

Comentarios al documento para consulta pública

“Carta de Derechos Digitales”

20 de enero de 2021

El documento sometido a consulta pública, “Carta de Derechos Digitales” (en adelante, LA CARTA), responde a la necesidad de dar cobertura al nuevo escenario en el que las tecnologías de la información y las comunicaciones -en un lenguaje más actual, “lo digital”- lo impregnan todo.

El texto no tiene carácter normativo, sino que parece responder a una declaración de intenciones con un compromiso claro de actuación de los poderes públicos. Parte de un conjunto de valores que, dentro del marco constitucional, han inspirado la configuración de una serie de derechos que se ofrecen agrupados como derechos de libertad (protección de datos, derecho a no ser localizado o perfilado, derecho a la seguridad digital, etc.); derechos de igualdad (incluidos los menores, las personas con discapacidad y los mayores); derechos de participación y conformación del espacio público (neutralidad de Internet, libertad de expresión e información o educación digital); derechos del entorno laboral y empresarial (ámbito laboral y empresa en el entorno digital); y derechos digitales en entornos específicos (como la investigación, la inteligencia artificial o el entorno digital sostenible).

El Consorcio Red Alastria (en adelante, ALASTRIA), que opera sin ánimo de lucro y se define como impulsor de la economía digital a través de la promoción del uso de tecnologías descentralizadas, tiene como objetivo fundamental crear una comunidad integrada por todo tipo de organizaciones, públicas y privadas, así como expertos individuales, con el objetivo de favorecer la implantación, normalización, protección y utilización de las tecnologías de registro distribuido (DLT, por sus siglas inglesas), en particular Blockchain, tanto a nivel nacional como internacional. ALASTRIA no presta servicios de Blockchain, por lo que no asume responsabilidad por la gestión o el funcionamiento de redes DLT productivas o en las que se presten servicios a terceros.

ALASTRIA puede ayudar a la puesta en marcha y aplicación efectiva de algunos de los derechos que recoge LA CARTA, en los siguientes términos:

Modelo de identidad digital: Dentro de sus competencias estatutarias, con la finalidad de devolver al ciudadano el control de sus datos personales y facilitar la materialización de los derechos arriba referidos, ALASTRIA ha impulsado el desarrollo de la “Identidad Alastria” (ID_Alastria), un modelo de identidad digital autogestionado, propuesto para su uso en servicios digitales y convertido hoy en norma ‘de iure’, a través de un proyecto liderado por la propia ALASTRIA para UNE, el organismo nacional español de normalización, quien el pasado 21 de diciembre de 2020 lo hacía público como norma “UNE 71307-1:2020. Tecnologías Habilitadoras Digitales. Modelo de Gestión de Identidades Descentralizadas sobre Blockchain y otras Tecnologías de Registros Distribuidos. Parte 1: Marco de referencia”.

El modelo se halla inspirado en el concepto de identidad “autosoberana” (del inglés “Self Sovereign Identity”, SSI) y, al mismo tiempo, ha servido de inspiración a la iniciativa “European Self-Sovereign Identity Framework” (ESSIF), impulsada por el European Blockchain Partnership (EBP) dentro del programa “European Blockchain Services Infrastructure” (EBSI).

El modelo resulta de especial interés en tanto que puede facilitar la gestión y garantía de todos aquellos derechos propuestos en LA CARTA que tienen como elemento conector a la privacidad y a la seguridad digital de las personas. A continuación, pasan a enumerarse los referidos derechos:

-. Derecho a la protección de datos. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 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, **a conocer los fines concretos para los que se usan, a recibirlos en un formato digital fácilmente procesable** y a obtener su rectificación.

-. Derecho a la identidad en el entorno digital. Se reconoce el derecho a la propia identidad en el entorno digital. La identidad no podrá ser alterada, controlada o manipulada por terceros contra la voluntad de la persona. **La identidad digital permanecerá en todo momento bajo el control directo de la persona, quien podrá gestionarla con plena autonomía**. Se establecerán las garantías que permitan preservar y controlar la propia identidad en el entorno digital.

-. Derecho al pseudonimato. De acuerdo con las posibilidades técnicas disponibles, los entornos digitales permitirán el acceso en condiciones de pseudonimidad. **El acceso anónimo o pseudónimo a infraestructuras descentralizadas, tanto en lectura como en escritura, se facilitará de forma que impida la reidentificación de las personas, mediante medidas técnicas y/o legales**. El diseño de la pseudonimidad asegurará la posibilidad de reidentificar a las personas en los casos y las garantías previstas en el ordenamiento jurídico.

-. Derecho a no ser localizado y perfilado. 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. **El acceso anónimo o pseudónimo a infraestructuras descentralizadas, tanto en lectura como en escritura, se facilitará de forma que impida el perfilado de las personas, mediante medidas técnicas y/o legales**. Solo serán posibles los tratamientos de información personal con el consentimiento de la persona afectada o en los casos y con las garantías previstos en las leyes.

-. Derecho a la seguridad digital. Toda persona tiene derecho a la seguridad en el entorno digital. Los poderes públicos **adoptarán y promoverán las medidas necesarias para minimizar la fragilidad digital que acompaña la actual corriente digitalizadora; y lo hará en colaboración con las empresas tecnológicas y con la complicidad de los usuarios concernidos (ciudadanos individuales, empresas no tecnológicas/especializadas y resto de entidades)**.

-. Derecho a la herencia digital. 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. 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 CCAA 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.

-. Derecho a la participación ciudadana por medios digitales. De acuerdo con las leyes, se impulsarán los 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. Los procedimientos de participación ciudadana garantizarán condiciones de igualdad sin discriminaciones ni exclusión de personas, con sujeción al ordenamiento jurídico.

-. Derechos digitales de la ciudadanía en sus relaciones con las Administraciones públicas. Se reconoce el derecho de igualdad en el acceso a los servicios públicos y en las relaciones digitales con las Administraciones públicas. El principio de transparencia y de reutilización de datos de las AAPP guiará la actuación de la Administración digital, de conformidad con la normativa sectorial. 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 LA CARTA.

Transparencia algorítmica: De cara al desarrollo y ciclo de vida de los sistemas de Inteligencia Artificial, la propuesta de Carta de Derechos establece la prohibición de toda discriminación algorítmica cualquiera que fuera su origen o causa y el aseguramiento de su transparencia, auditabilidad, explicabilidad y trazabilidad. Se impone además el deber de 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, garantizándose en todo caso la asistencia por un ser humano a solicitud de la persona interesada. LA CARTA prohíbe el uso de sistemas de Inteligencia Artificial dirigidos a manipular o perturbar la voluntad de las personas, particularmente los relativos a los procesos electorales y la participación política y cualesquiera otros que afecten a los derechos fundamentales.

A efectos de garantizar la transparencia en los términos indicados, la tecnología blockchain puede resultar de gran utilidad facilitando su auditabilidad, explicabilidad y trazabilidad no alterable. Blockchain puede ser asimismo una herramienta estratégica y fundamental de cara a asegurar la transparencia que se propone en LA CARTA como un elemento transversal a todos los derechos y libertades, además de asegurar el cumplimiento del artículo 9 del 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 (RGPD), que establece que el usuario debe ser informado por el responsable de todas las circunstancias relativas al tratamiento de sus datos “en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo”.

Adicionalmente, merece la pena detenerse en algunas partes de LA CARTA para realizar comentarios específicos que puedan servir a la consecución de sus objetivos:

Derecho a la protección de datos: La entrada en vigor del RGPD y la actualización de la normativa española en esta materia a través de la ya citada Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales han supuesto una profundización relevante del esquema de protección que hasta entonces amparaba al tratamiento de datos personales.

En la actualidad, ambas normativas establecen un marco regulatorio detallado aplicable al tratamiento de datos personales y los derechos aparejados que corresponden a las personas cuyos datos son tratados. Con el objetivo de asegurar que el lector tiene las herramientas necesarias para entender el contenido del derecho en su integridad, podría ser recomendable incluir, en el apartado primero del artículo dedicado al derecho a la protección de datos personales, una referencia a este marco normativo.

Por otro lado, la aplicación de este nuevo marco normativo ha supuesto en España la equiparación formal entre el consentimiento y el resto de bases de legitimación que pueden justificar el tratamiento de datos personales. Tras la aplicación del RGPD, el consentimiento deja ser la regla general para justificar el tratamiento y se convierte en una base de legitimación más, que funciona al mismo nivel que otras bases de legitimación.

La redacción actual del apartado segundo del derecho a la protección de datos personales podría no estar dejando constancia clara de esta equiparación e incluso apuntar a la noción ya obsoleta de que otras bases de legitimación actúan sólo como vía de excepción al consentimiento, en consonancia con la normativa derogada de protección de datos personales. En consecuencia, podría resultar interesante una redacción que prescinda de la referencia al consentimiento y se remita con carácter general a cualquier base de legitimación.

Finalmente, el mismo apartado menciona los derechos de acceso y rectificación como los derechos que corresponden a las personas en relación con el tratamiento de sus datos personales. Asimismo, merece la pena destacar que el RGPD otorga a los interesados

derechos distintos de los dos incluidos, resultando que la mención de los otros derechos reconocidos en el RGPD devenga no sólo interesante, sino también necesaria, en aras a garantizar la mayor coherencia posible.

Derecho a la identidad en el entorno digital y derecho al pseudonimato: la identidad digital es una extensión de la identidad física y afecta al desarrollo de la personalidad. La identidad digital, no obstante, no tiene por qué coincidir con la identidad física, ya que una misma persona puede funcionar a través de varias identidades en el entorno digital.

La creciente importancia de la identidad digital se hace patente si atendemos a la consolidación del modelo de Web 2.0 o Web social, manifestado en la expansión de las funcionalidades sociales de los servicios digitales; no sólo las redes sociales ofrecen un entorno en el que compartir quién es cada uno, sino que servicios de todo tipo en Internet permiten opinar, evaluar e interactuar con otras personas. La nueva Web la “escriben” personas que no se identifican necesariamente por sus atributos de identificación clásicos. Por esto, el control de la identidad en el entorno digital no debe limitarse a la identidad física en cuanto que identificación digitalizada de las personas, sino que debe claramente extenderse a la identidad digital, entendida como cualquier identidad vinculada a una persona en entornos digitales, a la que se pueden vincular atributos de personalidad muy diversos.

Merece la pena plantear la posibilidad, en consecuencia, de utilizar una redacción que asegure que el control de la propia identidad en el entorno digital se extiende a cualquier identidad que represente a una persona en este entorno y no sólo a aquella identidad que represente la identidad física de la persona.

El derecho a la identidad digital debe preservar el control directo de la misma por parte de la persona, asegurando su autonomía. A tal fin, se potenciará el uso de estándares para facilitar la existencia de aplicaciones y servicios interoperables, impulsando una regulación y normalización neutrales tecnológicamente, es decir, independientes de una tecnología concreta y, por tanto, abiertas a nuevas (futuras) tecnologías de registro distribuido.

El derecho al pseudonimato guarda una estrecha relación con el concepto de identidad digital que se acaba de exponer. La identidad pseudónima es parte de la identidad digital de las personas y merece, no sólo que se promueva su uso, sino que se proteja a través de otorgar mecanismos de control a las personas que corresponda. Al hilo de esta reflexión, cabría plantearse si este derecho funciona más como una faceta del derecho a la identidad en el entorno digital, que como un derecho autónomo.

El pseudonimato, por otro lado, no puede entenderse plenamente sin referencia a la normativa de protección de datos personales. Debe recordarse que las técnicas de pseudonimización no despersonalizan el dato, que mantiene, una vez pseudonimizado, su naturaleza personal y, por tanto, queda amparado por la protección que otorga la normativa de protección de datos personales.

La naturaleza personal de los datos pseudonimizados no es obvia, especialmente para agentes en industrias que basan su actividad prioritariamente en el tratamiento de datos pseudonimizados, como podría ser el ecosistema publicitario digital. Por esta razón, podría ser aconsejable hacer referencia directa a esta normativa al tratar el derecho al pseudonimato.

Derecho a no ser localizado y perfilado: la utilización de datos personales para la creación de perfiles es una realidad cada vez más presente, especialmente a raíz de la aparición de nuevas tecnologías en el campo del tratamiento automatizado e inteligente de datos personales, como la computación en nube, la utilización de funcionalidades de inteligencia artificial o de tratamiento masivo.

La creación de perfiles se utiliza en muchas ocasiones con el fin de tomar decisiones automatizadas. Así se manifiesta, por ejemplo, en las industrias bancaria y financiera, en

relación con la asignación de puntuaciones (*scoring*) basadas en el perfil de riesgo de la persona para evaluar la concesión de créditos u otros instrumentos financieros. También vale de ejemplo la industria publicitaria digital, que personaliza de forma automática la publicidad que ven los usuarios que navegan por la web en función del perfil que han creado del usuario, basado en su historial de navegación y características observadas del usuario. Estas decisiones pueden llevar aparejado un efecto jurídico o afectar a las personas significativamente de modo similar, determinando, en caso de producir estos efectos, un régimen de protección reforzado para aquellas.

En cualquiera de los casos anteriores, el perfilado resulta, con asiduidad, una técnica que antecede a la toma de decisiones individuales automatizadas. El propio perfilado es una forma de decisión individual automatizada, según queda manifestado por el RGPD.

El hecho de que el RGPD vincule de manera tan estrecha estas dos cuestiones puede servir de referencia a la hora de enfocar la definición de este derecho en LA CARTA. Así, la referencia al perfilado se podría acompañar de una mención a la toma de decisiones individuales automatizadas, su relación con el perfilado y el hecho de que existe un régimen jurídico reforzado en estos casos.

Nuevamente, la referencia al marco normativo de protección de datos personales puede servir para garantizar la información más completa del lector y un enfoque integrado a esta materia.

Derecho a la educación digital: no cabe pensar en educar a una sociedad para la Ciudadanía Digital sin ayudarla a que tome conciencia de los peligros inherentes al entorno digital. Cualquier impulso que se adopte desde la vertiente formativa habrá de contemplar, junto al desarrollo y robustecimiento de las capacidades digitales, aquellas otras que, cuando menos, contribuyan a aumentar el grado de sensibilización sobre la fragilidad digital que, como ya se ha señalado con anterioridad, acompaña al proceso digitalizador.

Cabe, por todo ello, sugerir también en este punto ampliar la redacción recogida en LA CARTA hacia la educación en conceptos vinculados a la seguridad digital como la ciberseguridad y la ciberresiliencia.

Servicio de acceso a infraestructuras blockchain:

Se impulsará la definición de un servicio de acceso a Blockchain, con un conjunto claro de derechos y obligaciones.

En relación con la identidad digital, los prestadores del servicio de acceso a blockchain, garantizarán el mantenimiento de las condiciones de anonimato y pseudonimato de los usuarios. El “prestador del servicio de acceso a blockchain” no debe utilizar la información operativa del servicio para reidentificar o perfilar al usuario. Estas obligaciones no dependen de que el servicio sea gratuito o de pago.

Finalmente, desde ALASTRIA se considera interesante incorporar a LA CARTA las recomendaciones de la OCDE en el desarrollo de aplicaciones e infraestructuras de registro distribuido o Blockchain:

1. Se deberán establecer mecanismos para evaluar y garantizar la coherencia de las aplicaciones e infraestructuras Blockchain con los derechos digitales, así como con los requisitos políticos, legales y reglamentarios vigentes en cada momento; incluso en el caso de las infraestructuras más descentralizadas que operan globalmente, más allá de las fronteras del Estado.

2. Los promotores de infraestructuras Blockchain deben garantizar que sus marcos de gobernanza sean transparentes y estén claramente definidos. Con este fin deberán:
 - a) garantizar un enfoque inclusivo en la gobernanza de las infraestructuras Blockchain, incluida la elaboración de medidas para asegurar su integridad y seguridad, en particular en el caso de las Blockchain más descentralizadas;
 - b) promover entre las personas y organizaciones que desplieguen servicios en las infraestructuras Blockchain el respeto de los derechos digitales de los ciudadanos en todo momento y el cumplimiento normativo adecuado;
 - c) realizar auditorías iniciales y periódicas en relación con el cumplimiento de estos principios; y,
 - d) divulgar cualquier cambio en los marcos de gobernanza de estas infraestructuras de manera responsable y oportuna.
3. Se deberá promover la interoperabilidad de las Blockchain, promoviendo estándares abiertos, integrándose con otras infraestructuras, de registro distribuido o no, para apoyar el desarrollo socioeconómico del Estado, fomentar la competencia y reforzar el control de los ciudadanos sobre sus datos personales.
4. Se deberá favorecer la comprensión de los riesgos de seguridad relacionados con esta tecnología, incluidos los relacionados con la gestión de la identidad digital, el control de acceso y las infraestructuras habilitantes. En este sentido se deberá asumir la responsabilidad de una gestión prudencial de estos riesgos, respaldada por la continuidad de las operaciones y acorde con las normas de seguridad digital pertinentes, entre otras cosas, actuando de manera transparente, por ejemplo, presentando informes oportunos sobre incidentes de seguridad. Debido a las características específicas de muchas Blockchains, en particular a la inmutabilidad de sus registros, su permanencia y naturaleza distribuida, sólo deben recopilarse y almacenarse datos identificables personalmente cuando sea estrictamente necesario para el propósito previsto de la aplicación Blockchain y con pleno respeto a los derechos digitales ciudadanos.
5. Se deberán promover la educación de la ciudadanía y la generación de capacidades especializadas en esta tecnología:
 - a) fomentando la comprensión de las tecnologías blockchain y sus posibles aplicaciones y limitaciones, incluso con relación a las infraestructuras de registro distribuido más descentralizadas; e,
 - b) impulsando oportunidades para la capacitación y desarrollo de las aptitudes pertinentes que eviten que la tecnología desplace o afecte negativamente a la empleabilidad de los ciudadanos.

El presente texto ha sido elaborado por algunos de los miembros del Comité Legal de Alastria, de su Comisión de Identidad y de su Comisión de Resiliencia, habiendo sido validado por un conjunto de vocales de su Junta Directiva. Asimismo, la asociación Data Economy España quiere manifestar expresamente su adhesión al texto.