

A la Secretaría de Estado de Digitalización e Inteligencia artificial

Ministerio de Asuntos Económicos y Transformación Digital

En relación con la “**Consulta pública para la elaboración de una Carta de Derechos Digitales**” cuyo plazo está abierto hasta el 20 de diciembre de este año, formulamos las alegaciones siguientes:

PRIMERA: Sobre la necesidad de clarificar la naturaleza jurídica de la Carta y su encaje en la normativa ya vigente

La “Introducción” que acompaña a la carta afirma que “La Carta no tiene carácter normativo”, sino que su objetivo es “reconocer los [...] retos de aplicación e interpretación que la adaptación de los derechos al entorno digital plantea”, así como “sugerir principios y políticas referidas a ellos en el citado contexto”. También, “proponer un marco de referencia para la acción de los poderes públicos”. Si la Carta no tiene carácter normativo no se termina de entender por qué se denomina carta “de derechos”. Un derecho es algo que su titular puede hacer valer o reclamar porque el ordenamiento jurídico le reconoce esa facultad; un derecho sin contenido normativo difícilmente puede ser considerado un derecho en sentido estricto.

Es conveniente que el título de un documento refleje el contenido del mismo. Y si lo que la Carta pretende es, como la propia Introducción señala, reconocer los retos que supone el entorno digital en materia de derechos, y/o establecer principios de actuación o pautas de interpretación, no habría ningún problema en que la carta se titulara, por ejemplo: “Pautas de interpretación de los derechos reconocidos en el ámbito digital” o “Objetivos en materia de derechos fundamentales en el ámbito digital”, o algo similar.

Es más, no sólo no sería problemático cambiar el título por alguno de estos otros, sino que sería incluso preferible, ya que evitaría confusiones. Porque el ordenamiento jurídico español ya reconoce numerosos derechos en el ámbito digital, especialmente – aunque no sólo – en la LO 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. Y los derechos que la nueva Carta enumera se solapan en buena medida con los ya existentes (un ejemplo de esto último se expone como segunda alegación en este escrito). Esto hace surgir muchas dudas sobre si se ha querido regular lo mismo otra vez (en este caso, ¿por qué repetir?), si lo que se quiere es ir más allá (pero entonces, ¿por qué sin carácter normativo?), si sólo se quieren dar pautas interpretativas de los derechos ya reconocidos en leyes ya vigentes (entonces, ¿por qué no decirlo expresamente así?), o si no se trata de ninguna de estas pretensiones sino de alguna otra. En resumen, sería necesaria mayor claridad sobre la naturaleza jurídica de la Carta, y su encaje en la estructura de los derechos ya reconocidos por las normas vigentes.

SEGUNDA: Sobre el apartado VI, Derecho a la seguridad digital. Necesidad de especificar su contenido.

El contenido de dicho derecho en la redacción actual del documento que se ha abierto a consulta pública es la siguiente: “1. Toda persona tiene derecho a la seguridad en el entorno digital.” No se especifica en qué consiste dicha seguridad digital. Lo único que se añade en el número 2 de este apartado es que “2. Los poderes públicos adoptarán y promoverán las medidas necesarias

para garantizar aquélla, en colaboración siempre con las empresas tecnológicas y con los usuarios.”

Si no se especifica qué es la seguridad digital, esta expresión puede entenderse en dos sentidos distintos. El primero, el del art. 82 de la LO 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, según el cual el derecho a la seguridad digital consiste en 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.” Es un derecho que tienen los usuarios, es decir, los ciudadanos, a que las comunicaciones que transmitan sean seguras. Lo cual significa que se respete la confidencialidad de las mismas (es decir, su secreto frente a terceros) y su integridad (que no sufran manipulaciones). Si es esto lo que la Carta quiere garantizar en el apartado VI, estimamos que debe especificarse, ya sea en los mismos términos del art. 82 LO 3/2018 o incluso en otros más concretos que hagan referencia expresa a estas dimensiones esenciales de confidencialidad e integridad.

Si no se hace así, se corre el riesgo de que la referencia a la seguridad digital pueda interpretarse en un sentido totalmente diferente: el de ciberseguridad, o seguridad digital como uno más de los componentes de la seguridad nacional (en el sentido en que define esta última la LO 36/2015, de Seguridad Nacional). Entendido en este segundo sentido, el apartado VI de la Carta estaría proclamando un derecho de los ciudadanos a ser protegidos en el ámbito digital frente a amenazas o peligros para sus bienes personales o patrimoniales que puedan provenir de terceros. A nuestro juicio es absolutamente desaconsejable reconocer un derecho de este tipo, o permitir que la redacción inespecífica del actual apartado VI de la Carta pueda dar pie a esta interpretación, por dos razones.

La primera, que en el entorno analógico no existe un derecho a la seguridad con ese contenido. Y si la pretensión de la Carta, como se afirma en las “Consideraciones previas” que la acompañan, no es descubrir nuevos derechos fundamentales para el ámbito digital, sino concretar cómo deben operar en el entorno y los espacios digitales los derechos ya reconocidos para el mundo físico, no existe en este último un Derecho a la seguridad que hubiera que proyectar también en el entorno digital. Cuando el art. 17 de la Constitución Española proclama que todos tienen derecho a la libertad y la “seguridad”, a lo que se refiere es a asegurar la libertad personal frente a las injerencias arbitrarias del Estado, y así lo ha interpretado unánimemente la doctrina. Por supuesto que proporcionar a los ciudadanos seguridad, entendida como protección frente a agresiones de terceros, es una función esencial del Estado. Pero eso no significa que tenga la naturaleza jurídica de derecho fundamental.

En segundo lugar, no sería bueno que en el mundo digital se introdujera un derecho de este tipo. Con el pretexto de garantizar la “seguridad” nacional o pública en el ámbito digital frente a graves amenazas (terrorismo, por ejemplo), los poderes públicos (con la colaboración muchas veces imprescindible de las empresas tecnológicas) pueden pretender llevar a cabo acciones que vulneran muchos de los derechos reconocidos en la Carta. La defensa del ciudadano frente a estas acciones es, precisamente tener garantizados derechos que le protegen frente a esas intromisiones: el secreto de las comunicaciones, la intimidad de los datos personales, acceso a los datos, no elaboración de perfiles, etc. Si se introduce un difuso “derecho a la seguridad digital” de contenido indefinido, su defensa podría ser esgrimida por el poder público como una coartada para vulnerar muchos de los derechos digitales que la propia Carta pretende tutelar.

Por todo ello, consideramos necesario que el contenido del derecho a la seguridad digital que proclama el apartado VI de la Carta se explicita, y se haga en el sentido del art. 82 de la LO 3/2018.

TERCERA: Sobre el apartado XXIII, Derechos ante la Inteligencia artificial. Debe incluirse como derecho del ciudadano el de acceder al código fuente de los algoritmos o programas informáticos que usen las Administraciones Públicas para tomar decisiones sobre la aplicación de las normas a los ciudadanos.

El número 2. del apartado XXIII de la Carta establece que las leyes pueden permitir en algunos casos que se tomen decisiones que produzcan efectos jurídicos basadas únicamente en procesos de decisión automatizada, incluidas aquéllas que empleen procedimientos de inteligencia artificial. Y para tales casos se reconocen los derechos a: a) Solicitar una supervisión e intervención humana; y b) Impugnar las decisiones automatizadas o algorítmicas.

Sin embargo, esos derechos, y especialmente el de impugnar las decisiones automatizadas, serán inanes si no se reconoce el derecho del ciudadano a conocer cómo funciona el algoritmo: si no se sabe con arreglo a qué criterios se ha tomado una decisión automatizada, cuáles son los factores que tiene en cuenta la máquina, qué peso les da y cómo los combina, ¿cómo puede argumentarse en un eventual recurso que dicha decisión es equivocada?

Cuando un funcionario persona física toma una decisión, el ciudadano afectado tiene derecho a acceder a la motivación, en la que se exponen los argumentos y criterios aplicados. Cuando no lo hace una persona física sino un algoritmo de manera automatizada, el equivalente al derecho a obtener una decisión motivada es el acceso a la forma en la cual el algoritmo ha sopesado y combinado determinados factores. El acceso al código fuente, en definitiva.

El argumento de la necesaria defensa de la propiedad intelectual no es aplicable en estos casos: las normas legales no son objeto posible de propiedad intelectual, y tampoco las decisiones judiciales ni administrativas. Cuando un juez dicta una sentencia aplicando una norma a un caso la motivación que contiene es, sin duda alguna, una creación original de su intelecto, pero la ley no la considera susceptible de propiedad intelectual porque ello dejaría en la absoluta indefensión al ciudadano. Lo mismo ocurre cuando no es un juez sino un funcionario administrativo el que resuelve un expediente. Y lo mismo debe ocurrir cuando lo haga un algoritmo.

Cuando los algoritmos sopesan y combinan de manera automatizada los criterios de los cuales depende la comprobación del supuesto de hecho de la norma, y en función de ello determinan o recomiendan la decisión jurídica aplicable, operan, materialmente, como normas jurídicas. Se ha argumentado, a nuestro juicio con razón, que los algoritmos son reglamentos (Boix Palop, A.: “Los algoritmos son reglamentos”, Revista de Derecho Público: Teoría y Método. Vol. 1, 2020 pp. 223-270, accesible online en <http://www.revistasmarcialpons.es/revistaderechopublico/article/view/33/49>), y por tanto hay que aplicarles las mismas garantías previstas para la elaboración de normas reglamentarias: participación, publicidad, planificación normativa y evaluación ex ante y ex post; acceso público total; reconocimiento de las posibilidades de defensa y recurso, tanto respecto del acto aplicativo derivado del empleo del algoritmo como de su programación en sí misma considerada, ya sea en abstracto -recurso directo-, ya como consecuencia de su aplicación

concreta -recurso indirecto. Garantías todas ellas que son inherentes a todas las normas jurídicas propias de un Estado de Derecho.

Juan Carlos Carbonell Mateu (Catedrático de Derecho Penal, Universitat de València)
Lucia Martínez Garay (Profesora Titular de Derecho Penal, Universitat de València)
Javier Guardiola García (Profesor Titular de Derecho Penal, Universitat de València)
Antoni Llabrés Fuster (Profesor Titular de Derecho Penal, Universitat de les Illes Balears)
Antoni Gili Pascual (Profesor Titular de Derecho Penal, Universitat de les Illes Balears)
Clara Viana Ballester (Profesora Contratada Doctora de Derecho Penal, Universitat de València)
Jorge Correcher Mira (Profesor Ayudante Doctor de Derecho Penal, Universitat de València)
María Sánchez Vilanova (Profesora Ayudante Doctora de Derecho Penal, Universitat de València)
María José Galvis Doménech (Profesora Ayudante de Teoría de la Educación, Universitat de València)

Miembros del Proyecto de I+D “Derecho penal de la peligrosidad: tutela y garantía de los derechos fundamentales” (DER2017-86336-R)”, financiado por el Ministerio de Ciencia e Innovación – AEI – FEDER. Correspondencia: lucia.martinez@uv.es