
Aportaciones Adigital

Consulta pública para la elaboración de una Carta de Derechos Digitales

Contexto de la Carta de Derechos Digitales

En el marco de la Estrategia digital para España "Agenda 2025", en el plan de recuperación asociado al Plan Europeo de Recuperación "España puede", o en los Presupuestos Generales del Estado para 2021, se hacen varias referencias a la intención del Ejecutivo de avanzar en materia de derechos digitales mediante la creación de una Carta de Derechos Digitales. Así, en junio de 2020, se llevó a cabo una consulta inicial y en noviembre una consulta pública sobre el primer borrador de Carta, a cuya audiencia responde este documento.

Prácticamente al mismo tiempo, el pasado 2 de diciembre, la Comisión Europea publicaba su **Estrategia para reforzar la aplicación de la Carta de Derechos Fundamentales de la UE**¹. La Estrategia prevé que, a partir de 2021, se publique anualmente un informe sobre la aplicación de la Carta. Justamente en relación con los derechos digitales, prevé que el "*primer informe del próximo año se centre en los derechos fundamentales en la era digital*".

En el caso español, en cambio, el proceso comienza por este borrador de Carta que hace referencia a 25 derechos y libertades, no todos fundamentales, relativos a un amplio elenco de prerrogativas, desde la igualdad hasta la privacidad, pasando por la educación, la libertad de expresión o la libertad de empresa, entre otros. Este catálogo, presentado de forma articulada únicamente por una cuestión práctica de facilitar la comprensión de la Carta, ha tenido en cuenta las contribuciones realizadas por un grupo de expertos designados por la SEDIA a tal efecto, aunque no haya habido consenso entre ellos, así como las aportaciones recibidas en la consulta pública previa, en el mes de junio. Al contrario que la Estrategia europea, no indica nada el preámbulo de la Carta sobre la oportunidad de llevar a cabo un **informe o estudio del estado de aplicación de dichos derechos con carácter previo, lo que sería recomendable**.

¹ COM 2020/771, del 2 de diciembre de 2020. Recuperado de: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0711&from=EN>

Carácter descriptivo, prospectivo y programático

De acuerdo con el preámbulo de la Carta, ésta *“no se hace con la intención de crear o descubrir nuevos derechos fundamentales, sino de concretar los más relevantes en el entorno y espacios digitales o describir los derechos instrumentales o auxiliares de los mismos”*. De esta afirmación **cabría deducir que esta Carta tiene, eminentemente, un carácter académico o descriptivo**. Así se deduce también de la previsión en el mismo preámbulo de que *“la Carta no tiene carácter normativo, sino que su objetivo es reconocer los novísimos retos de aplicación e interpretación que la adaptación de los derechos al entorno digital plantea”*. Justamente en este contexto, dado el procedimiento de consulta pública, Adigital valora positivamente la transparencia otorgada al proceso y celebra la oportunidad de poder contribuir con sus aportaciones al mismo.

No obstante, el mismo preámbulo indica también expresamente el carácter descriptivo, prospectivo y prescriptivo del documento. Destaca el **carácter prescriptivo** *“en el sentido de revalidar y legitimar los principios, técnicas y políticas que, desde la cultura misma de los derechos fundamentales, deberían aplicarse a los entornos y espacios digitales presentes y futuros.”* En este punto, es esencial recordar que **en un sistema jurídico el carácter prescriptivo es un adjetivo reservado exclusivamente a la normativa; normativa que, en este caso, obedece evidentemente al principio de reserva de ley y ley orgánica**. Continúa el preámbulo indicando, además, que el objetivo de la Carta es *“sugerir principios y políticas referidas a ellos [los derechos digitales] [...] y proponer un marco de referencia para la acción de los poderes públicos [...]”*.

Este carácter multimodal y ambicioso de la Carta y del procedimiento de consulta han dado lugar a no pocas dudas e incertidumbres. **Desde Adigital se pone de manifiesto la confusión que ha generado** esta previsión, ya que la presente Carta (con sus limitaciones) tiene el potencial de convertirse en un documento de gran relevancia política y social, incluso en el caso de que no se transforme en una norma con carácter vinculante.

Con carácter general, desde Adigital consideramos que **este documento debe mantenerse en el estilo descriptivo, evitando caer en prescripciones o “regulación blanda” que no harían sino añadir confusión en el marco jurídico**. En este sentido, como el propio preámbulo especifica, la Carta hace referencia a derechos que, en su práctica totalidad, ya se encuentran reconocidos y debidamente regulados. Introducir un nuevo instrumento jurídico que regulara los mismos derechos no supondría sino una duplicidad e inseguridad jurídica innecesarias.

Precisamente bajo este prisma se hacen múltiples comentarios a lo largo del documento. En muchas ocasiones, especialmente en la protección de datos, **lo prescrito en la Carta duplica de forma incompleta derechos ya regulados en su normativa específica**. Por una parte, es comprensible que se evite reproducir en la Carta la normativa completa de dichos derechos. Sin embargo, tampoco debe redactarse de forma que se enuncie un derecho de forma incompleta dada la evidente confusión e incertidumbre que generaría. Este proyecto, ya sea académico o prescriptivo, debe abordar necesariamente esta posible confusión y, en nuestra opinión, evitar la inclusión de derechos ya establecidos.

Al contrario, en otras ocasiones, como en la referencia a derechos digitales en el ámbito del trabajo, **la Carta se extralimita en sus previsiones, previendo prerrogativas no reconocidas actualmente en norma alguna**. En estos supuestos, en primer lugar, debe quedar patente que esta carta --sin carácter vinculante-- debe evitar caer en reconocimientos que pueden percibirse como regulación blanda o principios programáticos que únicamente generarían confusión. En este punto debe recordarse que el reconocimiento de derechos, aunque sea programático, debe prescribirse única y exclusivamente de acuerdo con el principio de reserva de ley (orgánica, en su caso). Por esta razón, la Carta que pueda resultar de esta consulta, debe evitar establecer previsiones que no tengan un respaldo legislativo expreso y referenciado.

En lo que la Carta tenga de novedoso, debería revisar su redacción prescriptiva y modificar sus expresiones para acomodarse mejor a un documento de posición política, es decir, invitando a los poderes públicos a considerar enmiendas a normas vigentes o a la regulación de derechos no previstos por la legislación aplicable, por ejemplo, incluyendo al inicio de todos sus preceptos frases como: *"La Secretaría de Estado de Digitalización e Inteligencia Artificial, tras las reuniones del Grupo de Expertos, propone..."* o *"La Secretaría de Estado de Digitalización e Inteligencia Artificial invita a los poderes públicos a..."*.

Adicionalmente, la Carta podría comprometer la armonización de futuras leyes que se están debatiendo actualmente en el ámbito de la UE, como el uso de sistemas de IA; contenidos personalizados y la aplicación de las neurotecnologías.

Apariencia normativa

A este tenor, como se ha mencionado anteriormente, la Carta establece expresamente que *"no tiene carácter normativo"*. En cualquier caso, tampoco ha seguido el procedimiento legislativo

para convertirse en un instrumento normativo vinculante. **Sin embargo, parece y se lee como si de una ley se tratase.** Resulta muy asertiva en su redacción ("*se reconoce el derecho...*", "*se garantizará...*") y, en algunos puntos, muy precisa en la descripción de los derechos que "reconoce" o "garantiza" (y de las obligaciones correspondientes). Dado que el texto de la Carta pretende ir más allá de servir como un marco de referencia para el entorno digital, podría dar lugar a una interpretación errónea de su contenido por parte de los ciudadanos.

Incluso suponiendo que la Carta carezca de efecto normativo, sus (en ocasiones detallados) **apartados podrían verse erróneamente como un instrumento de interpretación de las leyes ya existentes.** Uno de los criterios de interpretación previstos por el Código Civil es "*la realidad social del tiempo en que [las leyes] han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquellas.*" (art. 3.1). Por todos los motivos expuestos, es decir, su aprobación por el Gobierno, la participación de un grupo de expertos y asociaciones (a pesar de haber sido seleccionadas por la SEDIA) y su sometimiento a consulta pública, podría atribuirse erróneamente a la Carta la condición de reflejo de la "realidad social" actual en materia digital.

Además, la Carta no ha sido objeto de un debate legislativo ni de los procedimientos de consenso adecuados, ni se han publicado al respecto informe alguno de órganos consultivos. Como ya se ha dicho, incluye referencias que en ocasiones resultan incompletas y descontextualizadas a leyes en vigor, lo que provoca dificultades de interpretación, y en varias disposiciones esas referencias se extienden más allá del ámbito objetivo o subjetivo de las leyes a las que se remiten, añadiendo contenido a lo ya regulado. Del mismo modo, la Carta podría generar inseguridad jurídica dado que incluye conceptos y términos que no están definidos y que no tienen un equivalente en la legislación vigente.

Como se ha mencionado anteriormente, el preámbulo reconoce que la Carta no sólo "*concreta[r] los [derechos] más relevantes en el entorno y los espacios digitales*", sino que también "*describ[e] derechos instrumentales o auxiliares de los primeros*". En otras palabras, **anticipa de forma sutil o velada que se introducen derechos instrumentales o complementarios (al margen del proceso legislativo).**

Para mitigar esos problemas, entendemos que la Carta debería: (i) revisar a fondo su redacción prescriptiva y modificar sus expresiones para hacerlas más acordes a un documento de posición política, es decir, únicamente invitando a los poderes públicos a considerar enmiendas a normas vigentes; y (ii) dejar claro que las referencias a las leyes existentes no son exhaustivas ni derogatorias y, cuando proceda, que son una mera invitación a considerar enmiendas.

La Carta también afirma que sus principios son "compartidos por todos". Aunque suscita poca controversia la afirmación general de que los derechos fundamentales no deberían ser diferentes en el entorno digital que en el mundo analógico, la forma particular en la que se ejercen esos derechos y la manera en la que interactúan con los derechos de otras personas no está exenta de polémica.

Esa sutil idea de incontestabilidad reside en la redacción imperativa de la Carta. Sin embargo, esto contrasta con el reconocimiento por el Ministerio de que *"el resultado de los trabajos del Grupo no implica por parte de sus miembros consenso entre todos ellos sobre todos y cada uno de los aspectos tratados, los cuales no comparten necesariamente todas las propuestas en él contenidas, ni compromete las opiniones o posiciones individuales mantenidas por los expertos y expertas en el seno de los grupos de trabajo"*. **Esa discrepancia interna entendemos que debería traducirse en un lenguaje más suave, más propio de un papel de posición política.**

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 en línea o los usuarios adultos que no tienen en cuenta que los menores podrían ser incluidos en los destinatarios de contenidos generado por los usuarios inapropiados que generan 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 de la Carta, tal y como está redactado actualmente, no aborda cuestiones de suma importancia, como las citadas anteriormente. Además, dado que la Carta hace referencia al concepto de ciudadanía digital debería mencionar qué tipo de obligaciones se esperan de los ciudadanos, de manera individual, por ejemplo: 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 empresariales de los demás, etc.

Actuaciones paralelas en el ámbito internacional

Por último, en la Carta se mencionan "los procesos de reflexión que se están produciendo a nivel europeo". **Esos procesos de reflexión y el amplio debate suscitado en torno a diversas iniciativas europeas ponen en tela de juicio la conveniencia de una iniciativa nacional como la Carta.** Es el caso, entre otras, de la Estrategia para reforzar la aplicación de la Carta de Derechos de la UE del pasado 2 de diciembre, de la Carta de Derechos Digitales que podría ser presentada durante la presidencia portuguesa, diversas directivas aún no transpuestas en España o diferentes iniciativas en curso como el *White Paper on Artificial Intelligence*, el *Follow-up to the White Paper on Artificial Intelligence - Safety, Liability, Fundamental Rights and Data*, el *European Democracy Action Plan*, la *European Strategy for Data*, la *Data Governance Act*, la *Data Act*, la *Digital Services Act (DSA)*, la *Digital Markets Act* o la *Industrial Strategy*.

Consideraciones específicas sobre los distintos apartados de la Carta

Adigital está de acuerdo con que los derechos digitales son derechos humanos en la era de Internet. Con la evolución de la economía digital y el impacto de las nuevas plataformas *online*, las aplicaciones y los servicios digitales, es recomendable hacer un seguimiento continuo de la actual normativa para garantizar que los derechos fundamentales sean protegidos y garantizados tanto *online* como *offline*.

Sin lugar a duda, este objetivo de la Carta es necesario y pertinente. Sin embargo, se muestra de gran calado, poniendo de manifiesto la insuficiencia de esta consulta pública singular para abordar los ambiciosos propósitos del Ejecutivo. A este respecto, sería interesante prever una estrategia más amplia y holística que pueda abordar tal nivel de ambición más allá de una mera consulta pública. De la misma forma, tendría sentido abordar la cuestión desde la UE, siguiendo la Estrategia planteada recientemente por la Comisión, favoreciendo así acciones y debates coordinados a nivel nacional y europeo.

En cualquier caso, de mantenerse el objetivo de “aprobar” una Carta de Derechos Digitales por el Gobierno, Adigital propone a continuación una serie de consideraciones específicas adicionales sobre los distintos apartados de la Carta que espera puedan tenerse en cuenta.

I. Derechos y libertades en el entorno digital

- 1. Los derechos fundamentales y libertades reconocidos en nuestra Constitución, en la Declaración Universal de Derechos Humanos, la Carta de los Derechos Fundamentales de la Unión Europea y en los tratados y acuerdos internacionales sobre las mismas materias ratificados por España están garantizados en el entorno o espacio digital.*
- 2. Todas las personas poseen idénticos derechos en el entorno digital y en el analógico, sin perjuicio de las limitaciones que de acuerdo con la Constitución y las leyes pudieran establecerse atendiendo a las peculiaridades de cada ámbito.*
- 3. Las leyes concretarán, en cuanto sea necesario, las especificidades de los derechos en el entorno digital y regularán su desenvolvimiento y efectividad estableciendo garantías y promoviendo la igualdad en el ecosistema digital.*
- 4. Los procesos de transformación digital, el desarrollo y el uso de la tecnología digital, así como cualquier proceso de investigación científica y técnica relacionado con ellos o que los utilice instrumentalmente, deberán tener presente la exigencia de garantizar la dignidad humana, los derechos fundamentales, el libre desarrollo de la personalidad y ordenarse al logro del bien común.*
- 5. El principio de cumplimiento normativo desde el diseño deberá aplicarse íntegramente al desarrollo científico y tecnológico, así como a sus resultados. Los desarrollos científicos y tecnológicos contemplarán en la determinación de sus requerimientos un análisis sobre el cumplimiento de tal principio.*

Entre los principios que deben guiar los procesos de transformación digital y el uso de la tecnología digital, así como la educación digital (contemplada en el apartado XV de la Carta), cabe mencionar: i) las libertades fundamentales (y no sólo los derechos fundamentales); y ii) la necesidad de abordar un equilibrio adecuado entre el derecho y las libertades fundamentales (ya

que ningún derecho o libertad fundamental es absoluto y algunos de ellos pueden entrar en conflicto, como sucede a menudo en el mundo *offline*).

Por otro lado, resulta importante recalcar el uso a lo largo de todo el apartado de los términos "entorno o espacio digital", conceptos amplios e indeterminados que no están definidos por ninguna ley y que, por tanto, están sujetos a interpretación, lo que puede resultar confuso y problemático. Sería recomendable emplear un término ya definido que, por estar ya contemplado en nuestras leyes, aporte mayor seguridad jurídica.

En relación con el punto 5, no existe en el ordenamiento jurídico español un "*principio de cumplimiento normativo desde el diseño*". Si la intención de la Carta es afirmar que el ejercicio de los derechos en el entorno digital debe ser lo suficientemente flexible como para adaptarse a la evolución de la ciencia y la tecnología, debería redactarse de esa manera, y no constituir un principio jurídico inexistente.

En cambio, si la intención de la Carta en este punto es que los actores de los entornos digitales deban operar incorporando "desde el diseño" los derechos de esta Carta a sus desarrollos tecnológicos (de manera similar al principio de "privacidad desde el diseño" derivado del RGPD), en ese caso la Carta estaría creando una obligación legal inexistente sin tener habilitación para ello.

II. Derecho a la protección de datos

- 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 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.*
- 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.*

El derecho a la protección de datos es un derecho fundamental regulado en la Constitución Española (Art. 18.4), el RGPD (directamente aplicable en España) y la Ley 3/2018 que ya incluye la

regulación de los "derechos digitales". Por lo tanto, sería 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 párrafo 2, para ser coherente con el RGPD, el consentimiento no debería presentarse como la base jurídica única o principal para el tratamiento de los datos personales establecidos en la ley. El RGPD establece una serie de bases jurídicas para el tratamiento de los datos personales sin ningún orden de jerarquía entre ellas. Al referirse explícitamente sólo al "consentimiento" en el párrafo 2, este artículo sugiere que el "consentimiento" puede tener cierta prioridad. No obstante, cabe recordar que el consentimiento no es la base jurídica "estándar" ni tampoco es *per se* más legítima que el resto de bases jurídicas contempladas por la normativa aplicable en materia de protección de datos personales.

Asimismo, los principios y derechos mencionados en este párrafo no son ilimitados. Las leyes de protección de datos y otras leyes que regulan derechos fundamentales contienen limitaciones y restricciones, incluyendo los derechos de acceso y rectificación que menciona la Carta. Por lo tanto, este párrafo no debería redactarse en términos absolutos.

La Carta especifica que el consentimiento es la única base legitimadora para tratar los datos personales. Sin embargo, existen otras bases legitimadoras de tratamiento en el Reglamento General de Protección de Datos, más concretamente en su artículo 6, que no se reflejan en el texto y consideramos que deberían incluirse. Para ello, proponemos a continuación una redacción alternativa del párrafo 2.

"Estos datos se tratarán de modo leal, para fines concretos y fundamentándose en alguna de sobre la base del consentimiento de la persona afectada las bases jurídicas reguladas en el artículo 6 del Reglamento General de Protección de Datos, de conformidad con el resto de disposiciones del Reglamento General de Protección de Datos y demás normativa que resulte de aplicación. -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."

Además, este artículo 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.

III. Derecho a la identidad en el entorno digital

- 1. Se reconoce el derecho a la propia identidad en el entorno digital, de acuerdo con el ordenamiento jurídico nacional y europeo.*
- 2. La identidad no podrá ser alterada, controlada o manipulada por terceros contra la voluntad de la persona.*
- 3. Se establecerán las garantías que permitan preservar y controlar la propia identidad en el entorno digital.*

Como comentario general a este artículo, ya existe un delito de usurpación del estado civil, regulado en el Código Penal y perfilado por la interpretación de nuestros tribunales. Por ello, consideramos que este artículo podría interferir de manera negativa con esa base jurídica.

El párrafo 2 afirma que "*la identidad no podrá ser alterada, controlada o manipulada por terceros contra la voluntad de la persona*". El significado de esta frase nos parece confuso en su alcance e intención, lo que genera incertidumbre.

No está claro qué garantías "*se establecerán*" según el párrafo 3 para mantener y controlar la propia identidad en el entorno digital y, lo que es más importante en la práctica, quién será responsable de ello. Aunque esto puede interpretarse legítimamente como una invitación a los poderes públicos a reflexionar sobre las garantías jurídicas específicas aplicables a las identidades digitales, se debería evitar una redacción tan imprecisa que pueda ser interpretada por los ciudadanos como un derecho a hacer valer frente a los particulares una garantía genérica para preservar y controlar su identidad digital más allá de las condiciones contractuales aplicables al servicio específico.

En definitiva, este artículo también está redactado en términos absolutos, lo que podría conducir a resultados indeseados. La Carta debería reconocer que este derecho no es una obligación de las empresas de pedir a sus usuarios que se identifiquen en todos los casos o de verificar la

identidad de los usuarios. Algunos servicios pueden prestarse sin pedir al usuario todos los datos de identificación. El derecho a la propia identidad en el entorno digital debe equilibrarse con el principio de minimización de los datos reconocido en el RGPD y la LOPDGD. Imponer a las empresas la obligación de solicitar a los usuarios su identificación en todos los casos, o de verificar su identidad podría implicar la recogida de grandes cantidades de datos personales, lo que podría ser desproporcionado al objetivo perseguido.

Por último, en relación con la identidad en el entorno digital sería interesante **tratar la cuestión de la reputación como un bien y la portabilidad de la información que es generada en las plataformas por los usuarios**. Este es uno de los temas que genera más interés en la sociedad y agentes públicos interesados en la digitalización. Los sistemas de reputación son parte de los datos que componen esta información, contribuyen a la mejora operativa de los servicios a los que se accede a través de una plataforma y reducen la asimetría de información que puede afectar a un cliente.

Por ello, sin perjuicio de lo expuesto anteriormente 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.

IV. Derecho al pseudonimato

1. De acuerdo con las posibilidades técnicas disponibles los entornos digitales permitirán el acceso en condiciones de pseudonimidad.

2. El diseño de la pseudonimidad a la que se refiere el párrafo anterior asegurará la posibilidad de re-identificar a las personas en los casos y con las garantías previstos por el ordenamiento jurídico.

Si bien parece razonable permitir el pseudonimato, no consideramos que lo sea establecer que todos los servicios deban permitirlo en todos los casos. La referencia "*de acuerdo con las posibilidades técnicas disponibles*" no es suficiente limitación a la generalidad de los términos empleados en este artículo ya que los motivos para no permitir el pseudonimato no siempre son de tipo tecnológico.

Así pues, no todos los entornos digitales justifican un derecho de pseudonimidad de los ciudadanos. Existen múltiples entornos digitales (ej. de relación con administraciones públicas, banca, viajes...) en donde se debe garantizar la obligatoriedad de identificación de las personas. La identidad real también es pertinente para crear confianza y establecer relaciones significativas.

Ello no significa que, según el contexto, no se puedan utilizar seudónimos que permitan a las personas expresar determinados atributos de su identidad de distintas maneras, como parte de su libertad de expresión. Sin embargo, esto no equivale a la creación de un "derecho" al seudónimo que, si no está matizado, sólo contradice el derecho a la identidad real.

El RGPD y la LOPDGDD ya prevén la obligación de aplicar los principios de proporcionalidad, limitación del tratamiento y minimización de los datos, según los cuales los datos deben recogerse para fines específicos, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines. Además, deben ser adecuados, pertinentes y limitados a lo estrictamente necesario en relación con los fines para los que se tratan. Los responsables del tratamiento que recogen los datos ya deberían aplicar todos estos principios, por lo que la previsión de este artículo podría ser, o bien superflua, o bien distorsionadora. Al igual que los demás artículos de la Carta, este derecho parece establecer una regulación adicional que complementaría al RGPD y la LOPDGDD y que resulta contradictorio con lo siguiente: (i) el RGPD es un reglamento y los Estados miembros solo pueden añadir contenido o desviarse del contenido del RGPD en relación con las secciones específicas que les permite el propio RGPD (ninguna de las cuales incluye esta cuestión); e (ii) incluso si se pudiera añadir contenido, ello debería hacerse mediante una ley orgánica.

De acuerdo con el párrafo 1, los "entornos digitales" deben permitir el "acceso" en condiciones de pseudonimidad. A los efectos de la Carta, el concepto de "entorno digital" es extremadamente amplio, como ya se ha dicho. Se refiere al conjunto de sistemas, dispositivos, plataformas e infraestructuras que ofrecen espacios de relación, comunicación, interrelación, comercio, negociación, entretenimiento y creación que permiten a las entidades naturales o jurídicas establecer relaciones bilaterales o multilaterales similares a las del mundo físico tradicional.

En términos generales, esto es problemático por lo siguiente: ¿significa que, en general, los proveedores de servicios en Internet deben permitir la apertura de cuentas ("acceso") con un pseudónimo (es decir, sin datos de identificación reales)? En contra de una interpretación tan amplia, puede argumentarse que en el párrafo 2 se establece la obligación subyacente de ser identificado para que la persona con pseudónimo pueda volver a ser identificada cuando sea

necesario. No obstante, sería conveniente evitar la expresión maximalista "los entornos digitales permitirán el acceso en condiciones de pseudonimidad" y definir lo que significa "acceso", que no puede incluir la fase inicial de identificación.

Nótese que si el párrafo 1 se interpretase en sentido amplio, la Administración también debería permitir el acceso de los ciudadanos en condiciones de pseudonimidad, lo que parece inoportuno.

Por las razones antes expuestas, se propone la eliminación total de este artículo o, en todo caso, la modificación siguiente: *"De acuerdo con las posibilidades técnicas disponibles los entornos digitales permitirán el acceso en condiciones de pseudonimidad, siempre y cuando no sea necesaria la identificación personal para el desarrollo de las tareas propias de dicho entorno"*.

V. Derecho a no ser localizado y perfilado

1. El derecho a la libre autodeterminación individual y la garantía de las libertades comporta el derecho a no ser objeto de localización, ni a ser sometido a análisis de la personalidad o conducta que impliquen el perfilado de la persona.

2. Sólo serán posibles tales tratamientos de información personal con el consentimiento de la persona afectada o en los casos y con las garantías previstos en las leyes.

Este artículo contradice la normativa existente sobre geolocalización y elaboración de perfiles precisos (normativa sobre telecomunicaciones, privacidad y protección de datos). Además, sobre esta cuestión se están llevando a cabo debates sobre la reglamentación adecuada de la elaboración de perfiles en el marco de la Ley de servicios digitales. Adicionalmente, **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 ya está regulado en la normativa de telecomunicaciones y de privacidad electrónica, que no impone una prohibición, sino que somete su uso a condiciones

específicas que esta Carta no contempla. Además, la nueva ley de telecomunicaciones española (que regula el uso de estos datos) está actualmente en discusión.

Perfiles. El propio término es subjetivo y puede entenderse de distinta forma dependiendo del público. 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.

Como ya han reconocido las autoridades y reguladores españoles (incluida la Agencia Española de Protección de Datos), ciertos perfiles son clave para que el sector privado y la administración pública puedan ofrecer y prestar un servicio personalizado que responda a necesidades diferentes y específicas y, en consecuencia, puedan favorecer la inclusión.

La elaboración de perfiles también forma parte de obligaciones jurídicas específicas, como las obligaciones de lucha contra el blanqueo de capitales o la obligación de obtener determinada información para poder evaluar los perfiles de riesgo de determinadas operaciones del sector financiero (por ejemplo, para obtener un préstamo, invertir en un fondo o contratar un seguro). Asimismo, es fundamental para permitir una experiencia adecuada a la edad y es parte de las medidas que pueden utilizarse para proteger a los menores. Por otro lado, también es indispensable para fines de seguridad y ciberseguridad, tanto en lo que respecta a las empresas privadas como a las autoridades encargadas de hacer cumplir la ley, ya que les permite detectar las pautas de los 'agentes malintencionados'.

Además, la elaboración de perfiles ya está reglamentada en el RGPD. El RGPD no prohíbe la elaboración de perfiles ni dispone que sólo se permita la elaboración de perfiles cuando se obtenga el consentimiento del interesado. La RGPD limita la elaboración de perfiles (o la adopción de decisiones automatizadas) cuando esta decisión tiene efectos jurídicos u otros efectos igualmente importantes para el interesado. No prohíbe completamente la "elaboración de perfiles". La introducción de esta disposición crearía confusión. Además, la Agencia Española de Protección de Datos ha emitido varios informes en los que se analizan las actividades de elaboración de perfiles y nunca ha prohibido este tipo de actividades (ni siquiera cuando se realizan con fines publicitarios).

Además, la prohibición de los perfiles interfiere con la libertad fundamental de establecer un negocio. La prohibición de la elaboración de perfiles establecida en el Art. V también es contradictoria con el Art. XIII, que establece el derecho a ser informado de la elaboración de perfiles.

Por los argumentos propuestos anteriormente, se considera que este apartado debe eliminarse de esta Carta.

VI. Derecho a la seguridad digital

- 1. Toda persona tiene derecho a la seguridad en el entorno digital.*
- 2. Los poderes públicos adoptarán y promoverán las medidas necesarias para garantizar aquélla, en colaboración siempre con las empresas tecnológicas y con los usuarios.*

El propósito de incluir este artículo no está claro, ya que está formulado de manera tan absoluta que nadie podría garantizarlo o incluso definirlo.

Este artículo va más allá del contenido del artículo 82 de la LOPDGDD. Dicho artículo únicamente indica que *"Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos"*.

En relación con el **párrafo 2**, se desconoce si su propósito es imponer a las empresas tecnológicas alguna obligación de colaboración que no esté ya prevista en la ley " en colaboración siempre con las empresas tecnológicas..."). Este párrafo debería reformularse para aclarar que se refiere a la obligación de las autoridades públicas de *permitir* la intervención de las empresas tecnológicas y los usuarios en la promoción y garantía de la seguridad digital, pero no de *obligar* a esa intervención.

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.

VII. Derecho a la herencia digital

1. Se reconoce el derecho a la herencia digital de todos los bienes y derechos de los que sea titular la persona fallecida en el entorno digital.

2. El acceso a contenidos y servicios digitales de los que fuera titular la persona fallecida se hará conforme a las reglas generales del Código Civil, las leyes de las Comunidades autónomas con derecho civil, foral o especial, propio y el Título X de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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 las disposiciones 3 y 96 de esta ley son particularmente confusas y a veces contradictorias 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 para orientar futuras regulaciones, que tampoco podrán beneficiarse de una interpretación armonizada a nivel europeo, porque no es aplicable el RGPD ya que, según su considerando 27 no se aplica a la protección de datos personales de las personas fallecidas y deja su regulación a los Estados miembros.

Más concretamente, nos gustaría hacer dos comentarios acerca de las cuestiones que nos preocupan específicamente en el texto del apartado:

1. Existe el riesgo de que se interprete erróneamente que "*todos*" los bienes y derechos a los que una persona tiene acceso en vida pueden transmitirse como parte de una "*herencia digital*". Esto no es así. En ocasiones, los bienes digitales pueden tenerse en propiedad, pero en muchos casos el acceso a los bienes, servicios, relaciones, etc. digitales se realiza a través de un servicio prestado por un tercero y está sujeto a los términos del servicio, aceptados contractualmente por el usuario. En esos términos del servicio se suele

establecer que los usuarios no obtienen un derecho de propiedad y el servicio, y consecuentemente los derechos de acceso del usuario, podrían extinguirse cuando el usuario fallece. Así pues, creemos que la Carta debería modificarse para que no se interprete erróneamente que todos los accesos a los contenidos digitales de una persona fallecida pueden ser heredados.

2. El término "*herencia*" se refiere al patrimonio económico del fallecido. Sin embargo, los fallecidos también tienen derechos morales que siguen una vía legal diferente. El honor, la intimidad y la imagen del fallecido se extinguen tras el fallecimiento, pero no el derecho a preservar su memoria. El acceso a las cuentas digitales del fallecido puede afectar su memoria (por ejemplo, las comunicaciones mantenidas en secreto por el fallecido). La Ley Orgánica 1/1982 establece disposiciones específicas sobre quién puede encargarse de la protección de la memoria del fallecido. El Tribunal Supremo ha declarado que la mera condición de heredero (en lo que respecta a la "*herencia*" patrimonial) no proporciona la condición de protector de la memoria del fallecido (STS 414/2016, de 20 de junio de 2016). Por lo tanto: (a) para llevar a cabo el acceso a la cuenta digital del fallecido debe considerarse en primer lugar si dicho acceso puede afectar a su memoria; y (b) no son los herederos los designados para proteger la memoria del fallecido, sino la(s) persona(s) concreta(s) mencionada(s) en la Ley Orgánica 1/1982, que incluye(n) en primer lugar a la persona designada por el fallecido para ese cometido. En consecuencia, se debería modificar la Carta para dejar claro que la "*herencia digital*" no debe dar lugar a un acceso que pueda afectar a la protección del derecho moral del fallecido a preservar su memoria.

VIII. Derecho a la igualdad y a la no discriminación en el entorno digital

1. 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.

2. Los poderes públicos impulsarán políticas ordenadas a la garantía del acceso efectivo de todas las personas a los servicios y oportunidades que ofrecen los entornos digitales en cualquiera de sus dimensiones, garantizarán el derecho a la no exclusión digital y combatirán las brechas digitales en todas sus manifestaciones, atendiendo particularmente

a la brecha territorial y asegurando un derecho de acceso universal, asequible, de calidad y no discriminatorio a Internet para toda la población.

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.

En el párrafo 1 en el cual *"se reconoce el derecho a la igualdad en los entornos digitales"*, consideramos que la Carta podría tomar como referencia el artículo 14 de la Constitución que reza *"Los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social"*. Se reconoce el derecho a la igualdad en los entornos digitales sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social.

Luchar de manera efectiva contra la discriminación requeriría poder contar con datos de contraste que actualmente está prohibido recabar por art. 9 RGPD (y considerandos 51 a 56) y en art. 9 LOPD. Por ello, debería revisarse la posibilidad de uso de las categorías especiales de datos y, de levantarse, aclarar de manera transparente a aquellos ciudadanos a los que se pregunte por esas variables sensibles que su uso va a ser exclusivamente el de la lucha contra la discriminación y/o exclusión.

IX. Protección de menores en el entorno digital

1. Los progenitores, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos, de los entornos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en entornos digitales en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el

derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

3. Salvo en las excepciones previstas en las leyes, se prohíben los tratamientos de la información de los menores orientados a establecer perfiles de personalidad en entornos digitales.

4. Se consideran ilícitas las prácticas de perfilado susceptibles de manipular o perturbar la voluntad de los menores y, en particular, la publicidad basada en este tipo de técnicas.

5. Se impulsará el estudio del impacto en el desarrollo de la personalidad de los menores derivado del acceso a entornos digitales, así como a contenidos nocivos o peligrosos. Dicho estudio prestará particular atención a sus efectos en la educación afectivo-sexual, las conductas dependientes, la igualdad de género, así como los comportamientos antidemocráticos, racistas y violentos.

El párrafo 1 es prácticamente idéntico al párrafo 1 del artículo 84 de la LOPD, pero añade los "entornos digitales" a la lista de ámbitos en los que los padres, tutores, fideicomisarios o representantes legales deben proteger los derechos de los menores. Como hemos dicho, la definición de "entorno digital" que emplea la Carta no proviene de ninguna norma y es extremadamente amplia, lo que conduce a un ámbito de aplicación ampliado y no correctamente delimitado, por lo que no es claro que sea acorde con el artículo 84 de la LOPDGDD.

Lo mismo ocurre con el párrafo 2. Es prácticamente idéntico al párrafo 1 del artículo 92 de la LOPD, pero añade una referencia a los "entornos digitales".

En cambio, **los párrafos 3 y 4 no se derivan de disposiciones específicas de la ley y contienen acciones concretas que se declaran "prohibidas" e "ilícitas", como si la Carta tuviera la potestad jurídica de hacer tales declaraciones.** A diferencia de lo que sugieren estos párrafos, no existe una prohibición general de tratar datos de menores para establecer perfiles de personalidad, ni siquiera existe una lista de excepciones en la ley. Reiteramos lo dicho anteriormente sobre la falta de claridad en cuanto a lo que significa exactamente la elaboración de perfiles en este contexto. Una experiencia apropiada para la edad requiere la elaboración de perfiles por definición. Es esencial para permitir el acceso a productos y servicios apropiados para personas en diferentes tramos de edad, así como reducir al mínimo el acceso a experiencias perjudiciales/inapropiadas.

Así pues, la elaboración de perfiles basados en datos personales está regulada en la LOPD y el RGPD, y está sujeta a rigurosos requisitos, pero no existe una prohibición general, ni siquiera en lo que se refiere a los menores. Por lo tanto, aunque pueda haber poca controversia sobre el concepto de que los menores deben ser cuidadosamente protegidos (no solo en los entornos digitales), la Carta no puede imponer prohibiciones que no estén incluidas en la ley. Por ejemplo, un ámbito en el que la elaboración de perfiles, con las debidas garantías, puede ser legal, es el de la publicidad dirigida a los menores (no se olvide que se es menor hasta los 17 años y la aproximación es diferente en función de la edad real del menor y su capacidad de discernimiento).

Si la intención 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 atribuye indebidamente características negativas a toda actividad publicitaria. La actividad publicitaria tiene su propia legislación específica (Ley 34/1988 de Publicidad); además, existen disposiciones específicas incluidas en la normativa de consumo, protección de datos, comercio electrónico y telecomunicaciones, así como en otras normativas de actividad sectorial. Esta Carta no es el instrumento adecuado para determinar los límites de la actividad publicitaria, y desde luego no de forma 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 no contempla las disposiciones contenidas en la Carta de las Naciones Unidas sobre 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.

X. Protección de personas con discapacidad en el entorno digital

1. Se garantizará la accesibilidad de los entornos digitales a las personas con discapacidad tanto desde el punto de vista tecnológico como respecto de sus contenidos. En particular, asegurarán que la información relativa a las condiciones legales del servicio resulte accesible y comprensible.

2. Los entornos digitales, y en particular los que tengan por finalidad la participación política digital, asegurarán la participación efectiva de las personas con discapacidad o diversidad funcional.

3. Se garantizará el derecho a la educación digital de las personas con discapacidad.

El impacto de este derecho es vago. Por una parte, no se considera que esta Carta deba ser fuente reguladora de derechos y obligaciones. Y, en su caso, debe tenerse en cuenta que la discapacidad (como concepto general) es muy amplia. La Carta impone una obligación general de proporcionar información jurídica accesible y comprensible; sin embargo, en caso de establecer una obligación, deben proporcionarse muchos más detalles en cuanto a los detalles de esta obligación (por ejemplo, siguiendo criterios como los incluidos en la Disposición Adicional quinta de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico).

Destaca también la omisión (¿intencionada?) del sujeto en el punto 1 *in fine*. De manera que no se indica quién "aseguraré" que la información sobre los términos jurídicos del servicio sea accesible y comprensible para todas las personas discapacitadas.

Este artículo puede interpretarse en el sentido de que impone a toda persona que opere en entornos digitales la obligación de hacer que los términos jurídicos del servicio sean accesibles y comprensibles para todas las personas discapacitadas. Sin embargo, esa obligación específica no se impone como tal en la ley. La disposición adicional quinta de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, se refiere a la accesibilidad de las personas con discapacidad y de las personas mayores. Sin embargo, esa sección está dirigida únicamente a las páginas web del sector público, que deben hacerse accesibles a las

personas con discapacidad de conformidad con los requisitos de las normas de accesibilidad ampliamente reconocidas. Por lo tanto, no tiene un impacto directo en las entidades privadas.

Asimismo, el Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el texto refundido de la Ley General de Derechos de las Personas con Discapacidad y su Inclusión Social, impone obligaciones genéricas de accesibilidad que, en lo que respecta a los servicios digitales, están sujetas a su desarrollo reglamentario (art. 24) que, sin embargo, no se ha publicado (**La Comunidad Autónoma de Galicia promulgó la Ley 10/2014, de 3 de diciembre, de accesibilidad, trata parcialmente estas cuestiones y es aplicable solamente en su territorio.*). El Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas de accesibilidad de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y los medios de comunicación social, tampoco impone esa obligación específica. Por lo tanto, la obligación específica impuesta por la Carta no se deriva de una norma jurídica en vigor. La Carta no tiene la facultad de imponer nuevas obligaciones, por lo que debería modificarse para evitar equívocos.

XI. Protección de las personas mayores en el entorno digital

- 1. Se reconoce el derecho de las personas mayores al acceso a los entornos digitales.*
- 2. Se garantizará la accesibilidad a los entornos digitales a las personas de este colectivo.*

Al igual que en el caso anterior de protección de las personas con discapacidad, tampoco existe una disposición legal que establezca garantías específicas de accesibilidad a los entornos digitales aplicables a las personas mayores.

XIII. Libertad de Expresión y Libertad de Información

- 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 o bien provean tal servicio a sus usuarios, adoptarán protocolos adecuados para garantizar 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.

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.

Quando 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 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.

En primer lugar, este apartado XIII de libertad de expresión y de información debería **distinguir entre las responsabilidades** de las personas (incluidas las personas no naturales 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).

Asimismo, existen otros 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.

El término "responsables de medios de comunicación" que aparece en el **párrafo 2** es un concepto indeterminado, lo que genera incertidumbre e inseguridad jurídica.

En relación con los apartados a), b), c), d) y e), consideramos:

- En primer lugar, en relación con el **párrafo. 2 a)** nuestra opinión es que imponer a las empresas que operan en entornos digitales, el hecho de disponer de instrumentos para detectar contenidos creados sin intervención humana (por ejemplo, noticias falsas y "botposts") y de hacer todo lo posible para detectar este tipo de contenidos supondría una carga desproporcionada, al igual que la obligación de valorar y decidir si los contenidos fueron creados por medios humanos o automatizados. Por otro lado, el uso de la tecnología de automatización que afecte a los datos personales está regulado en

general en el RGPD. En concreto, el artículo 22 del RGPD ya establece los derechos que tienen las personas en relación con la toma de decisiones automatizadas, incluyendo la elaboración de perfiles, que produce efectos jurídicos en relación con el interesado o que le afectan de forma significativa. Por lo tanto, la Carta debería prescindir de este apartado.

- En segundo lugar, el apartado **2.b)** contiene una referencia genérica y fuera de contexto a obligaciones de transparencia equivalentes a las del Reglamento 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea, lo que plantea problemas de interpretación. La Carta debería evitar las referencias parciales a una materia regulada. Además, debería tener en cuenta que los requisitos de información y transparencia no deben entenderse como "sobre-información", ya que ello podría generar alarma y preocupación innecesaria en los ciudadanos. En este sentido, toda obligación de transparencia es una buena noticia si está "enfocada hacia el individuo", y no "enfocada hacia la regulación".
- En tercer lugar, **el párrafo 2.c)** equivaldría a una exclusión voluntaria de cualquier tipo de técnica de perfilado, ya que todas las ideas son susceptibles de "afectar" a la forma en la 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. Asimismo, cabe recordar que la elaboración de perfiles ya está regulada en el RGPD y la Carta no es un instrumento válido para modificar sus disposiciones. Además, este **apartado 2.c)** parece prohibir en términos absolutos a los "proveedores" el tratamiento de datos de categorías especiales. Esto sería mucho más restrictivo que el RGPD. Con arreglo al RGPD, si un responsable de tratamiento de datos personales está legitimado para tratar datos de categorías especiales/sensibles con base en una de las bases jurídicas del tratamiento previstas (por ejemplo, el consentimiento explícito, los intereses vitales o la exención con fines de investigación, por nombrar algunos de ellos), nada en esta Carta debe impedirle hacerlo.
- En cuarto lugar, el **párrafo 2.d)** se refiere al derecho de rectificación. Reproduce casi literalmente las disposiciones del artículo 85 de la LOPDGDD y, por lo tanto, hereda los mismos problemas de interpretación de ese artículo. Ambos se refieren a los "*requisitos y procedimientos*" regulados en la Ley Orgánica 2/1984, de 26 de marzo, del derecho de rectificación. Sin embargo:

- La Ley Orgánica 2/1984 sólo es aplicable a la rectificación de la información publicada por los medios de comunicación social, mientras que tanto el artículo 85 de la LOPDGDD como la Carta se refieren además a la información publicada por los "usuarios".
- La Ley Orgánica 2/1984 solo se refiere a *"hechos inexactos cuya publicación pueda causar perjuicio"*, mientras que tanto el artículo 85 de la LOPDGDD como la Carta se refieren más ampliamente a *"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"*.

Por tanto, los "requisitos" de la Ley Orgánica 2/1984 pueden no cumplirse y en esos casos los "procesos" diseñados por esa Ley Orgánica pueden no estar adecuadamente adaptados, dejando a los responsables de los entornos digitales en una situación de incertidumbre.

Además, como ya se ha dicho, no todos los proveedores de servicios de alojamiento son autores ni editores y los derechos de rectificación deben dirigirse debidamente a los usuarios de las plataformas de hospedaje y no a los propios proveedores de las plataformas de hospedaje. Por ello, 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 incompatible con la naturaleza y la función de un proveedor de hospedaje.

- En quinto lugar, el **párrafo 2.e)** reproduce el artículo 86 de la LOPDGDD, que va más allá del derecho al olvido y regula las condiciones específicas aplicables a los *"medios de comunicación digitales"* (no definidos) en materia de actualización de la información. Sería conveniente definir qué es un *"medio de comunicación digital"*, aunque la Carta no es el instrumento legislativo adecuado para hacerlo.

Por otra parte, entendemos que la redacción actual del **párrafo 3** no es clara. 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, entre otros instrumentos jurídicos, como la Directiva 2019/709 sobre los derechos de autor y derechos afines en el mercado único digital y los debates que se están llevando a cabo actualmente en Europa en relación con la propuesta de

Reglamento sobre un mercado único para servicios digitales (la conocida como *Digital Services Act*). Por su parte, 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, por un lado, en la persona o el organismo interesado y, por otro, en los tribunales, sin perjuicio de la posibilidad de intervención de otros interesados cuando las leyes lo permiten. No es apropiado que los prestadores de servicios de intermediación en línea estén mediando en disputas sobre la legalidad del contenido. En el curso de una investigación penal, existen situaciones en las que informar al usuario es contrario a la Ley de Enjuiciamiento Criminal (artículo 301); hacerlo puede considerarse un delito de desobediencia.

Es necesario aclarar más lo que significaría en la práctica la "prohibición de la censura previa". La censura previa es un concepto generalmente vinculado a la prohibición de la intervención de las autoridades antes de la publicación de noticias en la prensa y los medios de comunicación relacionados. Por lo tanto, conceptualmente no es aplicable a los servicios privados, que pueden decidir legítimamente qué contenidos desean publicar o distribuir, al amparo de su libertad de empresa. Del mismo modo, los servicios digitales no están sujetos a una prohibición de censura previa. Si con esta frase lo que se quiere es hacer referencia a la prohibición de imponer a determinados prestadores de servicios digitales una obligación de supervisión general (art. 15 de la Directiva 2000/31, art. 17.8 de la Directiva 2019/709), habría que modificar la redacción para decirlo con claridad.

Asimismo, la libertad de establecer una empresa debería permitir a cualquier empresa exponer los comportamientos de los usuarios que son inaceptables al utilizar sus servicios (como los comportamientos perjudiciales, además de los comportamientos ilegales) y tomar medidas para eliminar o prevenir tales comportamientos, siempre y cuando los términos y condiciones respeten el derecho vigente.

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. En este sentido, cabe recordar que, lo que es legal en un país puede ser ilegal en otro.

XIV. Derecho a la participación ciudadana por medios digitales

1. De acuerdo con las leyes, se impulsarán procedimientos de participación de las personas en la vida pública.

Para ello, se promoverán entornos digitales que contribuyan a un derecho de acceso efectivo a la información pública, la transparencia, la rendición de cuentas, así como a la propuesta, e implicación de las personas en las actuaciones de las Administraciones públicas en sus respectivos ámbitos competenciales, de acuerdo con la Constitución.

2. Los procedimientos de participación ciudadana garantizarán condiciones de igualdad sin discriminaciones ni exclusión de personas, con sujeción al ordenamiento jurídico.

La redacción del segundo párrafo del punto 1 se considera **imprecisa y confusa**, ya que 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. Por estas razones, se requiere aclaración.

XV. Derecho a la educación digital

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales.

2. El profesorado recibirá la formación para adquirir las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

3. En particular los poderes públicos con competencia en la materia promoverán:

- a) Los planes de formación profesional que se ordenarán a la inserción de las personas trabajadoras en los procesos de transformación digital.*
- c) La formación de personas adultas con particular atención a los mayores.*
- d) La educación audiovisual en el entorno digital, con la finalidad de promover la capacidad crítica y afrontar las prácticas de desinformación.*

4. Se reconoce el derecho a la libertad de acceso a la educación y a la libertad de creación de centros que presten sus servicios a través de entornos digitales, sin perjuicio de lo dispuesto en las leyes respecto al cumplimiento de la normativa educativa y de la obligación de la escolarización presencial en los niveles de educación obligatoria.

5. Se impulsará la Educación para la Ciudadanía Digital, porque una parte esencial de la estrategia de digitalización de la educación pasa por el desarrollo de competencias que permitan que el uso de las tecnologías sea beneficioso para cada individuo y para el conjunto de la sociedad. Esta dimensión pasa por cuestiones como:

- a) Que los estudiantes aprendan a hacer un uso ético de las herramientas digitales en cuestiones como el uso de datos y el respeto a la privacidad ajena; o la identificación de información y comportamientos en la red que puede comprometer su salud o bienestar y la de terceros.*
- b) Fortalecer el desarrollo del pensamiento crítico que les ayude a distinguir hechos objetivos de meras opiniones sin evidencias, que les permitan rechazar estereotipos discriminatorios, los discursos de odio o el ciberacoso.*
- c) Fomentar también la capacidad de participar en la generación de información de manera activa, creativa y, sobre todo, responsable.*
- d) Atender la diversidad de talentos y de procesos y ritmos de aprendizaje, particularmente aquéllos que tienen necesidades específicas de apoyo educativo.*

Este apartado contiene **previsiones excesivamente específicas, y por ello inapropiada para una Carta destinada a establecer principios**, particularmente cuando se está debatiendo una nueva ley de educación en el Congreso.

XVI. Derechos digitales de la ciudadanía en sus relaciones con las Administraciones públicas

1. Se reconoce el derecho de igualdad en el acceso a los servicios públicos y en las relaciones digitales con las Administraciones públicas. A tal fin se promoverán políticas públicas activas que garanticen el acceso a los sistemas y los procedimientos.

2. El poder público autor de una actividad en el entorno digital deberá identificar a los órganos responsables de la misma.

3. El principio de transparencia y de reutilización de datos de las Administraciones públicas guiará la actuación de la Administración digital, de conformidad con la normativa sectorial. En particular, se garantizará el derecho de acceso a la información pública, se promoverá la publicidad activa y la rendición de cuentas y se velará por la portabilidad de los datos y la interoperabilidad de los formatos, sistemas y aplicaciones.

4. 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. 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.

5. Se ofrecerán alternativas en el mundo físico que garanticen los derechos de aquellas personas que opten por no utilizar recursos digitales.

6. Los daños causados por actividades o decisiones digitales, podrán dar lugar a un derecho a la indemnización por toda lesión que las personas físicas o jurídicas sufran en cualquiera de sus bienes y derechos, de acuerdo con las leyes

7. Los derechos de la ciudadanía en relación con la Inteligencia Artificial reconocidos en esta Carta resultarán también de aplicación en el marco de la actuación administrativa, en particular en los aspectos referidos al diseño y al uso de algoritmos. En todo caso, se reconoce el derecho a:

- a) Que las decisiones y actividades en el entorno digital respeten los principios de buen gobierno y el derecho a una buena Administración digital.*
- b) Un procedimiento de toma de decisiones con las debidas garantías.*
- c) Obtener una motivación comprensible en lenguaje natural de las decisiones que se adopten en el entorno digital, con justificación de las normas jurídicas relevantes al caso y de los criterios de aplicación de las mismas*
- d) Que la adopción de decisiones discrecionales quede reservada a personas, salvo que una norma con rango de ley permita la adopción de decisiones automatizadas en este ámbito.*

Será necesaria 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.

El apartado 4 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. **Asimismo 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**”.*

El último inciso, señalado en negrita, 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”.

Por último, el punto 7 *in fine*, establece la **obligación de llevar a cabo una evaluación de impacto en el diseño de los algoritmos**. En este punto, se propone sustituir esta obligación por una recomendación de la siguiente forma:

~~“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. [...]”.~~

XVII. Derechos en el ámbito laboral

1. En el ámbito laboral trabajadores y los empleados públicos tienen derecho a:

- a) La desconexión digital.*
- b) La protección de su 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.*
- c) La intimidad ante la utilización de sistemas de geolocalización.*

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 promoverán 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 trabajadores 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 trabajadores y las personas directamente afectadas sobre el uso de la analítica de datos o sistemas de inteligencia artificial en la gestión, 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.

Valoramos la presente iniciativa como un avance hacia principios jurídicos más acordes a los vínculos laborales a través de plataformas digitales, en tanto varias de las cuestiones incluidas resultan aplicables a los mismos.

En el actual contexto de discusión y desarrollo normativo sobre las especificidades de los derechos en entornos digitales, es importante proveer a las relaciones que se establezcan a través de plataformas con principios legales específicos que contengan una descripción - aunque sea mínima, dada la variedad de perfiles de colaboradores y modelos - de las condiciones de la

prestación. Ello con el objetivo de facilitar la aplicación de la normativa laboral a estas realidades y para asegurar que las mismas se lleven a cabo en un contexto de seguridad y transparencia. En ese sentido, podría considerarse la incorporación de ciertos puntos en relación a la utilización de plataformas digitales en cuestiones como la protección a la intimidad y la intimidad ante la utilización de sistemas de geolocalización, que aporten una interpretación más armónica de esos derechos en este contexto digital particular.

A) Punto 1, derechos digitales en el ámbito laboral

Entre los derechos previstos en este apartado, se establece el **derecho a la protección de la intimidad** en el uso de dispositivos digitales puestos a disposición por el empleador o en los sistemas de vigilancia, **sin matices que son necesarios, ya que, si la medida resulta proporcional, es válida.**

Los Tribunales han reconocido la validez de la utilización de sistemas de geolocalización (i.e; coches de vendedores), siempre que se cumplan una serie de 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); 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 art 20.3 del Estatuto de los Trabajadores (ET en adelante), de acuerdo con el cual *"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 (...)".*

Por estas razones, se propone modificar el apartado 1.b) de la siguiente forma: *"La protección de su 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, salvo que sea necesario por motivos de seguridad y así se informe mediante carteles que adviertan de la presencia de cámaras de videovigilancia"*.

B) Punto 3, información sobre los procesos de transformación digital en la empresa

En este punto, a nivel general, podría extenderse el derecho también a los ámbitos en los que no se cuenta con representación de los trabajadores o bien en el que los usuarios utilizan plataformas digitales con fines laborales, pero no son necesariamente parte de un colectivo de trabajadores.

De esta forma, se hace extensiva la obligación de formación a más entornos digitales - tal como se entiende en la Carta - ampliando la protección a más tipos de interacciones de tipo laboral, que se dan a través de espacios digitales.

El apartado b) del punto 3 establece la obligación de informar a la representación de los trabajadores sobre los cambios tecnológicos que vayan a producirse en la empresa, junto con el derecho a participar en la toma de decisiones de transformación digital. A este respecto, la **redacción del apartado es imprecisa y genera confusión**, ya que no determina verdaderamente a qué se refiere.

Adicionalmente, de esta redacción se deduce una **extralimitación de la Carta respecto a la normativa vigente**. La representación de los trabajadores ya tiene reconocidos una serie de derechos de información y consulta (art. 64, 40, 41, 51 del ET), entre los que podríamos entender ya incluida su participación sobre cualquier cambio tecnológico o transformación digital relevantes que se fuesen a introducir en la empresa y tuviesen consecuencias laborales.

En este sentido, cuando estos cambios (derivados de la transformación digital o no) puedan suponer cambios en la estructura y/o evolución del empleo o cambios relevantes en la organización del trabajo y/o contratos de trabajo, sí deben ser informados. Esta cuestión es muy distinta a que deban participar de la transformación digital que la empresa adopte dentro de su capacidad de dirección, debidamente otorgada al empresario por el artículo 20 del ET.

La toma de decisiones iniciales sobre cualquier transformación que pretenda introducirse en la empresa debe quedar bajo el paraguas del poder de dirección del empresario y el derecho fundamental a la libertad de empresa (art. 20 ET y art. 38 CE), y todo ello sin perjuicio al derecho que ostenta la representación de los trabajadores de participación y consulta en todas aquellas decisiones que tuviesen consecuencias laborales.

En definitiva, a la vista de los anteriores argumentos, y vista la redacción actual del artículo 64 del ET sobre derecho de información y consulta, que nada dice respecto a la necesidad prevista en esta carta, es esencial que se preserve la libertad de empresa y se propone la modificación de este apartado de la siguiente manera:

“En los procesos de transformación digital: (...) b) Se informará a la representación de los trabajadores 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”.

C) Punto 4, uso de IA en la gestión, monitorización y toma de decisiones en materia de recursos humanos

En relación con este apartado, consideramos que en parte ya se encuentra regulado como derecho que va más allá de la mera información y es el derecho a emitir informe previo a la ejecución de la medida (art. 64 ET) sobre la implementación y revisión de sistemas de organización y control de trabajo o estudios de tiempos. Sin embargo, el mismo ET no establece que los representantes de los trabajadores tengan que ser informados durante los “procesos de toma de decisión”, por lo que la Carta estaría nuevamente extralimitándose respecto a la normativa existente.

Adicionalmente, este punto hace de nuevo la referencia a que *“sin perjuicio del derecho a no ser objeto de una decisión basada únicamente en procesos de decisión automatizada [...]”*. Sobre esta referencia, se considera descontextualizada, puesto que consiste (de nuevo) en una modificación del artículo 22 del RGPD, y omite partes del artículo 22.1 del RGPD, como por ejemplo: *“El interesado tendrá derecho a no ser objeto de una decisión basada únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, *que produzca efectos jurídicos que le conciernan o que le afecten de forma análoga y significativa”*.

Asimismo, en relación al *“derecho a no ser objeto de una decisión basada únicamente en procesos de decisión automatizada”*, se sugiere la inclusión de definiciones para aquellos conceptos con los que no se cuentan con definiciones legales o que son tomados de áreas del derecho ya desarrolladas, pero interpretadas a la luz de las dinámicas digitales. Más allá de que las decisiones automatizadas deban adecuarse a la legislación nacional, garantizando el respeto y compatibilidad con los derechos fundamentales, los algoritmos deben ser entendibles para los usuarios y todos los actores implicados (sin menoscabar el I+D+i y *know-how* de las organizaciones que los utilizan).

Además, se debe hacer alusión nuevamente a los principios recogidos en el artículo 64 de ET, sobre derechos de información y consulta y competencias. Llama la atención 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”*), entendiéndose necesaria su eliminación dado que esta obligación puede ser enormemente intrusiva para la empresa ya que puede afectar a secretos industriales, al *Kow How* de la compañía o a procesos internos de la misma.

Por estas razones, consideramos que debe eliminarse esta mención y proponemos la siguiente redacción del apartado: “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 trabajadores 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~~”.

XIX. Derecho de acceso a datos con fines de investigación científica, innovación y desarrollo

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.
 - b) Únicamente 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.
 - 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.

A) Datos como bien de interés general

En primer lugar, el punto 1 **declara que los datos del sector privado se consideran un bien de interés general**. Esta afirmación de interés pública "por definición" es problemática. Los datos del sector privado, al igual que cualquier otro bien de naturaleza privada, pueden estar sujetos a derechos de propiedad legítimos. Considerarlos, en su conjunto (es decir, no para un fin específico, justificado y limitado) bienes de interés general, **apunta peligrosamente a mecanismos de expropiación que pueden contravenir el derecho a la propiedad privada**, tal y como se recoge en la Ley de expropiación forzosa de 16 de diciembre de 1954 y en la jurisprudencia relacionada.

A este respecto, 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 imponiendo 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. En este sentido, el intercambio de datos entre empresas es un mercado incipiente que seguirá creciendo a medida que las empresas de todos los sectores avanzan hacia modelos de negocio basados en datos. Lo mismo se aplica al intercambio de datos entre el sector privado y la Administración Pública.

Así, lo importante en este momento 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 último, este derecho debería **aplicarse 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.

Además, en este mismo párrafo 1, la referencia al uso de datos para “*el bien común*” debería definir de manera más concreta a que se refiere por bien común en el entorno digital, así como establecer criterios más claros y definidos.

Por estas razones, proponemos la exclusión de los datos del sector privado del párrafo 1.

B) Punto 2, reutilización de datos para la investigación

En este punto, consideramos que el foco debería ponerse en los puntos señalados en el informe del grupo de expertos convocado por la Comisión Europea a este respecto, *Towards a European Strategy on Business-to-Government data sharing for the public interest*². Más concretamente:

- El apartado 2.2.3 del informe desarrolla una serie de incentivos para el sector privado en relación, entre otros, con el retorno de costes, desgravaciones fiscales, reconocimiento público, etc.
- El apartado 2.2.4 del informe, relativo a la fragmentación del marco regulatorio para la compartición de datos propone adaptar el marco legal para estas actividades, manteniendo la voluntariedad de la cesión para la mayoría de casos de uso. Concretamente, los criterios para evaluar este aspecto serían los mencionados en el primer punto de dicho apartado, sobre probabilidad y magnitud de los impactos positivos negativos en el uso de datos, urgencia del caso de uso, falta de alternativas sustitutivas, etc.

C) Punto 3, acceso a datos personales con fines de investigación

Para la reutilización de datos personales con fines de I+D+i, el apartado b) supedita la admisibilidad del tratamiento de dichos datos (personales o pseudonimizados) cuando (a) la naturaleza de la actividad lo requiera y se cuente con el consentimiento, o (b) cuando exista

² Recuperable en: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954

autorización expresa prevista en la ley. Esta redacción excede de lo fijado por la normativa de protección de datos.

La Carta vuelve omitir que la normativa de protección de datos establece toda una serie de bases legitimadoras adicionales, además del consentimiento y la ley, para esta finalidad, como puede ser el interés legítimo, el interés público, interés vital, etc., y presupone la compatibilidad de tratamientos posteriores para estos fines basados en la seudonimización.

El RGPD, en la práctica, lejos de restringir exhaustivamente el tratamiento de datos de salud y datos genéticos con fines de investigación científica, innovación y desarrollo, lo que hace es habilitar otro cauce por el que la legitimación puede discurrir puesto que el artículo 9.2 RGPD también contempla la posibilidad de que este tipo de tratamiento de datos se lleve a cabo cuando “es necesario con fines de archivo en interés público, fines de investigación científica o fines estadísticos”.

Adicionalmente, el mismo RGPD, en su artículo 89, ahonda sobre las garantías que se deben cumplir para el tratamiento de datos no fundamentado en el consentimiento. En concreto menciona el principio de minimización y la pseudonimización.

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 no prevén las limitaciones incorporadas en la Carta, y proponemos que se eliminen las siguientes referencias.

“3. Cuando se trate de datos personales:

a) Los datos podrán ser tratados con fines de investigación científica, innovación y desarrollo ~~previa anonimización.~~

b) ~~Únicamente 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. (...)~~

Adicionalmente, cabe deducir de la redacción de los apartados a) y b) que los datos sólo pueden utilizarse para la investigación científica una sola vez: (i) los datos personales pertinentes son anónimos; o (ii) la naturaleza de la actividad de investigación lo requiere y el tratamiento pertinente ha sido consentido o autorizado por la ley.

Teniendo en cuenta que muchas autoridades de protección de datos han sugerido que no pueden existir datos personales totalmente anónimos, tal disposición significaría esencialmente que toda investigación científica debe ser consentida o autorizada específicamente por la ley.

Tal disposición sería contraria al RGPD. El RGPD establece una serie de bases jurídicas para el tratamiento de los datos personales en relación con la investigación científica y no se limita a la obtención del consentimiento. Además, una disposición de ese tipo haría que muchas investigaciones científicas fueran muy poco prácticas o, en el peor de los casos, imposibles.

XX. Derecho a un desarrollo tecnológico y a un entorno digital sostenible

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 impulsarán 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.

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 medioambientales, han originado situaciones de imposibilidad o ralentización del despliegue de redes e infraestructuras, lo que impide el desarrollo tecnológico y digital. La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en su artículo 140, establece como principios generales de las relaciones interadministrativas, entre otros, coordinación y eficacia.

Por ello, sugerimos que se añada la siguiente mención en el párrafo 2 de este apartado: “2. Los poderes públicos, coordinada y eficazmente, impulsarán 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”.

XXI. Derecho a la protección de la salud en el entorno digital

1. Se reconoce el derecho de todas las personas al acceso a los servicios digitales de salud en condiciones de igualdad, accesibilidad y universalidad.

2. Los poderes públicos promoverán que la investigación y la tecnología contribuyan al logro de una medicina preventiva, predictiva, personalizada, participativa y poblacional.

2. El sistema de salud garantizará el desarrollo de sistemas de información que aseguren la estandarización, la interoperabilidad, el acceso y la portabilidad de la información del paciente.

3. El empleo de sistemas digitales de asistencia al diagnóstico, y en particular de procesos basados en inteligencia artificial no limitará el derecho a la libertad diagnóstica del personal facultativo.

4. Los entornos digitales de salud garantizarán el pleno respeto de los derechos fundamentales del paciente y en particular su derecho a ser informado y consentir en el tratamiento de sus datos personales con fines de investigación y en la cesión a terceros de tales datos cuando tal consentimiento sea requerido.

6. Los poderes públicos impulsarán el acceso universal de la población a los dispositivos tecnológicos desarrollados con fines terapéuticos o asistenciales.

Como sucede a lo largo de la Carta en múltiples apartados, el punto 4 también se refiere al **consentimiento como único fundamento jurídico** para permitir el tratamiento de datos personales con fines de investigación científica, lo que es contrario al RGPD.

XXIII. Derechos ante la Inteligencia artificial

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.

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.

A) **Apreciación general**

En primer lugar, en relación con el apartado XXIII en general, se prevé un reconocimiento de derechos de carácter general y alcance amplio, siendo de máxima importancia que se tenga en cuenta que la formulación de este derecho se debería hacer expresamente para los casos en los que la aplicación de tecnologías de IA tenga un **impacto en los derechos fundamentales de las personas**, al contrario de lo previsto en la redacción actual de aplicación general. En este sentido, se propone hacer la aclaración descrita a continuación:

*“En el desarrollo y ciclo de vida de los sistemas de Inteligencia Artificial **con un impacto en los derechos fundamentales**: [...]”*

Además conviene destacar la importancia de **evitar regular una tecnología en particular, sin especificar de qué servicios se trata**. Los derechos y obligaciones que se establezcan pueden ser muy relevantes para determinados servicios basados en IA cuando impacten negativamente sobre los derechos de las personas, pero irrelevantes y/o contraproducentes en otros casos en los que no concurra esta circunstancia.

En este contexto, destacamos los trabajos de la UE y el Consejo de Europa que han adoptado un **enfoque basado en el riesgo**. Es decir, se identifican los servicios de alto riesgo ("high risk") a los que se les aplicaría un régimen normativo determinado, frente a otros en los que se aplicarían otros enfoques como una autorregulación basada en principios éticos. Así, para la Carta en general, y este derecho en particular, 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.

Adicionalmente, el apartado XXIII **queda condicionado por el derecho a la limitación de localización y perfilado previsto también en la Carta, generando confusión sobre la aplicación prevalente de uno u otro derecho**. El perfilado es la técnica más utilizada en sistemas de inteligencia artificial y, sin embargo, este apartado XXIII de la Carta no viene a establecer las mismas limitaciones en materia de IA respecto a las establecidas para el perfilado. 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.

A este respecto, es imprescindible resolver las dudas y contradicciones que genera este apartado, a la vez que se respetan los principios rectores de la normativa vigente sobre el uso de estas tecnologías.

B) Punto 1, garantías en el desarrollo y ciclo de vida de los sistemas de IA

En relación con el **primer punto del apartado XXIII**, se hacen una serie de prescripciones que generan dudas e inseguridad jurídica. De una parte, se emplea **lenguaje prescriptivo**, i.e. "garantizar" o "asegurar" que, siguiendo comentarios anteriores, se considera poco adecuado en la medida en que el posible y futuro valor jurídico o programático de esta Carta no ha quedado suficientemente claro, creando así múltiples dudas al presunto destinatario de la misma. A este respecto, esta Carta no debería conducir a la creación de nuevas obligaciones para las partes

privadas o crear nuevas prohibiciones distintas a las previstas en la normativa europea y armonizada.

Por ello, convendría sustituir los términos "garantizar", "asegurar" o "se prohíbe" por una invitación a valorar el impacto y estudiar una posible regulación.

Por otra parte, el apartado a) del párrafo 1 establece una **prohibición absoluta de todo tipo de sesgo** sin tener en cuenta la posibilidad de que existan razones para discriminar positivamente, por ejemplo, para fomentar una mayor igualdad. **La atención de esta sección debería centrarse en el sesgo injusto** y, nuevamente, siempre que afecte a derechos fundamentales.

Adicionalmente, debe tenerse en cuenta el art. 22 GDPR, sobre *decisiones individuales automatizadas, incluida la elaboración de perfiles*, que ya regula esta cuestión con claridad y alcance suficiente. Por esta razón, debe valorarse especialmente la confusión e inseguridad que este apartado en su redacción actual genera y evitar que esta Carta aluda, directa o indirectamente, a una posible modificación del RGPD.

Por las razones ya expuestas, se propone la eliminación de la mención a la "discriminación algorítmica" y ceñirse únicamente a hablar de "discriminación".

Siguiendo con el punto 1 de este apartado XXIII, el apartado b) **establece que "se asegurarán la transparencia, auditabilidad, explicabilidad y trazabilidad" sin determinar el significado de estos conceptos** en la práctica. Así pues, en nuestra opinión estas exigencias deberían hacerse en función del caso de uso y bajo estándares y criterios homogéneos aún por definir. Para ello, sería necesario un modelo de requisitos por capas que parta de una evaluación de impacto potencial (como es la PIA a la privacidad) y que exonere de estos condicionantes --que siempre suponen un mayor esfuerzo y coste de desarrollo y control-- a las aplicaciones triviales sin impacto potencial.

En este punto proponemos la siguiente matización "Se asegurará un nivel adecuado de transparencia, auditabilidad (...)".

Además, en este mismo párrafo se hace referencia a la **"transparencia"**. En este sentido, cabe preguntarse qué formas de transparencia podrían llevar a un empoderamiento significativo de los usuarios. Si la inteligencia artificial desempeña un papel sustantivo en la toma de decisiones o interactúa directamente con las personas, puede informarse de ello al usuario mediante:

- Una indicación clara de la lógica general y los supuestos en que se basa un modelo de inteligencia artificial, en particular si están diseñados para su uso en entornos de alto riesgo.
- Una indicación de cualquier expectativa operativa que se tenga en cuenta al diseñar el sistema, como por ejemplo si se pretende que funcione de forma independiente o sujeto a supervisión humana.
- Cualquier limitación conocida en el empleo de la inteligencia artificial.

No se considera necesaria ni conveniente la obligación de proveer información adicional, no solo por la protección de los secretos empresariales y la propiedad intelectual del titular de la inteligencia artificial, sino también como protección contra usos o manipulaciones fraudulentas o maliciosas de los algoritmos que, en última instancia, afectan negativamente tanto a los usuarios como al titular de la tecnología.

En el mismo párrafo se hace referencia al término **“auditabilidad”**. No es claro si se refiere a una propiedad intrínseca de la tecnología o a la intención de establecer (más bien, *invitación* a establecer) obligaciones de auditoría periódica, interna o externa, a las organizaciones que elaboren o utilicen herramientas de inteligencia artificial.

Finalmente, el apartado c) del punto 1 contiene referencias a **“la accesibilidad y la usabilidad”** que pueden leerse como un “derecho” a acceder a los servicios relacionados con la inteligencia artificial. Las empresas privadas que usan inteligencia artificial no tienen actualmente la obligación legal de garantizar el acceso o el uso por parte de todos; ese acceso o uso puede estar válidamente sujeto a decisiones de negocio. Además, el uso puede estar vinculado a la responsabilidad civil o contractual asociada, cuyo alcance excede a la Carta.

C) Punto 2, toma de decisiones automatizadas

El punto 2 del apartado XXIII hace referencia a ser objeto de **decisiones basadas en procesos de decisión automatizada**, cuestión ya prevista en el artículo 22 del RGPD. **Sin embargo, lo previsto en esta Carta excede lo establecido en el RGPD**, puesto que el Reglamento limita el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado cuando ésta produzca efectos jurídicos en él o le afecten significativamente de modo similar. No obstante, la Carta incluye expresamente las decisiones que empleen procedimientos de inteligencia artificial, excediéndose de lo previsto en el artículo 22.1 del RGPD.

Por esta razón, respecto al segundo punto, se propone su eliminación parcial.

D) Punto 3, obligación de información y asistencia

El punto 3 del apartado XXIII hace referencia a la **obligación de "informar a los individuos sobre el uso de los sistemas de inteligencia artificial que se comunican con los seres humanos utilizando el lenguaje natural en todas sus formas"**. Esta previsión se considera **demasiado amplia, lo que la puede tornar en innecesariamente gravosa**. Además, cabe recordar que los principios establecidos por la OCDE sobre la Inteligencia Artificial establecen que esta obligación sólo debe surgir cuando el sistema de inteligencia artificial tenga por objeto hacerse pasar por seres humanos.

Análogamente, el requisito absoluto de que **"se garantizará en todos los casos la asistencia de un ser humano a petición de la persona interesada"** no necesariamente generará mayor seguridad para los ciudadanos y, sin embargo, supondrá un requisito absoluto con graves consecuencias negativas para las empresas.

Respecto a esta misma obligación de asistencia, **debería preverse que la misma esté ponderada según la naturaleza del servicio, el riesgo inherente del mismo y el eventual impacto que pueda tener sobre el derecho de la persona**. De este modo, sería necesario incluir la distinción de los riesgos del uso de la Inteligencia Artificial puesto que cada uso no impactará de igual modo a las personas. Asimismo, cabe recordar, que actualmente existen una gran variedad de servicios que mejoran la eficacia de sus prestaciones gracias al uso de la IA, con una mayor personalización, sin que ello repercuta negativamente sobre los derechos de las personas.

E) Punto 4, manipulación o perturbación de la voluntad

En el contexto de esta Carta, el término "manipular" se ha empleado únicamente en otra ocasión, directamente vinculada a la publicidad, generando el fundado temor de que estas disposiciones puedan equivaler a la **prohibición de facto de cualquier sistema de publicidad que utilice un sistema de IA**, lo que sería absolutamente inaceptable. De la misma forma, en este punto 4, se considera que **establecer prohibiciones en términos absolutos debe ser un ejercicio llevado a cabo con la máxima cautela y prudencia**, especialmente en relación con un campo tan prometedor y en desarrollo como la IA. Cualquier prohibición general debe ser evaluada

cuidadosamente. En este sentido, la terminología “manipular” o “perturbar” la voluntad del individuo (visto además en el contexto publicitario) se considera imprecisa.

En este punto, consideramos que la propuesta es muy imprecisa y sería conveniente mayor claridad para evitar interpretaciones erróneas.

XXIV. Derechos digitales en el empleo de las neurotecnologías

1. Las condiciones, límites y garantías de implantación y empleo en las personas de las neurotecnologías serán reguladas por la ley con la finalidad de:

- a. Preservar la identidad individual como conciencia de la persona sobre sí misma.*
- b. Garantizar la autodeterminación individual, soberanía y libertad en la toma de decisiones.*
- c. Asegurar la confidencialidad y seguridad de los datos obtenidos o relativos a sus procesos cerebrales y el pleno dominio y disposición sobre los mismos.*
- d. Ordenar el uso de interfaces persona-máquina susceptibles de afectar a la integridad física o psíquica.*
- e. Asegurar que las decisiones y procesos basados en neurotecnologías no sean condicionadas por el suministro de datos, programas o informaciones incompletos, no deseados, desconocidos o sesgados, o por intromisión en conexiones neuronales.*

2. Para garantizar la dignidad de la persona, la igualdad y la no discriminación, y de acuerdo en su caso con los tratados y convenios internacionales, la ley regulará aquellos supuestos y condiciones de empleo de las neurotecnologías que, más allá de su aplicación terapéutica, pretendan el aumento cognitivo o la estimulación o potenciación de las capacidades de las personas.

Las tecnologías desarrolladas en este apartado se encuentran en una **fase muy temprana de desarrollo**, sin existir aún referencias ni información sobre el impacto de las mismas. En este sentido, sería más prudente abordar una **evaluación de impacto** inicial de dichas tecnologías antes de avanzar en el establecimiento de principios rectores, obligaciones o derechos en esta Carta que, como se ha dicho en repetidas ocasiones, tiene un valor jurídico o programático que no está claro y que está generando gran confusión. Hacerlo de otro modo supone el riesgo de impactar negativamente el desarrollo de estas nuevas tecnologías, algo totalmente desaconsejable en esta fase temprana.

XXV. Garantías de los derechos en los entornos digitales

- 1. Sin perjuicio de lo dispuesto en la legislación sectorial específica, todas las personas tienen derecho a la tutela administrativa y judicial de sus derechos en los entornos digitales.*
- 2. Cuando la lesión de tales derechos, o el daño causado, produzca sus efectos en territorio español podrá invocarse la garantía de estos derechos por la autoridad administrativa o el órgano jurisdiccional competente en España.*
- 3. Se promoverán mecanismos de autorregulación regulada y procedimientos de resolución alternativa de conflictos.*
- 4. Los poderes públicos evaluarán las leyes administrativas y procesales vigentes a fin de examinar su adecuación al entorno digital y propondrán en su caso la realización de reformas oportunas en garantía de los derechos digitales.*

La redacción de este apartado da lugar a inseguridad jurídica debido al **conflicto derivado entre los derechos previstos en la Carta y la jurisdicción**. La mayor parte de derechos contemplados en la Carta conllevan el tratamiento de datos personales, que se rige por el RGPD y las normas de ventanilla única, cuestiones no previstas en este apartado. A este tenor, es importante recordar que uno de los principales impulsores del proceso de reforma de la protección de datos en Europa fue precisamente el deseo de lograr una mayor claridad y coherencia tanto de la reglamentación como de la aplicación de la protección de datos en toda la Unión; una de las formas en que el RGPD trata de lograr esa uniformidad es introduciendo el principio de la ventanilla única.

Adicionalmente, este apartado prevé determinadas disposiciones que se consideran apropiadas en forma y tono, por ejemplo, "*los poderes públicos evaluarán...*", "*se promoverán [x]*", etc. Sin embargo, al mismo tiempo introduce **disposiciones prescriptivas**. Es el caso del párrafo 2, que atribuye a los tribunales españoles la competencia internacional en materias ya reguladas por el RGPD, como ya se ha dicho, y por varios tratados internacionales, por ejemplo, en materia de daños extracontractuales. Tratándose de un asunto muy complejo y armonizado internacionalmente, es aconsejable no abordarlo en un documento como la Carta cuyo valor jurídico o programático no queda suficientemente claro.