

Somos una comunidad de personas independientes, diversas, interdisciplinarias, multisectoriales interesadas en el impacto social de las tecnologías digitales, especialmente la inteligencia artificial. Creemos que la tecnología puede ser un vector de modernización de procesos en entornos privados y públicos pero queremos asegurar que su despliegue se haga cumpliendo con los Derechos Humanos. Entre los integrantes de la comunidad hay personas expertas en ciencias de la computación, periodismo, Derechos Humanos, participación ciudadana, academia e impacto social de las tecnologías. Uno de los objetivos de la comunidad es asegurar que la ciudadanía participa en los procesos de diseño, seguimiento y evaluación de políticas relacionadas con el despliegue de tecnologías digitales, especialmente en el campo de la inteligencia artificial.

Sobre Proceso

Es necesario un énfasis en la participación ciudadana porque es una carta de los derechos de las personas. La ciudadanía debe y merece ser una parte necesaria de la creación de la carta de derechos. Esta carta es una proposición “transformadora”, pero la verdadera transformación empieza en el proceso.

El proceso de consulta pública basado en un canal unidireccional de comunicación es un proceso de participación ciudadana muy deficiente. Este mecanismo no permite una devolución a las personas participantes, no existe ningún mecanismo para adherirse a iniciativas de terceros ni ofrece ningún procedimiento para garantizar la trazabilidad de las aportaciones. Además, consideramos que se debería de haber realizado una buena campaña de difusión para generar en la ciudadanía conciencia y motivar de esta manera la participación mediante aportaciones para enriquecer la Carta. Además, solicitamos la publicación de todas las propuestas recibidas en la consulta pública.

Tampoco nos parece que haya habido transparencia acerca de las alegaciones del grupo de expertos, cuáles fueron sus intervenciones y recomendaciones y documentos de trabajo. Creemos que sería deseable la publicación de estos aspectos, de la misma manera que sería deseable la publicación de todas las aportaciones de la consulta pública.

Comentarios generales:

- ❖ Consideramos, de entrada, que una **carta sin un proceso de garantías legislativas no sirve de mucho**, ¿qué leyes acompañarán para poder defender su cumplimiento? Aún no siendo de mucha ayuda, si al menos se anuncia y se da a conocer, sirve para concienciar a la ciudadanía de que tiene unos derechos digitales"
- ❖ Creemos que la carta debería de ir acompañada de un **glosario**. Hay términos en los que no hay consenso como “Transformación digital”, “Dispositivo digital”, etc. Delimitar los marcos para cada concepto es deseable para entender los límites de la propia Carta.

Asuntos que la carta no aborda y que consideramos importantes:

- ❖ Se habla de que habrá programa de donantes de datos (no se habla de cómo funcionaría), pero **no de si habrá datos de fuente abierta**. ¿Quién podrá hacer uso de

esos datos: solamente las instituciones públicas, sólo por delegación/cesión de datos de las AAPP a entidades privadas u organizaciones?

- ❖ No se contemplan las **reparaciones (remedy) por decisiones automatizadas** que produzcan daño, perjuicio, o discriminación. No se tiene que especificar ya qué cosas concretas se harán, pero sí que es cierto que en tanto que documento declarativo, debería mencionar al menos la “intención”.
- ❖ Se habla mucho de monitoreo (segunda fase), pero no tanto de diseño (primera fase, esencial) ni de evaluación (tercera fase, esencial también).
- ❖ No se habla de **arquitectura institucional y territorial de competencias**: ¿Administración General del Estado, CC.AA., nivel municipal?
- ❖ No se habla de la **brecha rural**: se menciona una vez la “brecha territorial”, pero bajo la perspectiva de igualdad y no discriminación. Sin embargo, la brecha territorial no tiene por qué equivaler a brecha rural.
- ❖ Se menciona poco o nada de la robótica asistencial (residencias, gente mayor, gente con discapacidades, niños, etc).
- ❖ Falta de concreción sobre el acceso, recopilación y tratamiento de datos biométricos de personas en entornos privados y públicos.
- ❖ Falta de mención específica sobre el acceso, recopilación y tratamiento de datos biométricos de personas.

Comentarios por puntos:

[En azul los comentarios que hacemos respecto a los puntos de la carta]

CARTA DE DERECHOS DIGITALES

DERECHOS DE LIBERTAD

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.

Definición poco precisa de “Derechos Fundamentales y Libertades”. Si recurrimos a la literalidad de la palabra, entonces esta Carta garantizaría los derechos digitales de aquellos Derechos Fundamentales reconocidos de los arts.14-29 y 30.2 de la Constitución Española, pero no de aquellos derechos programáticos de carácter económico y social (que siguen a partir del art.30). Si la Carta quiere abrazar estos derechos programáticos de carácter social y económico (y no sólo los Dº Fundamentales), debería mencionarlo explícitamente.

Esto tiene consecuencias no sólo en cuanto a contenido, sino también en los propios mecanismos de protección jurídica ante la vulneración de estos derechos. Los Dº Fundamentales (arts.14-29+30.2) pueden beneficiarse del recurso de amparo ante el Tribunal Constitucional. Los derechos programáticos, no.

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.

Consideramos esta sentencia (redacción) muy ambigua, no se especifican qué leyes o legislatura concretas. Además, se debería mencionar equidad en lugar de igualdad.

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.

Creemos necesario añadir garantías, especificar que es necesario desarrollo de ley o reglamento o directamente ir más allá y añadir que se deberán llevar a cabo Social Impact Assessments (como los estudios de medio ambiente pero en ámbito social y que una norma detalla cómo se deben llevar a cabo).

II Derecho a la protección de datos

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.

Echamos de menos el derecho a la eliminación de esos datos (derecho al olvido). También creemos necesario añadir el respeto al principio de proporcionalidad y minimización.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente.
En el marco español, ¿qué tipo de autoridad?

III Derecho a la identidad en el entorno digital

2. La identidad no podrá ser alterada, controlada o manipulada por terceros contra la voluntad de la persona.

Consideramos que falta concreción: ¿Quién decide qué es manipulación, sus límites, cuándo y cómo y cuál es aceptable y cuándo, cómo y cuál no?

IV Derecho al pseudonimato

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

Consideramos que este punto es deficiente. No se menciona ni la duración de ese pseudonimato, ni bajo qué condiciones/mecanismos de protección se eliminaría.

Creemos se debería ir más allá y también reconocer la anonimización y la anonimidad como derecho. Entendemos que hay riesgos como el delito de odio pero la anonimidad es clave en

contextos de censura y grupos que luchan contra el status quo, por lo que se debe poder garantizar tal derecho. Por ejemplo en situaciones o contextos poco democráticos o sin garantías, la anonimización y la anonimidad presentan un escudo frente a represalias, ataques discriminados, etc.

“Posibilidades técnicas” deja demasiado margen de maniobra para no asegurar la pseudo anonimidad. Necesario especificar en qué casos o qué condiciones permiten saltarse tal derecho con más precisión.

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

Este punto nos genera bastantes preguntas: ¿Qué implica exactamente? ¿Decisión judicial? ¿Orden policial? ¿Deben ser específicas o pueden ser otorgadas en general? ¿Lo puede decidir una entidad privada?

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.

Creemos que debería añadirse el derecho a no ser sujeto a una decisión automatizada. Además presenta una serie de dudas: ¿A qué se aplica el no ser objeto de localización? ¿Se extiende a cámaras CCTV?

El perfilado está extendido en procesos de RRHH y compañías de seguros y es el objeto del mercado de los datos. ¿Cómo se controlará? ¿Implica derecho de reclamación, indemnización, de borrado de datos...? ¿A quién y cómo se podría ejercitar? ¿Obligación de notificación de que se ha sido perfilado - disclaimers?

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.

¿Esto implica que es un consentimiento como el de las cookies? Debe de ser un consentimiento en situación de igual a igual. No como “lo tomas o lo dejas”, porque si la práctica del perfilado está extendida, por ejemplo, en aseguradoras, no hay posibilidad real de no aceptar. Además debe poderse saber en que se basa tal perfilado y que implica, que datos se usan y a que conclusión llegan, para facilitar la reclamación en casos de errores y discriminación, y mitigar desigualdades. Si los casos y garantías ya están previstos en las leyes, hacer una mención más exacta de qué leyes se aplican.

VI Derecho a la seguridad digital

1. Toda persona tiene derecho a la seguridad en el entorno digital.

¿Qué tipo de seguridad? ¿Seguridad ante contenido de radicalización, ante el ciberacoso? ¿Incluye seguridad en el sentido de proteger contra el perfilado que promociona contenido dañino (por ejemplo, alt-right)?

DERECHOS DE IGUALDAD

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.

¿Y la perspectiva anti racista, anticapacitista y anti clasista?

IX Protección de menores en el entorno digital

¿Se han tenido en cuenta/se ha animado a participar a entidades que representen a menores o menores directamente? ¿Se prevé algún proceso en este sentido?

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.

Nos preguntamos: ¿Mediante qué mecanismos se articula este punto si generalmente los propios progenitores/etc tienen un problema para hacer un uso equilibrado y responsable? Además que se entra dentro de la esfera privada y la libertad de los individuos. Y tal uso equilibrado y responsable es difícil si el diseño de las herramientas digitales está hecho con el objetivo opuesto.

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.

Nos preguntamos ¿Cómo justifica esto el Convenio Google? ¿Afectará a los acuerdos que ya existen con grandes corporaciones?

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.

¿Cómo se harán tales estudios sin ser intrusivos? Consideramos que es necesario incluir atención a los efectos en la salud mental.

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.

Echamos de menos vincular este punto con la legislación sobre accesibilidad ya existente en nuestro país, de hecho, según una serie de leyes que existen en España desde hace unos cuantos años, los sitios web de las Administraciones Públicas y de las empresas de especial transcendencia económica deben ser accesibles desde el 31 de diciembre del 2008. Sin embargo, sigue sin ser así aunque se hayan publicado reales decretos, como el 1112/2018 que apunta también a las aplicaciones móviles y estipula las penalizaciones, adaptándose además a la directiva europea. ¿Cómo se garantizará la accesibilidad cuando la legalización al respecto se incumple sistemáticamente?

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.

Tal y como está escrito consideramos que este es un punto vacío. Es el mismo acceso que tienen todas las personas. Creemos que se necesita precisar la existencia de una brecha digital por edades y la necesidad de proporcionar alternativas analógicas, posibilidad de elección así como promoción e inclusión de las personas mayores en la transformación digital. Creemos necesario mencionar ámbitos concretos (AAPP, sectores privados). Además pensamos que en este apartado se necesita trabajar directamente con grupos afectados.

XII Derecho a la neutralidad de Internet

Los poderes públicos garantizarán el derecho de los usuarios a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos, en los términos previstos en el Reglamento (UE) 2015/2120 de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Echamos de menos el acceso garantizado en todo el territorio estatal.

XIII Libertad de Expresión y Libertad de Información

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.

¿Entra aquí añadir que es necesario avisar de cuando se habla con una persona o con un chatbot como se comenta en el art XXIII Derechos ante la inteligencia Artificial? Merece mención propia en este apartado, tiene particular relevancia si hablamos de los chatbots usados en Salud.

La transparencia algorítmica en los medios que utilizan la IA para crear noticias o para perfilar los lectores para colocarles publicidad es nula. ¿Cómo se va a obligar a medios privados que cumplan con este requisito?

Esta transparencia se debería extender a más sectores. Necesidad de aplicación de tal transparencia a cualquier información o resolución hecha mediante procesos automatizados sin intervención automatizada (y también los casos con intervención humana).

También debe incorporarse un mecanismo de control "ex ante" (y no sólo "ex post"). Es decir: no vale sólo con que el medio de comunicación lo notifique más tarde. Los 10.000 lectores que lo hayan leído el primer día no se van a enterar.

Y un segundo punto: en caso de que el medio de comunicación no incorporara ese aviso, ¿quién se hace responsable? ¿Debería ser el medio privado, o más bien un Comité Independiente que monitoree todas las acciones? Nos parece preocupante la delegación de "culpas y responsabilidades".

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.

Creemos que "mecanismos de autorregulación transparentes", es poco definido y no se menciona bajo qué estándares mínimos y máximos, ni quién sería el "coordinador" general de estos asuntos. Y es de dudosa eficacia si no se impone un plazo para publicar el aviso al proveedor.

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.

Consideramos que se trata de un punto vacío de contenido si no se añaden medidas concretas o reglamento que especifique en que se traduce esta participación.

XV Derecho a la educación digital

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.

Nos surge la duda si en esta formación se incluirán aspectos relacionados con la afectación de la tecnología al desarrollo personal, a nuestro comportamiento y a nuestra salud.

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

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.

Si se trata de un aspecto que es voluntario y no obligatorio, ¿cómo se va a hacer efectivo en la realidad entonces?

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

Se debería enfatizar que el canal digital en ningún caso debería ser una ventaja ni suponer una ventaja respecto al resultado de una actuación administrativa. Debe garantizarse el principio de igualdad con independencia del canal utilizado.

Remarcar que algunas personas no optan sino que no tienen acceso a internet.

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.

Punto muy necesario, pero ¿cómo y quién va a hacer esta evaluación de impacto en los derechos digitales? ¿Se publicará para que la ciudadanía nos enteremos, en caso que salga que no se están cumpliendo?

DERECHOS DEL ENTORNO LABORAL Y EMPRESARIAL

XVII Derechos en el ámbito laboral

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

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.

Dadas las tendencias en relación al trabajo nos preguntamos: ¿Qué se entiende por lugar de trabajo? Debería de ser un concepto amplio de lugar de trabajo. Cualquier lugar donde estés trabajando. Se ha venido aceptando que si el trabajador está informado de los medios de

monitorización se puede hacer, esto presenta problemas cuando el trabajador comparte el espacio de trabajo por ejemplo en un coworking o en su casa teletrabajando.

3. 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;

Creemos que si conlleva modificación sustancial de las condiciones de trabajo debe formar parte de la negociación colectiva.

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.

Esto es prometedor aunque parece redundante con el punto "V. Derecho a no ser localizado y perfilado" que determina el derecho de no ser sometido a tales procesos.

XVIII La empresa en el entorno digital

3. Se desarrollarán las condiciones que permitan la creación de espacios de pruebas controladas para desarrollar nuevos modelos de negocio, aplicaciones, procesos o productos basados en la tecnología (sandbox).

Creemos que si se tratan datos de carácter personal en estas pruebas se debería contar con el consentimiento expreso y/o utilizar datos pseudoanonimizados.

DERECHOS DIGITALES EN ENTORNOS ESPECÍFICOS

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

No se habla de la [integridad científica](#) esperada (la independencia, imparcialidad, y necesidad de réplica de la investigación, entre otros puntos) ¿Se asume?

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.

Los datos seudonimizados siguen siendo datos personales ya que puedes llegar a la reidentificación.

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.

Nos surgen dudas: ¿Con qué temporalidad? ¿Con qué fin? ¿Con qué proporcionalidad? ¿se adecuará a la Estrategia Europea de Datos?

Además, se habla de donantes de datos, pero no de si habrá fuentes de datos abiertos.

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

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.

Esto es un punto positivo pero puede sufrir el desgaste de los ciclos electorales y visión cortoplacista de legislaturas. Entonces ¿cómo se podría evitar la sustitución integral cada 4 años a una nueva empresa? Esto debería ser tratado en más detalle, porque toca la cuestión de las competencias sobre estas tecnologías (¿nivel municipal, autonómico, estatal?).

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

Existe un importante lock-in-vendor en este tema. Debería explicitarse que en ningún caso la negativa a la cesión de datos al fabricante del dispositivo debería suponer una exclusión de la persona usuaria del servicio. Por ejemplo: Marcapasos y DAI se ofrece servicio de telemetría a través de un modem que tienes en casa (tiene el aspecto de un móvil). Para acceder al servicio, debes consentir que los datos sean compartidos con los fabricantes con la finalidad de mejorar los aparatos. No indica anonimizados previamente.

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.

Consideramos que hablar de armonización parece más realista que hablar de estandarización. La estandarización promueve un único lenguaje, mientras que la armonización ofrece más flexibilidad exigiendo la interoperabilidad entre sistemas.

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.

Esta cesión a terceros de datos de salud debería estar más limitada y protegida. Establecer en qué casos se puede ceder tales datos a terceros y siempre necesidad de contar con el consentimiento explícito del paciente a los fines específicos, sin posibilidad de una cláusula general.

XXIII Derechos ante la Inteligencia artificial

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

b) Se asegurarán la transparencia, auditabilidad, explicabilidad y trazabilidad.

¿Cómo se llevará a cabo? Necesita especificarse cómo se asegurará para evitar situaciones como la batalla de Civio por el código del Bono Social.

Además existe la necesidad de una definición paramétrica de qué se exigirá como explicabilidad, auditabilidad, transparencia (y trazabilidad) para que este punto no se quede vacío de contenido y para que no se den casos en los que explicaciones sencillas y/o explicaciones insuficientes sirvan para satisfacer estos requisitos. Ahora por ahora no es posible asegurar la explicabilidad. Por ejemplo, en este sentido, se podría cambiar explicabilidad por “un mecanismo o explicaciones que lleven a entender cómo ha tomado la decisión el algoritmo”.

¿Se incluye la rendición de cuentas en la auditabilidad? Tal y como se entiende en la guía ["directrices éticas para una IA fiable"](#) de la comisión europea que especifica que "la auditabilidad es la capacidad para evaluar los algoritmos, los datos y los procesos de diseño."

c) Deberán garantizarse la accesibilidad, usabilidad y fiabilidad.

Nos surgen dudas acerca del término “fiabilidad” Creemos que esto vendría dado por el punto 2. Es decir, si el sistema es transparente, auditable y explicable, entonces será fiable. De otra manera, no será.

2. Las personas tienen derecho a no ser objeto de una decisión basada únicamente en procesos de decisión automatizada, incluidas aquéllas 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.

Qué significa ¿de modo similar? Se debería reducir solo al efecto jurídico.

Se debe tener en cuenta y se debería añadir aquí también las decisiones y diagnósticos clínicos. En ningún momento una decisión clínica puede estar determinada por un algoritmo. Se debe resaltar que el algoritmo IA soporta el proceso de decisión pero no lo determina.

Además, ¿Qué supuestos son previstos por las leyes? ¿Por qué hay supuestos en los que es posible que las decisiones sean completamente automatizadas y cómo se justifican? Creemos que se debería garantizar que siempre haya un humano que supervise. Y en relación a la impugnación, ¿ante quién y con qué mecanismos de defensa?

XXV Garantía de los derechos en los entornos digitales

3. Se promoverán mecanismos de autorregulación regulada y procedimientos de resolución alternativa de conflictos.

Vemos la necesidad de mencionar plazos para asegurar el cumplimiento.

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.

Vemos la necesidad de mencionar plazos para asegurar el cumplimiento.

Comunidad Inteligencia Artificial y Derechos Humanos

14 diciembre 2020

comunidadddhia@prontonmail.com