ya que afecta directamente a la capacidad de desarrollo en planos tan estratégicos como el de la IA o el Big Data, tecnologías vertebradoras de la industria digital.

Este derecho viene a considerar la localización y la elaboración de perfiles como un límite a la autodeterminación individual y la garantía de libertades. Se trata, por lo tanto, de una presunción injustificada y que no tiene ninguna base jurídica ni tecnológica.

A este respecto, es preciso indicar que la localización y la elaboración de perfiles no son otra cosa más que operaciones del tratamiento de datos y que no son una finalidad del tratamiento en sí misma. Por ello, se presupone injustificadamente un riesgo sin atender a la finalidad para la que se utilicen dichos datos. Además, se debe tener en consideración que, por ejemplo, la localización puede ser necesaria para atender servicios solicitados por el titular de los datos. Pej., servicios de Maps / cartografía, servicios de apertura a distancia de puertas u otros objetos (car sharing, bici sharing, etc.)

Es más, bien podría ocurrir no sólo que estas operaciones del tratamiento no sean un límite a la autodeterminación individual y a la garantía de libertades, sino que el uso de estas técnicas sirvan y apoyen su materialización práctica.

Por lo tanto, hay múltiples ejemplos donde estas técnicas son inocuas o positivas para la ciudadanía, motivo por el cual no se puede presumir su impacto negativo, al ser un elemento más del tratamiento y no un fin en sí mismas.

En segundo lugar, el punto V.2 de la Carta, parece exigir que estas técnicas sólo puedan realizarse bien con el consentimiento de la persona o por una obligación legal; ello, de nuevo, sin tener en cuenta la finalidad del tratamiento. Esto es especialmente problemático, puesto que existen múltiples ejemplos donde el uso de estas técnicas está justificado, sin que sea necesario para cumplir una obligación legal y donde tampoco sea necesario contar con el consentimiento del interesado. Se trata de tratamientos de datos como, por ejemplo, con fines de seguridad y ciberseguridad, mejora de calidad de servicio, detección y prevención de fraude y blanqueo de capitales, detección y prevención de incidencias, etc. También existen tratamientos de datos basados en estas tecnologías que son necesarias para la ejecución de un contrato (p.ej. un recomendador de contenidos), sin que sea necesario contar con el consentimiento o basarse en una obligación legal; todo ello, además, sin suponer un incumplimiento de la normativa.

No puede establecerse el consentimiento como única base legitimadora de los tratamientos de datos personales pues, tal y como indican las autoridades de protección de datos, el consentimiento no es más que una base legitimadora más, siendo lo importante el principio de la licitud del tratamiento, es decir, la concurrencia de cualquiera de las bases

legitimadoras reguladas en la normativa de protección de datos, sin que exista prevalencia entre ellas.

Esto hace que la redacción actual de este derecho establezca limitaciones no previstas en la normativa actual que ya regula estas tecnologías (RGPD y LOPDGDD, la futura regulación de ePrivacy, LSSI y Ley General de Telecomunicaciones, etc.) e, incluso, incompatibles con la interpretación de las autoridades de protección de datos encargadas de interpretar dichas normas.

La prohibición de los perfiles también es contradictoria con el punto XIII, que establece el derecho a ser informado de la elaboración de perfiles.

**Fines estadísticos.** El derecho a la gestión de los datos personales para usos estadísticos ya está contemplado ampliamente contemplado en el reglamento actual vigente de protección de datos. En el caso de fines estadísticos, ya se separan conceptos de datos, datos identificativos y datos puramente métricos y referentes al producto asociado al cliente. Ya existe una gestión diferenciada de los datos en función de su naturaleza, y si bien el dato identificativo es importante en términos de seguridad y amparo jurídico, el dato estadístico se puede separar del dato identificativo, dados los órganos de gobierno de datos de la empresa y los procesos de auditoria, y los procesos de supervisión de los reguladores, otorgan la suficiente seguridad del correcto uso de los datos, sin vulnerar los derechos establecidos de privacidad, y al mismo tiempo, otorgando las mejoras que se derivan del uso correcto de los datos con un fin lícito de mejora y atención del cliente.

En conclusión, se considera necesaria la eliminación de punto V debido a las incongruencias identificadas con las normativas que actualmente ya regulan el uso de estas tecnologías, las cuales no prevén las limitaciones incorporadas en la Carta.

## **6. Punto VI. Derecho a la seguridad digital**

El propósito de incluir este artículo no está claro, ya que está formulado de manera tan absoluta que nadie podría garantizarlo o incluso definirlo, suponiendo, en cualquier caso, una carga excesiva para el titular del servicio de la sociedad de la información, a quien se le puede exigir la implementación

de todas las medidas técnicas y organizativas a su alcance para garantizar la seguridad digital, pero no la seguridad digital “absoluta.

Además, como se ha anticipado en las observaciones generales, la seguridad digital requiere la colaboración de todas las partes interesadas, incluidas las personas que reclaman dicha seguridad. Por ejemplo, las personas deben mantener la confidencialidad de sus contraseñas, utilizar contraseñas seguras, evitar el uso de la misma contraseña en varios dispositivos, instalar actualizaciones de seguridad de software, no abusar de las medidas de seguridad aplicadas, informar de patrones inusuales (si ve algo, diga algo), leer las políticas de privacidad y de cookies, etc. Este artículo debería reconocer la importancia del papel de los particulares en el mantenimiento de la seguridad digital.

## **7. Punto VII. Derecho a la herencia digital**

Sobre el contenido de este apartado, se considera necesario clarificar a qué se está refiriendo exactamente al hablar de “herencia digital”. No queda claro si, por ejemplo, se trata de un perfil digital en una red social, de las fotos de la persona compartidas en esa red social o de las fotos almacenadas en la cloud.

Sin perjuicio de lo anterior, debe precisarse que el derecho a la herencia digital debe determinarse de acuerdo con las normas de herencia del Código Civil. La referencia a la Ley Española de Protección de Datos en este artículo es particularmente poco útil teniendo en cuenta que los artículos 3 y 96 de la Ley 3/2018 son particularmente confusas y a veces contradictorios con el Código Civil. La redacción del derecho a la herencia digital como mera remisión al Código Civil y a la Ley española de Protección de Datos, en lugar de proporcionar orientación y claridad, sirve para crear un marco legal más confuso y no servirá de forma efectiva para orientar futuras regulaciones.

Esta disposición tampoco es coherente con las leyes europeas sobre privacidad. De conformidad con el Considerando 27 del RGPD, el Reglamento General de Protección de Datos no se aplica a la protección de datos personales de las personas fallecidas. Aunque si bien es cierto, habilita a los Estados miembros con competencias para establecer normas relativas al tratamiento de los datos personales de estas.

## **8. Punto VIII. Derecho a la igualdad y a la no discriminación en el entorno digital**

El impacto de este derecho es algo vago. No está claro si el derecho tiene por objeto crear obligaciones específicas por parte del entorno digital. Debería aclararse si se espera que un entorno digital adopte todas las políticas relativas a las cuestiones de igualdad que son apoyadas por las autoridades públicas y si hay otras acciones proactivas que los entornos digitales están obligados a tomar en virtud de este artículo.

Entrando en el detalle del contenido de este punto VIII, en el apartado 1, se indica que *“Se reconoce el derecho a la igualdad en los entornos digitales, la no discriminación y la no exclusión. En particular, se reconoce el derecho a la igualdad efectiva de mujeres y hombres en entornos digitales. Los procesos de transformación digital aplicarán la perspectiva de género”*. Sin embargo, no especifica qué se entiende por perspectiva de género ni cómo se aplicaría la perspectiva de género en los procesos de transformación digital, aspectos que resultaría necesario concretar y tratar con la profundidad requerida.

## **9. Punto IX. Protección de menores en el entorno digital**

La misma problemática y preocupaciones indicadas para el derecho a no ser localizado y perfilado son, si cabe, más relevantes en este derecho. En línea con lo indicado anteriormente, este derecho establece limitaciones no previstas en la normativa que actualmente ya regula la protección de los menores en el entorno digital y, concretamente, al tratamiento de sus datos personales en lo que a la elaboración de perfiles respecta.

La normativa de protección de datos no prohíbe la elaboración de perfiles de menores y también permite que los mayores de 14 años, pese a ser menores de edad, tengan control sobre sus propios derechos de protección de datos, de acuerdo con el artículo 7 de la Ley 3/2018.

Todos estos aspectos son obviados en la Carta, la cual prohíbe injustificadamente el perfilado de menores, salvo en los casos en que sea requerido por la ley. Es decir, obvia que los menores de edad, que sean mayores de 14 años, pueden, de hecho, consentir la elaboración de perfiles y que existen múltiples casos más allá del cumplimiento de la obligación legal donde la elaboración de dichos perfiles puede tener lugar de forma legal y justificada.

La disposición adicional decimonovena de la Ley 3/2018 establece un mandato al Gobierno para que remita al Congreso de los Diputados, en el plazo de un año desde la entrada en vigor de dicha Ley, un Proyecto de Ley dirigido específicamente a garantizar los derechos de los menores ante el impacto de Internet, con el fin de garantizar su seguridad y luchar contra la discriminación y la violencia que sobre los mismos es ejercida mediante las nuevas tecnologías.

Por otro lado, si la intención de este punto IX era referirse a la publicidad (incluida la elaboración de perfiles), se trata de una actividad legítima llevada a cabo por el sector privado, así como por los organismos gubernamentales y las Administraciones Públicas. El uso de los verbos "manipular" o "perturbar" en el artículo IX es inapropiado en este contexto, ya que demoniza indebidamente toda actividad publicitaria. La actividad publicitaria tiene su propia legislación específica (Ley 34/1988, de 11 de noviembre, General de Publicidad), así como Códigos de Conducta de los que el sector publicitario se ha dotado mediante el mecanismo de autorregulación para garantizar la licitud y adecuación de la publicidad con carácter general, así como de la publicidad específicamente dirigida a menores de edad. Además, existen disposiciones específicas sobre la actividad publicitaria y la propia publicidad incluidas en la normativa de consumo, protección de datos, comercio electrónico y telecomunicaciones, así como en otras normativas de actividad sectorial. Consideramos que esta Carta no es el instrumento adecuado para determinar los límites de la actividad publicitaria, y desde luego no puede ser contradictoria con otras normativas aplicables.

La prohibición de los anuncios personalizados sería también una interferencia inaceptable con la libertad fundamental de establecimiento de una empresa. En cambio, el interés superior del niño es el principio fundamental que debe guiar toda actividad privada y pública dirigida a él, incluida la publicidad. De lo contrario, se correría el riesgo de que los niños se vieran expuestos a anuncios no personalizados, lo que podría dar lugar a que vieran contenidos absolutamente inapropiados para su edad y madurez.

Además, este artículo hace caso omiso de la Carta de las Naciones Unidas sobre los Derechos del Niño (Declaración Universal de los Derechos del Niño), que exige que se establezca un equilibrio entre los diferentes derechos y libertades de los niños y que se tenga en cuenta su evolución hasta que se

conviertan en adultos, incluidos sus derechos a la intimidad, el derecho a jugar, a ser educado, a estar seguro, etc.

Por último, en este artículo tampoco se aborda que es necesario un equilibrio entre la privacidad y la seguridad para abordar adecuadamente la seguridad digital de los menores, es decir, la forma en que el sector privado y la Administración Pública pueden utilizar la tecnología para detectar y prevenir comportamientos y/o contenidos perjudiciales o ilegales contra los niños.

En conclusión, se hace necesario respetar los principios rectores de las normativas que actualmente ya regulan el uso de estas tecnologías, las cuales no prevén las limitaciones incorporadas en la Carta.

## **10. Punto X. Protección de personas con discapacidad en el entorno digital**

El impacto de este derecho es vago. Como concepto general, la discapacidad es un concepto muy amplio; la Carta impone una obligación general de proporcionar información jurídica accesible y comprensible; sin embargo, deben proporcionarse muchos más pormenores en cuanto a los detalles de esta obligación (por ejemplo, siguiendo criterios como los incluidos en la disposición adicional quinta de la LSSI (Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico) relativa a la accesibilidad para las personas con discapacidad y de edad avanzada a la información proporcionada por medios electrónicos).

## **11. Punto XII. Derecho a la neutralidad de Internet**

La obligación de no discriminación del Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 por el que se establecen medidas en relación con el acceso a una internet abierta se refiere únicamente a los proveedores de servicios de acceso a Internet. Sin embargo, para garantizar el acceso sin discriminación a los servicios de internet parece razonable que los poderes públicos extiendan esta obligación a otros agentes que también mantengan una relación directa con el usuario y ofrezcan a los consumidores servicios de internet.



En este sentido, se propone la siguiente redacción alternativa:

~~Los poderes públicos garantizarán el derecho de los usuarios a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos, en los términos previstos en el Reglamento (UE) 2015/2120 de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.~~ **El derecho a la neutralidad de Internet debe abarcar a todos los agentes de la cadena de valor que mantengan una relación directa con los ciudadanos. En este sentido, los poderes públicos garantizarán este derecho de los usuarios, a una oferta transparente de servicios sin discriminación por motivos técnicos o económicos, por parte de todos aquellos agentes que ofrezcan servicios al usuario final incluyendo aquellos que provean de los sistemas operativos, las tiendas de aplicaciones (AppStores) y los dispositivos móviles entre otros.**

## 12. Punto XIII. Libertad de Expresión y Libertad de Información

Sobre el contenido de este punto, se desea manifestar las siguientes observaciones:

- Se debería distinguir entre las responsabilidades de las personas (incluidas las personas físicas y las personas jurídicas como las empresas, etc.) que crean el contenido (y tienen una responsabilidad editorial al respecto) y las plataformas utilizadas por esas personas para comunicar o compartir dicho contenido (que pueden tener un papel en la forma en que se muestran esos contenidos, pero no tienen ningún papel en lo que respecta al contenido en sí). Por ejemplo, el derecho de rectificación (párrafo 2.d) puede y debe referirse únicamente a las personas/proveedores que crean, autorizan o publican el contenido por sí mismos. Es necesario distinguir entre las responsabilidades de las personas y las plataformas y, asimismo, la forma de responder en cada uno de los supuestos para garantizar los derechos de todas las personas, en el caso de que exista alguna diferencia al respecto. Definir en cada supuesto, las líneas generales a



seguir en cada caso, que se han de contener en los protocolos de actuación.

- Los proveedores de hospedaje no son autores ni editores y los derechos de rectificación como los del apartado d) del párrafo 2 deben dirigirse debidamente a los usuarios de las plataformas de hospedaje y no a los propios proveedores de las plataformas de hospedaje. Es preciso hacer mención de esta figura y su exención de responsabilidad en cuanto a esta cuestión para acotar la responsabilidad que ha de asumir cada responsable en estos supuestos.
- No debería imponerse a los proveedores de servicios intermediarios la obligación positiva de llevar o mostrar determinada información (por ejemplo, la idea de que se publique un contra aviso) cuando sea totalmente incompatible con la naturaleza y la función de un proveedor de hospedaje.
- La libertad de expresión es uno de los principios consagrados dentro de la Unión Europea, que comprende la libertad de opinión y la libertad de recibir o comunicar informaciones, respetando la libertad de los medios de comunicación y su pluralismo. En este sentido, los medios de comunicación son los mecanismos a través de los cuales se transmite información al público y cumplen, junto con los medios audiovisuales, con su objetivo principal de proveer contenidos para informar, entretener o educar al público en general y para lo que deben cumplir con ciertas salvaguardias. Adicionalmente, la evolución de internet y la proliferación de servicios en internet, ha dado lugar a la posibilidad de difundir dicha información de manera interpersonal (comunicaciones dentro de un contexto más privado, entre dos, tres o más personas, un ejemplo son los correos electrónicos, el teléfono, etc.). Por tanto, una cuestión es la información y su contenido (de la cual son responsables los autores de esta) y otra es el medio/canales a través de los cuales el contenido viaja y llega a su destinatario/os. No obstante, existen otros agentes que son meros "transitadores" que desconocen el contenido de la información y, por ello, no pueden garantizar derechos de cuyo contenido no son responsables. Esta distinción debería quedar clara a lo largo de todo el texto.
- La garantía de los derechos sobre un contenido sólo puede recaer en aquellos agentes que tienen un rol activo en la preparación, organización y difusión o puesta a disposición de los mismo. De nuevo, es preciso definir

con más precisión el rol de cada uno de los intervinientes en el proceso de transmisión de la información.

- Por último, tampoco se puede obviar la actual situación de relaciones en la cadena de valor de servicios digitales, más amplia respecto de los servicios tradicionales (telecomunicaciones, audiovisuales o de sociedad de la información), para conseguir de forma efectiva los objetivos que se propone en esta Carta, entre ellos la defensa de los derechos de los usuarios y una competencia sostenible.
- El Párrafo. 2 a) no es práctico. Si bien las empresas que operan en entornos digitales disponen de instrumentos para detectar contenidos creados sin intervención humana (por ejemplo, noticias falsas y "botposts") y hacen todo lo posible por detectar este tipo de contenidos, sería muy difícil que esas empresas pudieran confirmar de manera concluyente si los contenidos fueron creados por medios humanos o automatizados. Esta cuestión se debe eliminar ante la ausencia de desarrollo tecnológico al respecto por lo que su recogida en esta Carta es demasiado precoz, sin perjuicio de su regulación futura.
- En el apartado 2b se señala lo siguiente:

*2. Los responsables de medios de comunicación, así como los de los entornos digitales que o bien tengan por objeto el ejercicio de libertades del párrafo anterior por sus titulares o bien provean tal servicio a sus usuarios, adoptarán protocolos adecuados para garantizar los derechos de todas las personas a: (...)*

*b) A conocer cuándo una información ha sido clasificada o priorizada por el proveedor mediante técnicas de perfilado o equivalentes. (...)*

En este sentido, cabe indicar que los requisitos de información y transparencia no deben entenderse como "sobre información" que podría generar alarma y preocupación innecesaria en los ciudadanos. Toda obligación de transparencia es una buena noticia si está "enfocada hacia el individuo", y no "enfocada hacia la regulación".

- Por otra parte, el párrafo 2.c) de este punto XIII equivaldría a una exclusión voluntaria de cualquier tipo de perfil, ya que todas las ideas son susceptibles de "afectar" a la forma en que una persona piensa y cree (las

ideas científicas pueden dar explicaciones distintas de la religiosa a cuestiones concretas, los valores específicos o los debates en una sociedad pueden contradecir determinadas creencias religiosas, etc.). La libertad de creencias (incluidas las creencias religiosas) está directamente relacionada con la libertad de expresión y de información. Una vez más, la elaboración de perfiles ya está regulada en el RGPD y la Carta no tiene derecho a modificar sus disposiciones. Además, este apartado c) del párrafo 2 parece prohibir en absoluto a los "proveedores" el tratamiento de datos de categoría especial. Esto es mucho más restrictivo que lo establecido en el RGPD. Con arreglo al RGPD, si un responsable del tratamiento de datos tiene una base legitimadora para tratar los datos de categoría especial o, en el lenguaje del legislador español, «especialmente protegidos» (por ejemplo, el consentimiento explícito, los intereses vitales o la exención con fines de investigación, por nombrar algunos de ellos), se le debería permitir tratarlos. Sin perjuicio de la necesidad de regular esta cuestión con cierta cautela y dentro del margen de actuación otorgado a los Estados Miembros, se propone el mantenimiento de este apartado si bien como una posibilidad a valorar en cada caso concreto, es decir, sin carácter imperativo, lo que permitiría la aplicación de técnicas de análisis cuando concurra base legitimadora a tal efecto.

- El significado exacto de la primera frase del párrafo 3 no está claro. La redacción es ambigua y, en cualquier caso, la Carta no es el lugar adecuado para regular ningún procedimiento de eliminación de contenidos, en particular, si están vinculados a un comportamiento ilícito, que está sujeto a las disposiciones de la Directiva sobre el Comercio electrónico (Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior), entre otros instrumentos jurídicos por lo que su contenido excede de lo previsto en la normativa vigente. La segunda frase implica que existe un derecho de apelación si el contenido se retira por motivos legales. En tales casos, el derecho de apelación debe recaer en la persona o el organismo o en los tribunales. No es apropiado que los intermediarios estén mediando en disputas sobre la legalidad del contenido y no existe tal derecho, se recoge un exceso de competencias que en ningún caso resultan aplicables por lo que este extremo debe ser revisado de forma pormenorizada.

Es necesario, también aclarar más lo que significaría, en la práctica, la "prohibición de la censura previa". Muchas plataformas eliminan ciertos contenidos que son perjudiciales pero legales (por ejemplo, las imágenes sexuales) aplicando las directrices propias de la plataforma. Esas directrices son necesarias para garantizar que los usuarios de la plataforma, que suelen estar radicados en todo el mundo, apliquen y respeten un conjunto coherente de normas y comportamientos. Después de todo, lo que es legal en un país puede ser ilegal en otro. Este extremo es de relevante importancia puesto que pueden verse afectados colectivos vulnerables, como ocurre en el caso de los menores de edad respecto de los cuales ha de primar el interés superior del menor.

Con todo ello, se propone, sin perjuicio de lo expuesto anteriormente y de las modificaciones adicionales que pudieran ser necesarias como consecuencia de ello, la modificación de este punto XIII en la forma que sigue:

*1. Todos tienen derecho a las libertades de expresión e información en entornos digitales en los términos previstos por la Constitución. Se garantizarán los principios constitucionales relativos a la veracidad, el pluralismo informativo y la diversidad de opiniones e informaciones.*

*2. Los responsables de medios de comunicación, así como los de los entornos digitales que ~~o bien~~ tengan por objeto el ejercicio de libertades del párrafo anterior por sus titulares **mediante un rol activo en la organización y puesta a disposición de la información** ~~o bien provean tal servicio a sus usuarios~~, adoptarán protocolos adecuados para garantizar **la información y transparencia respecto a** los derechos de todas las personas a:*

- a) Conocer cuándo la información sea elaborada sin intervención humana mediante procesos automatizados.*
- b) ~~A conocer cuándo una información ha sido clasificada o priorizada por el proveedor mediante técnicas de perfilado o equivalentes.~~ Cuando esta información sea patrocinada por un tercero deberá informarse de modo específico sobre la naturaleza publicitaria de la misma.*
- c) A solicitar del prestador la no aplicación de técnicas de análisis que permitan ofrecer información que afecte a las libertades ideológica, religiosa, de pensamiento o creencias. **Esta solicitud se someterá a valoración atendiendo al caso en concreto.***
- d) A posibilitar el ejercicio del derecho rectificación ya sea frente a medios de comunicación, ya sea ante aquellos usuarios que*

*difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.*

*Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.*

- e) *A solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.*

*En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.*

3. Los procesos de verificación y retirada de contenidos se limitarán a aquellos que en entornos digitales se encuentran limitados por la prohibición de censura previa. En los supuestos en los que la ley ampare la retirada de un contenido, los prestadores **a los que hace referencia el apartado 2 del presente Título XIII** deberán notificarla al usuario y disponer de un procedimiento de reclamación de estas decisiones. Se impulsarán mecanismos de autorregulación transparentes que contemplen los criterios y los procedimientos que determinan en este ámbito la actuación de los prestadores e incorporen procedimientos de reclamación y revisión de las decisiones de retirada de contenidos.

### **13. Punto XIV. Derecho a la participación ciudadana por medios digitales**

No está claro qué se quiere decir cuando la disposición establece que se "promoverán" ciertos entornos digitales para contribuir a un derecho efectivo de acceso a la información pública, la transparencia, la

responsabilidad, ni tampoco está claro qué obligaciones, de haberlas, puede imponer este derecho a un entorno digital y si esas obligaciones serían compatibles con la función de los proveedores de hospedaje. Es decir, no se prevé cómo llevar a la práctica la participación por medios digitales para hacer efectivo este derecho. Por ello, se ha de materializar el mismo con una regulación más exhaustiva al respecto en la propia Carta para no generar un vacío legal que pueda desvirtualizar el derecho que se reconoce.

#### **14. Punto XVI. Derechos digitales de la ciudadanía en sus relaciones con las Administraciones públicas**

El apartado 4 de este punto XVI establece que *“siempre que sea posible se promoverá la universalidad y la neutralidad de las tecnologías usadas por las Administraciones públicas, así como su diseño y uso conforme a los principios éticos que acompañan a esta Carta.”*, añadiendo, a continuación, que *“Así mismo se adoptarán las medidas precisas para garantizar que la prestación de los proveedores de servicios que colaboren con ellos por medios digitales se realicen conforme a las disposiciones de esta Carta”*.

En este sentido, es preciso señalar que este último inciso, supone un conflicto con lo dispuesto en el punto II de esta Carta donde se establece que la base del tratamiento de datos personales es únicamente el consentimiento de la persona afectada. En concreto:

*II. 2. “Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación”.*

En consecuencia, y en línea con los comentarios señalados en el correspondiente apartado, sería necesario modificar el punto II.2 e indicar las bases legitimadoras reguladas en el artículo 6 del Reglamento General de Protección de Datos. Es decir, se ha de especificar que existen otras bases legitimadoras del tratamiento de datos personales en virtud del referido artículo y hacer mención de cada una de estas que puede resultar aplicable atendiendo al caso en concreto.

Por último, se propone la siguiente modificación sobre el último apartado de este punto XVI en la forma que sigue:

***Se recomienda*** ~~será necesario~~ *realizar una evaluación de impacto en los derechos digitales en el diseño de los algoritmos en el caso de adopción de decisiones automatizadas o semiautomatizadas. En todo caso, serán objeto de aprobación previa de los sistemas algorítmicos que se vayan a usar para la toma de decisiones, con determinación de su ámbito concreto de aplicación y estructura de funcionamiento.*

Se ha de prever la posibilidad de realizar una evaluación de impacto, pero no de forma imperativa, ya que la obligatoriedad de esta variará en cada supuesto en concreto por lo que no puede recogerse como una obligación a cumplir en todo caso, de conformidad con el artículo 35 del RGPD.

## **15. Punto XVII. Derechos en el ámbito laboral**

Respecto al contenido de este punto XVII, se desean realizar las siguientes observaciones:

En primer lugar, se debe indicar que las consideraciones sobre la desconexión digital, la intimidad en el uso de dispositivos digitales y en el uso de dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo se encuentran reguladas en los artículos 87 a 89 de la LOPDGDD, que establecen los derechos / obligaciones en ese sentido. Se estima que la Carta debería referirse a dicha normativa, ya que regula expresamente tales cuestiones.

Sin perjuicio de lo anterior, debe matizarse el apartado 1.b), donde se establece el derecho a la intimidad en el uso de dispositivos digitales puestos a su disposición por su empleador, así como frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, teniendo en consideración la jurisprudencia existente que reconoce la validez de la utilización de sistemas de geolocalización bajo las siguientes condiciones: (i) tiene que tener una clara finalidad empresarial encaminada a mejorar los servicios; (ii) debe ser comunicada a los empleados con carácter previo a su utilización/implementación (así como en su caso a la Representación Legal de los Trabajadores (RTL) y (iii) siempre se debe buscar el método menos intrusivo que pueda combinar el derecho a la intimidad de los trabajadores y el derecho del empresario



regulado en el artículo 20, apartado 3 del Estatuto de los Trabajadores: "El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad (...)". Se han de tener cuenta estas consideraciones y referenciarlas en la Carta para garantizar que este derecho se va a cumplir de forma efectiva para ambas partes.

Sobre el apartado 3.b), se debe señalar que la representación de los trabajadores ya tiene reconocidos una serie de derechos de información y consulta (artículos 64, 40, 41, 51 y siguientes, del Estatuto de los Trabajadores), entre lo que podríamos entender ya incluida su participación en cualquier cambio tecnológico o transformación digital relevantes que se pretendiesen introducir en la empresa y tuviesen consecuencias laborales.

La toma de decisiones iniciales sobre cualquier transformación que se pretenda introducir en la empresa debe quedar bajo el paraguas del poder de dirección del empresario y del derecho fundamental a la libertad de empresa (artículos 20 del Estatuto de los Trabajadores y 38 de la Constitución Española), todo ello sin perjuicio del derecho que ostenta la representación de los trabajadores de información y consulta en todas aquellas decisiones relevantes, y en especial aquellas que tuviesen consecuencias laborales.

Sobre el apartado 4, nuevamente se debe hacer alusión a los principios recogidos en el Estatuto de los Trabajadores, en este caso, en el artículo 64, Derechos de información y consulta y competencias. Asimismo, se llama la atención sobre la referencia que recoge al término de este apartado 4 (*"Este deber de información alcanzará como mínimo al conocimiento de los datos que se utilizan para alimentar los algoritmos, su lógica de funcionamiento y a la evaluación de los resultados"*), entendiendo necesaria su eliminación dado que esta obligación puede ser enormemente intrusiva para la empresa ya que puede afectar a secretos industriales, al *Know How* de la compañía o a procesos internos de la misma. Esta indicación excede del alcance del artículo 13 del RGPD y puede generar daños materiales a las empresas que implicarían un retroceso en el desarrollo del entorno digital. Incluso contraviene lo dispuesto en el punto 4.2 del Dictamen del Comité Económico y Social Europeo sobre



inteligencia artificial (dictamen iniciativa 2018/C 440/01) de 15 de febrero de 2018 donde se señalaba que la "transparencia algorítmica no consiste en revelar códigos".

Con todo ello, se propone la modificación de este punto XVII en la forma que sigue:

### ***Derechos en el ámbito laboral***

1. En el ámbito laboral **los/las** trabajadores/as y los empleados/as públicos/as tienen derecho a:

- a) La desconexión digital, **salvo situaciones de guardia y urgencia con carácter excepcional.**
- b) La protección de su intimidad en el uso de dispositivos digitales puestos a su disposición por su empleador/a, así como frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, **salvo que sea necesario por motivos de seguridad y así se informe mediante carteles que adviertan de la presencia de cámaras de videovigilancia. Procederá su aplicación siempre y cuando no exista un medio menos intrusivo en su privacidad, respetándose en todo caso el principio de proporcionalidad.**
- c) La intimidad ante la utilización de sistemas de geolocalización, **sin perjuicio de lo que pueda establecer la normativa laboral de aplicación.**

***En todo caso, se deberá estar a lo dispuesto en la normativa reguladora de los derechos digitales.***

En todo caso se garantizarán condiciones de trabajo digno en los entornos digitales.

2. Cuando la naturaleza del puesto y las capacidades de la organización lo permitan **se podrá tener en consideración la promoción ~~promoverán~~ de** condiciones de acceso al teletrabajo. En este caso, la ordenación de la prestación laboral se desarrollará con pleno respeto a la dignidad de la persona trabajadora garantizando particularmente su derecho a la intimidad, la esfera privada del domicilio, los derechos de las personas que residen en él y el derecho a la conciliación de la vida personal y familiar.

### 3. En los procesos de transformación digital:

- a) Deberá proporcionarse a las personas trabajadoras una formación adecuada que permita su adaptación a las nuevas condiciones laborales;
- b) Se informará a la representación de los/as trabajadores/as sobre los cambios tecnológicos que vayan a producirse en la empresa ~~y a participar en la toma de decisiones~~ sobre la transformación digital y las consecuencias laborales que la misma pueda implicar;

4. Sin perjuicio del derecho a no ser objeto de una decisión basada únicamente en procesos de decisión automatizada, salvo en los supuestos previstos por la ley, se informará a los representantes de los/as trabajadores/as y las personas directamente afectadas sobre el uso de la analítica de datos o sistemas de inteligencia artificial en la gestión **y seguimiento**, ~~monitorización y procesos de toma de decisión~~ en materia de recursos humanos y relaciones laborales. ~~Este deber de información alcanzará como mínimo al conocimiento de los datos que se utilizan para alimentar los algoritmos, su lógica de funcionamiento y a la evaluación de los resultados.~~

## 16. Punto XVIII. La empresa en el entorno digital

Aunque la libertad de realizar una actividad comercial se reconoce en el contexto de los entornos digitales, está condicionada con respecto a los derechos digitales. Si se entiende que los "derechos digitales" se describen y regulan en la presente Carta, se aplicarán ciertos límites ilícitos a la libertad de llevar a cabo una actividad comercial (por ejemplo, la prohibición de establecer perfiles).

Adicionalmente, se considera necesaria la incorporación de un apartado adicional con la siguiente redacción:

***XX. Los poderes públicos velarán por que exista un nivel de competencia eficiente en el sector digital conforme a los postulados de la economía de mercado de forma que se asegure la existencia de una pluralidad de productos, servicios y proveedores y oferentes para garantizar el cumplimiento de la legislación vigente.***

## **17. Punto XIX. Derecho de acceso a datos con fines de investigación científica, innovación y desarrollo**

En primer lugar, se desea manifestar, en relación con la referencia que realiza al sector privado en el apartado 1 de este punto XIX (*El uso de los datos del sector público y privado para el bien común se considera un bien de interés general*), que este derecho debería aplicar solamente a los datos del sector público en línea con la Directiva 2019/1024 relativa a los datos abiertos y la reutilización de la información del sector público. Respecto a los datos del sector privado, debería mantenerse el principio general de libertad contractual en el intercambio voluntario de dichos datos. De lo contrario, la innovación en aplicaciones de *Big Data* sufrirá drásticamente.

Cualquier iniciativa que imponga el intercambio de datos del sector privado es prematura teniendo en cuenta que no hay un fallo de mercado, ya que apenas existe un mercado, en comparación con la enorme oportunidad que se presenta.

El intercambio de datos entre empresas es un mercado incipiente que seguirá creciendo a medida que las empresas de todos los sectores avancen hacia modelos de negocio basados en datos. Lo mismo se aplica al intercambio de datos entre el sector privado y la Administración Pública.

Lo importante es crear los incentivos para un modelo de negocio sostenible en el que el uso responsable de los datos permitirá desarrollar políticas públicas más eficientes. Se creará así un círculo virtuoso en el que las Administraciones Públicas podrán reducir el gasto público y reducir impuestos en los ciudadanos, además de liberar presupuesto para compensar a su vez a las empresas que presten servicios basados en datos.

Por otro lado, la investigación clínica implica un tratamiento de datos muy riguroso, al tratarse de datos de salud, para lo cual la determinación de la base jurídica de dicho tratamiento exigiría el cumplimiento de dos requisitos: a) dicha base jurídica deberá ser una de las establecidas en el artículo 6, apartado 1, del Reglamento Europeo de Protección de Datos; b) el tratamiento de los datos de salud deberá estar amparado en una de las excepciones a la prohibición general de tratamiento de dichos datos y, en consecuencia, en uno de los supuestos mencionados en el artículo 9, apartado 2, del citado Reglamento.

Sobre la base de lo anterior, el tratamiento de los datos de los participantes en la investigación clínica se fundamenta en la existencia de una obligación legal (artículo 6.1 c) del RGPD) en conexión con lo dispuesto en el artículo 9.2 i)

y j). En efecto, el tratamiento, por una parte, tiene por objeto el cumplimiento de las obligaciones legales impuestas para garantizar un elevado nivel de calidad y seguridad del medicamento y, por otra, se lleva a cabo con fines de investigación científica sobre la base de las normas del derecho español y de la Unión Europea en materia de garantías y uso racional de los medicamentos y productos sanitarios, que imponen la obligación legal de llevar a cabo las actuaciones de investigación con carácter previo a la comercialización de un medicamento, así como a la realización de estudios posteriores a su autorización.

De este modo y en virtud de esa obligación legal impuesta por la normativa reguladora de los medicamentos y productos sanitarios, no es necesario contar con el consentimiento del interesado para el tratamiento de sus datos personales una vez el mismo haya aceptado formar parte de la investigación.

Los datos identificativos de los participantes no suelen constituir información relevante para la consecución de los objetivos que se persiguen en el marco de las investigaciones clínicas. En este sentido, los datos identificativos de los participantes en las investigaciones clínicas se pseudonimizan a fin de que el Promotor de la investigación clínica no acceda a ellos, dado que, desde el punto de vista científico, no es recomendable trabajar con datos anónimos - salvo alguna excepción que así lo permitiera por la necesidad de garantizar la veracidad y exactitud de esos datos conforme al marco regulatorio.

Con todo ello, se propone modificar este punto XIX en la forma que sigue:

- 1. El uso de los datos del sector público ~~y privado~~ para el bien común se considera un bien de interés general.*
- 2. En el marco definido por las leyes se promoverán condiciones que garanticen la reutilización de la información y el uso de los datos para promover la investigación, la innovación y el desarrollo.*
- 3. Cuando se trate de datos personales:*
  - a) Los datos podrán ser tratados con fines de investigación científica, innovación y desarrollo ~~previa anonimización mediante pseudonimización, o anonimización, en los supuestos que la investigación así lo permitiera y de acuerdo con los requisitos establecidos por la normativa reguladora de la protección de datos personales y de la investigación clínica, biomédica o sanitaria o cualesquiera otra de aplicación.~~***

- b) ~~Únicamente será~~ **Será** admisible el tratamiento de datos personales o pseudonimizados cuando la naturaleza de la actividad lo requiera y se cuente con el consentimiento o una autorización expresa prevista en norma con rango de ley. **En el ámbito de la investigación clínica dicha autorización expresa está amparada en el artículo 6.1.c) del Reglamento Europeo de Protección de Datos en conexión con el artículo 9.2 i) y j), por lo que no resulta necesario el consentimiento.**
- c) Se promoverán programas de donantes de datos para fines de investigación.

En todo caso serán de aplicación el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y la legislación sectorial que corresponda.

4. El desarrollo de la investigación científica y tecnológica susceptible de repercutir en el ser humano respetará su dignidad y garantizará a toda persona, sin discriminación alguna, el respeto a su integridad y a sus demás derechos y libertades fundamentales con respecto a las aplicaciones de la biología y la medicina.

5. La investigación en áreas como la neurociencia, la genómica o la biónica, entre otras, aplicará lo dispuesto en los párrafos anteriores y, en particular, garantizará el respeto a la dignidad, la libre autodeterminación individual, la intimidad y la integridad de las personas.

## **18. Punto XX. Derecho a un desarrollo tecnológico y a un entorno digital sostenible**

En relación con las funciones que se atribuyen a los poderes públicos en el apartado 2 de este punto XX, se debe indicar que el actual reparto competencial establecido en la Constitución Española y la pluralidad de Administraciones y Poderes Públicos, en el pasado, por pluralidad y superposición de diferentes normativas medio ambientales, han originado

situaciones de imposibilidad o ralentización de despliegue de redes e infraestructuras, lo que impide el desarrollo tecnológico y digital. La Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, en su artículo 140, establece como principios generales de las relaciones interadministrativas, entre otros, la coordinación y eficacia. Asimismo, los poderes públicos deberán asumir un poder de concienciación social en la materia a través de promoción de la educación digital sostenible, lo que debe llevar implícito el fomento de la adopción de dichas políticas para garantizar la sostenibilidad medioambiental. Por ello, se propone modificar este punto XX en la forma que sigue:

- 1. El desarrollo de la tecnología y de los entornos digitales deberá perseguir la sostenibilidad medioambiental y el compromiso con las generaciones futuras.*
- 2. Los poderes públicos, **coordinada y eficazmente**, impulsarán **y fomentarán la adopción de** políticas ordenadas a la consecución de tales objetivos con particular atención a la sostenibilidad, durabilidad, reparabilidad y retrocompatibilidad de los dispositivos y sistemas evitando las políticas de sustitución integral y de obsolescencia programada.*
- 3. Los poderes públicos promoverán la eficiencia energética en el entorno digital, favoreciendo la minimización del consumo de energía y la utilización de energías renovables y limpias.*

## **19. Punto XXIII. Derechos ante la Inteligencia artificial**

Respecto al contenido de este punto XXIII, conviene destacar, en primer lugar, la importancia de evitar regular una tecnología en particular, sin especificar de qué servicios se trata. Asimismo, y desde un punto de vista más general, conviene señalar que, teniendo en cuenta que la Comisión Europea está en proceso de definir a nivel de la Unión Europea la futura legislación sobre la Inteligencia Artificial, resulta inapropiado que los Gobiernos nacionales regulen este ámbito.

Los derechos y obligaciones que se establezcan puedan ser muy relevantes para determinados servicios basados en Inteligencia Artificial cuando impacten negativamente sobre los derechos de las personas, pero irrelevantes y/o contraproducentes en otros casos en los que no concurra esta circunstancia.

Por ello, tanto la Unión Europea como el Consejo de Europa han adoptado un enfoque basado en el riesgo. Es decir, se identifican los servicios de alto riesgo (“high risk”) a los que se le aplicaría un régimen normativo determinado, frente a otros en los que se aplicaría otros enfoques como una autorregulación basada en principios éticos.

Respecto al primer punto de este apartado, consideramos que se debería prestar atención al debate legislativo abierto a nivel europeo sobre esta clase de derechos con el fin de adoptar una posición coherente con los mismos.

En este sentido, existen además principios sectoriales que están inspirados y alineados con estas iniciativas europeas.

Además, la Carta no explica qué significa en la práctica transparencia, auditabilidad, explicabilidad y trazabilidad de los sistemas de Inteligencia Artificial.

Respecto al segundo punto, se propone su eliminación parcial. El motivo es que la Carta excede lo establecido en el RGPD puesto que éste limita el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que esta produzca efectos jurídicos en él o le afecten significativamente de modo similar. La Carta incluye las decisiones que empleen procedimientos de Inteligencia Artificial y esto excede lo regulado en el artículo 22, apartado 1, del RGPD.

Respecto al tercer punto, en el que se establece que “(...) *Deberá garantizarse en todo caso la asistencia por un ser humano a solicitud de la persona interesada*”. Se debe indicar que no queda claro a qué tipo de asistencia se está refiriendo el texto, debiendo, en cualquier caso, estar sujeta al riesgo inherente al servicio. De tal modo que sería necesario incluir una distinción de los riesgos del uso de la Inteligencia Artificial puesto que cada uso no impactará de igual modo a las personas.

Actualmente existen una gran variedad de servicios que mejoran la eficacia de sus prestaciones, con una mayor personalización sin que ello repercuta negativamente sobre los derechos de las personas.

En este sentido, la obligatoriedad de este derecho debe estar sujeta a la naturaleza del servicio y al eventual impacto que pueda tener sobre el derecho de la persona.



Este apartado queda condicionado por el derecho a la limitación de localización y perfilado prevista en la Carta, ya que, en particular el perfilado, es la técnica más utilizada en sistemas de IA. Sin embargo, este apartado de la Carta no viene a establecer esa clase de limitaciones en materia de IA.

En este sentido, se establece una diferenciación injustificada entre la IA y la elaboración de perfiles cuando, a efectos prácticos, son virtualmente lo mismo. Limitar la elaboración de perfiles, es limitar, de facto, el desarrollo de la Inteligencia Artificial.

Por último, se considera necesaria una aclaración (o eliminación) del apartado 4, en particular de la referencia que se realiza sobre *el uso de sistemas de Inteligencia Artificial dirigidos a manipular o perturbar la voluntad de las personas (...)*, entendiéndose que los términos empleado resultan imprecisos.

En conclusión, se hace necesario resolver estas incongruencias y respetar los principios rectores de las normativas que actualmente ya regulan el uso de estas tecnologías, las cuales ya regulan correctamente estos puntos de la Carta.

Con todo ello, se propone la modificación de este punto XXIII, en la forma que sigue:

*1. En el desarrollo y ciclo de vida de los sistemas de Inteligencia Artificial:*

- a) Se deberá garantizar el derecho a la no discriminación algorítmica, cualquiera que fuera su origen, causa o naturaleza del sesgo, en relación con las decisiones y procesos basados en algoritmos.*
- b) Se asegurarán la transparencia, auditabilidad, explicabilidad y trazabilidad.*
- c) Deberán garantizarse la accesibilidad, usabilidad y fiabilidad.*

*2. Las personas tienen derecho a no ser objeto de una decisión basada únicamente en procesos de decisión automatizada, ~~incluidas aquellas que empleen procedimientos de inteligencia artificial~~, que produzcan efectos jurídicos o les afecten significativamente de modo similar, salvo en los supuestos previstos en las leyes. En tales casos se reconocen los derechos a:*

- a) Solicitar una supervisión e intervención humana;*
- b) Impugnar las decisiones automatizadas o algorítmicas.*



3. Se deberá informar a las personas sobre el uso de sistemas de Inteligencia Artificial que se comuniquen con seres humanos utilizando el lenguaje natural en todas sus formas. Deberá garantizarse en todo caso la asistencia por un ser humano a solicitud de la persona interesada **que implique una toma de decisiones racional**.

~~4. Se prohíbe el uso de sistemas de Inteligencia Artificial dirigidos a manipular o perturbar la voluntad de las personas, en cualesquiera aspectos que afecten a los derechos fundamentales.~~

## **20. Punto XXIV. Derechos digitales en el empleo de las neurotecnologías**

Respecto a este punto, es necesario indicar que, nuevamente, vemos innecesario establecer principios rectores, derechos u obligaciones relativas al empleo de estas tecnologías en la Carta, especialmente dado que se encuentran en un estado de desarrollo muy temprano y no se tienen referencias ni información sobre el impacto de estas. Por tanto, es preciso esperar a un desarrollo más específico de esta tecnología para regular estos ámbitos.

Consideramos que sería más prudente realizar una evaluación de impacto de estas tecnologías antes de avanzar en el establecimiento de principios, derechos u obligaciones al respecto. Hacerlo de otro modo, implica el riesgo de impactar negativamente su desarrollo, algo totalmente innecesario en esta fase de desarrollo. Por ello, se propone la eliminación de este precepto para su inclusión futura.

## **21. Punto XXV. Garantías de los derechos en los entornos digitales**

Este punto XXV crea automáticamente conflictos de derecho y de jurisdicción. En efecto, la mayoría de las circunstancias que implican los derechos establecidos en la Carta conllevarían el tratamiento de datos personales, que se rige por el RGPD y las normas de ventanilla única, que no se contemplan en este artículo. XXV. Uno de los principales impulsores del proceso de reforma de la protección de datos en Europa fue el deseo de lograr una mayor claridad y coherencia tanto de la reglamentación como de la aplicación de la protección de datos en toda Europa; una de las formas en que el RGPD trata de lograr esa uniformidad es introduciendo el principio de la ventanilla única.

Por tanto, este punto genera ambigüedad por lo que su redacción y contenido debe ser más concreto y, en particular, ha de hacer remisión al Reglamento General de Protección de Datos y a la LOPDGDD, como normas principales que regulan la materia relativa a protección de datos personales y que garantizan una aplicación uniforme de la normativa europea.