
Respuesta de Interferencias y Trackula a la consulta de la Carta de Derechos Digitales

19 de diciembre de 2020



Índice

Cuestiones preliminares.....	4
Quiénes somos.....	4
Agradecimientos al equipo de expertos.....	4
Sobre el instrumento elegido.....	4
Sobre la falta de intencionalidad.....	5
Objetivos de este documento.....	6
Problemas, cuestiones y propuestas.....	7
Sobre derecho al olvido, al pseudonimato y la identidad digital.....	7
El derecho al olvido.....	9
El derecho al pseudonimato.....	10
Identidad digital.....	11
Sobre el derecho a no ser localizado y perfilado.....	13
Sobre los derechos de conexión y desconexión.....	14
Sobre la salud mental y adicción a redes, productos y servicios.....	15
Sobre el acceso a datos con fines de investigación científica, innovación y desarrollo.....	16
Sobre la herencia digital.....	17
Sobre los derechos de igualdad.....	18
¿Igualdad para quién?.....	18
Acabar con las brechas digitales.....	19
Sobre la igualdad de las personas con discapacidad en el entorno digital.....	21
Protección de menores en el entorno digital.....	22
Sobre la libertad de creación y acceso a la cultura en el entorno digital.....	23
El acceso a la cultura en Internet.....	24
Acceso a la cultura y neutralidad de la red.....	24
Promoción de la cultura libre y democratización del contenido para garantizar una ciudadanía libre.....	24
Sobre los derechos ante la inteligencia artificial.....	28
La rendición de cuentas en la inteligencia artificial.....	28
Transparencia y control.....	30
Accesibilidad, usabilidad y fiabilidad.....	31
Prohibición de sistemas IA dirigidos a manipular la voluntad de las personas.....	31
Tecnologías de reconocimiento biométrico y facial.....	32
Antecedentes.....	34
Consideraciones.....	35
Nuestra proposición.....	35
Sobre el derecho a la seguridad digital.....	38
Necesidad de definición de la seguridad digital.....	38
Seguridad digital más allá del ámbito público.....	40

Seguridad en contenido.....	40
Derecho al cifrado, a la integridad y la privacidad de las comunicaciones.....	41
Sobre los derechos del individuo en relación con la Administración Pública..	43
Software libre.....	43
Open data.....	46
Garantizar la igualdad y el principio de neutralidad tecnológica.....	47
Algunas propuestas.....	48
Garantizar la transparencia en el uso de decisiones automatizadas en las relaciones con la administración.....	49
Sobre la empresa en el entorno digital.....	51
Conclusiones.....	54

Cuestiones preliminares

Quiénes somos

Esta respuesta a la consulta pública de la Carta de Derechos Digitales es una acción conjunta entre los componentes de dos asociaciones: Interferencias y Trackula. Ambas centradas en la defensa de la soberanía digital y tecnológica, la privacidad y la seguridad en la red.

Nuestro deber como sociedad civil es trasladar problemas públicos a la agenda política, por lo que agradecemos la existencia de esta consulta pública y esperamos aportar una visión complementaria a la ya existente en la carta.

Las personas que firmamos este documento somos:

Lorena Sánchez

Pablo Castro

Ángel Pablo Hinojosa

Santiago Saavedra

Germán Martínez

Sofía Prósper

Paula de la Hoz

Agradecimientos al equipo de expertos

Los miembros de los colectivos Trackula e Interferencias quieren, antes que nada, agradecer el esfuerzo y trabajo del equipo de expertos que han colaborado en la realización de esta carta. Grandes profesionales en su campo, muchos de los cuales admiramos profesional y personalmente, y que han trabajado con fervor para intentar innovar en una materia pionera.

Sobre el instrumento elegido

Nos gustaría comenzar este escrito cuestionando si una “Carta de Derechos Digitales” es el instrumento adecuado para trasladar el tipo de políticas públicas que en ella se enuncian.

Si la Secretaría de Estado quiere llevar a cabo políticas en materia de derechos digitales, un instrumento sin fuerza jurídica pero con apariencia de norma no parece el mecanismo más apropiado, por lo engañoso de la forma y su ausencia de eficacia.

Sin embargo, si el objetivo de la Secretaría de Estado era el de enunciar deseos sobre derechos todavía no adquiridos, también resulta engañosa la forma. El

contenido incluye referencias legislativas actuales a aquellas cuestiones con base legal, y peca de ser poco ambiciosa en el reconocimiento de nuevos derechos en la esfera digital. La enunciación de un “derecho” cuya eficacia queda limitada a “según determine la legislación que ya está vigente” relega el nombramiento de dicho derecho como tal al mero plano teórico, ya que su eficacia estaba ya conseguida y el derecho afianzado. El espíritu a la hora de enunciar derechos debería de ser aquel en el cual las leyes pudieran modificarse para hacerlos existir y cumplir.

Por lo tanto reiteramos que, en nuestra consideración, la redacción y la forma en la que se ha realizado la aproximación a esta Carta es insuficiente para el objetivo que la Agenda Digital podría pretender.

Si el objetivo fuese simplemente el de resumir una serie de derechos que ya están afianzados en la sociedad (y reiterar que el Parlamento legislará sobre tantos otros que no tenemos y que la carta se limita a mencionar el interés en legislarse), entonces hay muchas otras cuestiones normativas que han quedado fuera de la carta, y en las que incidimos en esta contestación más adelante. Cuestiones como las relacionadas con los Esquemas Nacionales de Interoperabilidad y de Seguridad, o derechos ya establecidos en normativa europea ya transcrita a la nacional, como el Derecho al Olvido y el de Portabilidad de los datos, o los derechos a la desconexión en el ámbito laboral (Artículos 87 a 91 de la LOPDDD).

Sobre la falta de intencionalidad

Con la excepción de algunas cuestiones concretas, especialmente relativas a la educación, que ocupan un volumen mayor en texto de la carta que ninguna otra, en general, es destacable la falta de intencionalidad en la enunciación de estos derechos. El lenguaje que se ha elegido para describirlos es tan ambivalente que puede interpretarse de formas radicalmente diferentes. Nosotros mismos, a la hora de realizar esta contestación, hemos tenido desacuerdos respecto de lo que significan algunos de los enunciados descritos, que detallamos en cada apartado.

Un ejercicio muy importante tendría que ver con describir con mayor intención ciertos derechos. Tras la publicación de la Carta se han llevado a cabo varias actividades de divulgación y en prensa escrita, dirigidas a explicar de una manera sencilla la intencionalidad de la carta. Sin embargo, consideramos inoportuno que todas estas aclaraciones no formen parte del texto oficial, y que sean además la interpretación de miembros individuales del grupo, y no parte del borrador de la Secretaría de Estado.

Desde un punto de vista externo y analítico y sin el contexto de la participación en las discusiones dentro del Grupo de Expertos y de la Secretaría, existen a lo largo de la Carta varios elementos que no se entienden o que pueden interpretarse en un sentido contrario.

Un ejemplo de ello es el derecho al pseudonimato, cuya redacción actual puede interpretarse de distintas formas. Este derecho puede interpretarse, por una parte, como la posibilidad de imponer un sistema de autenticación global nacional como clave@365 para entrar a plataformas como Facebook -medida que consideraríamos abusiva, por supuesto, pero que podría ser perfectamente legible con la actual redacción. O, por el contrario, podría interpretarse como el derecho a no ser identificado con datos personales y, por tanto, con la prohibición de que Facebook demande el nombre real del usuario al crearse una cuenta por la existencia del derecho a la presentación en el entorno digital con pseudónimo. Las diferentes interpretaciones de este derecho solo son un ejemplo de la necesidad de matizar, explicar y madurar muchas de las propuestas de la carta.

Creemos por lo tanto que es importante diferenciar las generalidades, de las vaguedades.

Los derechos han de ser enunciados con generalidad suficiente como para que sean derechos y no solamente aplicaciones a cuestiones específicas; la segunda es la base fundamental de la inseguridad jurídica y social, y deberíamos de evitarla en la medida de lo posible, y de forma superlativa en la enunciación de derechos básicos.

Tal vez algunas de estas vaguedades podrían ser solucionadas si se hubiese publicado el Anexo a la Carta que ésta menciona, pero sin él, no tenemos tampoco definiciones de muchas cuestiones enunciadas con lenguaje natural en la carta y que puede referirse a una abanico más o menos amplio de cuestiones concretas. Por lo tanto, el ámbito de aplicación de ciertos derechos queda incierto.

Objetivos de este documento

Sobre la base de las cuestiones preliminares presentadas, el objetivo de esta respuesta es presentar algunos de los problemas teórico-prácticos que la actual formulación de la Carta plantea, y proponer soluciones a los mismos mediante la utilización de la propia Carta y/o otras políticas públicas digitales.

Se han planteado cuestiones formuladas desde diferentes perspectivas para poder entenderlas desde un enfoque multidisciplinar. Por lo tanto, no abordamos la Carta como un instrumento unitario, sino que esta respuesta está enmarcada en las actuales políticas públicas digitales y su implicación en las mismas.

El documento presenta la siguiente estructura. (i) Un resumen ejecutivo de las propuestas. (ii) Diferentes secciones en las que se han agrupado varios derechos en función de su tipología o los problemas colindantes que conllevan y (iii) unas conclusiones finales.

En las secciones de análisis se presentan tres tipos de contenidos:

- Justificación de problemas que presenta la Carta y reflexiones sobre los mismos.
- Cuestiones y preocupaciones directas sobre el contenido de la Carta y cómo este está presentado.
- Propuestas concretas para abordar los problemas planteados en la Carta. Estas propuestas trascienden la Carta dando lugar a la solicitud de políticas públicas concretas. Por supuesto, todas las aportaciones pueden tenerse en cuenta para incluirse directamente en una futura redacción de la carta. Sin embargo, al considerar que la forma de la Carta no es la más adecuada, proponemos que se plantee un potencial *roadmap* digital que incluya las políticas públicas digitales propuestas en línea con la Agenda Digital 2025.

La siguiente sección describe en profundidad cada una de estas partes.

Problemas, cuestiones y propuestas

Derechos del individuo

Sobre derecho al olvido, al pseudonimato y la identidad digital

El pseudonimato tal y como se describe no es suficiente y su interpretación es ambigua. Así mismo necesitamos una mayor garantía de anonimidad en el entorno digital para tener derechos equiparables al pseudonimato en el entorno analógico.

Los valores que subyacen a la Declaración Universal de los Derechos Humanos¹, así como a los establecidos en la Carta de los Derechos Fundamentales de la Unión Europea² nos permiten la equidad entre nosotros, en un porvenir pacífico, y partiendo del respeto de la dignidad humana, la integridad, libertad, igualdad y solidaridad hacia otras personas.

¹ Resolución 217 A (III) de la Asamblea General de las Naciones Unidas, [https://undocs.org/es/A/RES/217\(III\)](https://undocs.org/es/A/RES/217(III))

² Parlamento Europeo, Consejo y Comisión. Carta de los Derechos Fundamentales de la Unión Europea. DOUE 2007/C 303/1 https://eur-lex.europa.eu/eli/treaty/char_2007/oj

Los derechos digitales habrán de ser enunciados con el objetivo de preservar esos valores, aunque para ello no siempre tenga que reflejarse el mismo derecho para conseguirlo.

En ocasiones lo más sencillo para un derecho es trasladarlo de forma natural a un entorno digital. Sin embargo, en otras, para garantizar estos mismos valores han de utilizarse otros recursos, ya que la capacidad de actuación sobre las circunstancias por parte de las personas en entornos digitales puede ser diferente.

En particular, y respecto a la identidad, entre los Derechos Fundamentales nos podemos encontrar el de la dignidad o la privacidad, así como a la protección de datos de carácter personal, el derecho a la presunción de inocencia y el derecho a una defensa justa. Hacer un traslado directo en entornos digitales puede ser diferentes.

Cuando, por ejemplo, una cámara de seguridad graba a una persona en un espacio público, esta puede ejercer sus derechos de acceso, o incluso supresión, por encontrarse en su misma jurisdicción, además de poder cuestionar la legitimidad de dicho tratamiento en primer lugar. Sin embargo, las fronteras jurisdiccionales en entornos digitales, y en particular, a través de Internet, son mucho más difíciles de establecer claramente. En ocasiones es difícil saber cuál es la entidad que está tratando tu información personal, ya que aunque técnicamente un nombre de dominio es de una única entidad, los términos y condiciones que uno acepta pueden realizar distinción en lugar de la jurisdicción origen del usuario del servicio, que en pocas ocasiones se encontrará en la misma jurisdicción que la persona.

Consecuentemente, es importante dar un paso atrás y plantear qué derechos plantearían un ejercicio efectivo de la salvaguarda de los valores fundamentales que guardamos en este Estado y en la Unión Europea a la hora de garantizarlos.

Debemos plantearnos otra vía para garantizar los derechos digitales individuales debido a las relaciones de asimetría de poder. Los consumidores no siempre tienen herramientas suficientes para defender sus derechos, especialmente cuando se relacionan con empresas fuera de la jurisdicción española.

Podría pensarse en forzar la capacidad de las entidades de control de regular el acceso a Internet, pero esto desmerecería su propia naturaleza, sentando un mal precedente respecto a la neutralidad de la red que nosotros, al igual que la Carta, estamos a favor de mantener. Y aunque el primer acceso estuviese regulado entre un usuario y un responsable del tratamiento legítimo, es posible que otros actores extranjeros pudiesen obtener información personal por medios lícitos pero en contra de los términos y condiciones de aquellas plataformas en las que el interesado hubiese dado su consentimiento, y a partir de ahí, el mismo interesado carecería de capacidad para gestionar esta información.

Existen numerosos servicios que mediante técnicas como el “scraping” acceden al contenido de redes sociales y extraen información personal de individuos.

Estas actuaciones podrían no estar autorizadas segundo la legislación vigente, pero aún así, su persecución eficaz es muy intensiva en recursos y a cambio de pocos resultados.

En general, una vez llega información a Internet, es extremadamente complicado eliminar esa información, e incluso cuando el esfuerzo es mayor se puede producir el conocido como Efecto Streissand³, por el cual se vuelve impracticable la eliminación del contenido.

Si bien es extremadamente importante establecer un acceso efectivo a la educación que pueda mitigar a largo plazo estas cuestiones, urge considerar una solución transitoria. Por lo tanto, a partir de aquí creemos que es necesaria una mayor discusión respecto al anonimato, pseudonimato y capacidad de restauración de la imagen pública de una persona, así como la capacidad de poder presentarse esa persona en un medio o plataforma digital sin ser perfilada por su comportamiento anterior por la web o a través de otros medios que la identifiquen de forma cruzada.

Por ello proponemos, en primer lugar, recordar ya la existencia de ciertos derechos de los que partimos aunque, de cara a la creación de una Carta de Derechos Digitales, creemos que son insuficientes, si bien son un punto de partida interesante.

El derecho al olvido

Nos gustaría comenzar destacando la omisión en la Carta, que creemos fundamental, del llamado “derecho al olvido”, ya regulado a partir del Reglamento (UE) 2016/679 (en adelante, RGPD).

Sin embargo, dada la capacidad y velocidad en Internet de la diseminación de información, es relevante considerar que aunque un usuario de un servicio resida en este país, la entidad titular del servicio puede no hacerlo, o bien terceros con acceso de forma internacional al servicio podrían no estar sujetos a nuestra ordenación jurídica, limitando la efectividad de este derecho, así como de otros de los que esta Carta pretende garantizar.

Si consideramos el espacio en línea en su naturaleza, ha de uno ser plenamente consciente de la facilidad de traspasar barreras internacionales y jurisdiccionales, y por lo tanto, ofrecer derechos que, en la jurisdicción de origen, permitan salvaguardar los valores comunes que deseemos de la forma más garantista posible con esta circunstancia.

Por ello, creemos que en el presente y futuro digitales, estos derechos garantistas con nuestra imagen pública son menos aplicables. Nos referimos con esto a que uno puede ser objeto de escarnio por razones inocuas simplemente a través de la manipulación y voluntad de algoritmos. Sin embargo, los individuos carecen de capacidad y mecanismos para restaurar su

³ "Streisand effect". Wikipedia https://en.wikipedia.org/wiki/Streisand_effect

imagen una vez sale fuera de su control, y especialmente cuando el servicio a través del que operan está fuera de nuestra jurisdicción.

Propuestas

- Incluir el ya existente “Derecho al olvido” en la Carta.
- Invitar a la reflexión sobre los límites jurisdiccionales en internet y la dificultad de ofrecer derechos cuando el acceso a internet es global.

El derecho al pseudonimato

Como el derecho al olvido queda limitado en alcance, y en jurisdicción, aplaudimos la iniciativa de esta Carta de incorporar un derecho al pseudonimato en su redacción.

Sin embargo, no parece que la redacción vaya tan claramente a favor de los valores de los que se habla al principio de esta sección. En su lugar parece recordarnos que lo importante es no tener un anonimato real para poder permitir a las Fuerzas y Cuerpos de seguridad perseguir la delincuencia. Por lo tanto, con la redacción propuesta, el derecho al pseudonimato no describe lo que pretendemos. Es decir la orientación debería de ofrecer unas consideraciones de anonimato mayores.

Reconocemos la falta de un derecho al anonimato en el derecho constitucional e internacional. Creemos que en el mundo analógico, nuestros valores comunes están garantizados por los derechos que establecen la Declaración Universal, o la Carta de Derechos Fundamentales de la UE. Sin embargo, ya que el empoderamiento que nos dan ciertos derechos en el mundo en línea es más limitado, debido a la existencia de diferentes jurisdicciones que pueden entrar en juego en los entornos digitales, especialmente fuera de la UE, se vuelve impracticable. La única posibilidad es evitar que se nos reconozca en el proceso de la comunicación.

Por esto, proponemos no solo que se permita eliminar datos previos -cuando se encuentren en nuestra jurisdicción efectiva-, sino además poder actuar de forma que no se relacionen con el individuo ya en primera instancia, es decir, establecer un derecho más efectivo de anonimización de las actuaciones personales en Internet, y especialmente con los proveedores de servicios. Esto debería de ser independiente de la capacidad de rastreo por parte de los Cuerpos y Fuerzas de Seguridad en caso de tener causa probable, y bajo las consideraciones que puedan limitar el derecho al secreto de las comunicaciones según establecen las Leyes, respetando otros derechos que ya tenemos, como el del secreto de las comunicaciones.

Desde la aproximación de un derecho al pseudonimato, según se describe en la Carta, presentamos una redacción más clara, concreta y desgranada, para que no admita margen a ser malinterpretado.

1. Por ejemplo, en la propuesta actual podría leerse una pretensión de que las actuaciones sean siempre identificables hacia personas físicas, lo cual no solo podría ir en contra del principio de minimización del Reglamento de Protección de Datos, sino que, en general, puede ser de un esfuerzo inconmensurable su implementación.
2. Sin embargo, dado que hoy en día los términos de uso de ciertas plataformas, como Facebook, por ejemplo, requieren el uso del nombre real en sus Términos y Condiciones generales, ¿podría ser la intención de este derecho el de garantizar que los Términos y Condiciones generales de una plataforma tengan la obligación de aceptar mi pseudónimo si es así como yo quiero presentar mi identidad digital? Esto, además, iría completamente alineado con el principio de minimización de datos en el tratamiento de datos de carácter personal.

Como puede verse, ambas interpretaciones son extremadamente contrarias, pero tal y como se señala en el Capítulo de Cuestiones Preliminares, la falta de intencionalidad en el desarrollo de los derechos que estipula la carta nos deja en una sensación de incertidumbre que no permite posicionarse al respecto y, además, sentar el precedente equivocado, por una brevedad mayor en el enunciado de lo que permite afianzar el concepto deseado.

Por ello, proponemos que el derecho al pseudonimato se reformule como el Derecho a no ser identificado en Internet con carácter general, y se enuncie como:

“El derecho de toda persona física a que, cuando actúa en nombre y cuenta propios (o apoderadamente), pueda evitar comunicar el nombre y la cuenta de para quién actúa, en el ejercicio ordinario de sus comunicaciones y ejercicio de actividades personales, en el uso de servicios digitales, excluyendo solamente aquellos en los que la identificación sea un medio material o técnicamente necesario para proporcionar el servicio deseado por el usuario.”

Identidad digital

A partir de lo anterior, cabe hablar del concepto mismo de identidad y de cuál es la naturaleza del pseudonimato.

En el contexto de la Carta no queda clara si la identidad digital es una y única para cada individuo o si una persona puede disponer de múltiples identidades en el mundo digital. Tampoco si la independencia de cada identidad podría ser garantizada por el derecho al pseudonimato, o si, por el contrario, se pretende unificar las identidades en línea y en persona.

Para responder a esta pregunta uno requiere plantearse el concepto mismo de identidad y qué es lo que nos identifica en línea. En este sentido, podría tener sentido hablar de múltiples identidades en función de los dispositivos y comunidades con los que uno se relaciona en cada ámbito, también para tener en cuenta una mayor capacidad de protección de los datos personales, y evitar la correlación entre datos de unas y otras circunstancias de las personas.

Para garantizar un acceso efectivo al pseudonimato, esta iniciativa es partidaria de obligar a los proveedores de servicios digitales a tratar de forma separada los datos personales de aquellas partes de sus servicios que puedan estar disponibles bajo un pseudónimo, de aquellas otras que por diferentes razones requieran levantar el velo de la identidad física.

Como ejemplo, durante una compra online, el proveedor de pagos del comercio, deberá tratar información personal en requerimiento de ordenación internacional de anti-blanqueo de capitales, pero no será el caso cuando el usuario se registre, por ejemplo, en una red social de forma gratuita. En el caso de existir pagos en una plataforma que tenga funcionalidades gratuitas, habrá que proporcionar a los usuarios métodos de pago registrados con medidas técnicas que garanticen el tratamiento de sus datos de una forma mal menos tan anonimizada como la que se hace de los usuarios que hagan uso de funcionalidades gratuitas únicamente, especialmente en cuanto al tratamiento de datos basado en el interés legítimo del responsable del tratamiento.

En un ejemplo más concreto, podríamos imaginarnos dos servicios de Google: el buscador (“Google Search”) y la tienda de dispositivos (“Google Store”).

Si bien podemos tener una cuenta de Google para realizar búsquedas, e incluso permitir que estas búsquedas formen parte del perfil (potencialmente pseudónimo) de la persona usuaria, en el momento en el que esta persona desee comprar un dispositivo a esta compañía, deberá dar su dirección de entrega, así como su nombre real y otros datos de pago, levantando el velo de la identidad física. Nuestra propuesta es que Google no debería de poder utilizar estos datos como parte del perfil de este usuario en Google Search, manteniendo el carácter pseudónimo del usuario en este otro servicio, de forma que usuarios que por querer utilizar otras partes del servicio no se vean privados de ello por su interés en mantener su identidad pseudonimizada en otras partes separadas del uso de servicios del mismo proveedor.

Propuestas

- Tratar de forma separada datos personales de alguien bajo un pseudónimo frente a datos que requieran una identidad física.

Sobre el derecho a no ser localizado y perfilado

El consentimiento puede no ser en todos los casos una base legal suficiente para el uso de estas tecnologías por lo que es importante indicar correctamente la intencionalidad de este derecho.

Si bien acogemos con agrado la incorporación en la Carta de la necesidad de no ser objeto de localización, ni a ser sometidos a análisis de la personalidad o conducta mediante tecnologías ubicuas. En la redacción de las excepciones hay un potencial interpretación que puede dar carta blanca al uso de estas tecnologías.

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

Este matiz daría lugar a que el consentimiento siempre fuera una base legal suficiente para el uso de estas tecnologías, cuando no siempre debería serlo.

Creemos que la redacción como “y/o” en lugar de “y” solamente (es decir, que tenga siempre que garantizar los casos previstos en las leyes) es un fallo de redacción, pero si esta fuese la intención real, nuestra propuesta es contraria al consentimiento como base legitimadora suficiente, en particular, en aquellas circunstancias en las que resulta desproporcionado poder garantizar que el consentimiento es adecuadamente informado.

Propuestas

- Corregir un defecto de forma en la redacción del derecho.

Sobre los derechos de conexión y desconexión

Se manifiesta la ausencia del derecho a la conexión en la Carta. Necesidad de concreción y detallado en el si nombrado, derecho a desconexión.

Es manifiesto también que, a pesar de que el Gobierno está haciendo hincapié en reducir la brecha digital, cuestión que mencionaremos más adelante, resulta chocante no ver el derecho a la conexión como un derecho fundamental de esta carta, mientras se postulan otros derechos tal vez mucho menos básicos (como el de un estado de pruebas).

Creemos que el derecho a la conexión es un deber en esta Carta, ya que el primer punto enunciado en la misma ya establece una equiparación entre derechos y libertades fundamentales aplicadas también al mundo digital, sin garantizar la existencia de este medio para las personas. Esto debería de ser lo primero de lo que se hablase, seguido de la protección de datos.

Respecto al derecho de desconexión, también requiere una mayor elaboración que la breve mención estipulada en la carta en el punto 1.a) del apartado XVII, y que establezca esta protección con carácter general, aunque pueda haber ciertas condiciones que reduzcan la disposición efectiva de este derecho.

Por ejemplo, podría ser razonable requerir de las empresas la presentación de información por vías telemáticas (como ya es obligatorio hoy en día), aunque esto no se deba de hacer extensible a particulares. Es necesario poner estos debates sobre la mesa puesto que la aplicación de normas sobre desconexión digital puede traer consigo una mayor utilización de herramientas de vigilancia en el ámbito laboral. Un ejemplo en este sentido sería plantearse la necesidad de utilización de servicios MDM (Mobile Device Management ⁴) para gestionar la desconexión del empleado. Esto puede implicar que en sectores en los que, por defecto, no se utiliza móvil de empresa, se recurra a políticas de “*bring your own device*” para gestionar el control de la desconexión digital garantizando que el usuario no recibe correos electrónicos a deshoras o que no se conecta. En consecuencia, se puede necesitar un gestor de dispositivos MDM, con los riesgos que una mala implementación de estos sistemas conlleva para la privacidad del empleado. De este modo, intentando garantizar un derecho, podría estar incurriéndose en un riesgo mucho mayor de vigilancia en el entorno laboral, extendiendo una función de vigilancia del ámbito laboral al entorno personal. Este riesgo de vigilancia continua se extendería a la vida personal del empleado. Es por ello que plantear un derecho a la desconexión digital requiere de reflexión en tanto en cuanto a las consecuencias de su implementación práctica.

⁴ Continuum Product Team. “What is Mobile Device Management”. 20 Abr. 2019. Disponible en: [https://www.continuum.net/resources/mspedia/everything-to-know-about-mobile-device-management-mdm#:~:text=Mobile%20device%20management%20\(MDM\)%20is,being%20used%20in%20the%20organization.](https://www.continuum.net/resources/mspedia/everything-to-know-about-mobile-device-management-mdm#:~:text=Mobile%20device%20management%20(MDM)%20is,being%20used%20in%20the%20organization.)

Propuestas

- Definición concreta de cómo se aplica las normas sobre desconexión digital.
- No obligar a particulares a comunicarse con la Administración exclusivamente por vías telemáticas.

Sobre la salud mental y adicción a redes, productos y servicios

La economía de la atención en la que se basan los modelos de negocio de las plataformas de contenido digital impactan en la salud mental de la sociedad. Se insta a legislar sobre estas plataformas para limitar estos efectos.

La irrupción en la sociedad de las nuevas tecnologías también está afectando a la salud mental de las personas. En concreto, nos referimos a las redes sociales y a otras plataformas cuyo principal modelo de negocio se sustenta en la publicidad digital, y por lo tanto en el interés de mantener a sus usuarios activos y conectados a la plataforma el mayor tiempo posible para que consuman una mayor cantidad de publicidad.

Estas plataformas utilizan métodos y diseños persuasivos con la intención de crear conductas adictivas entre sus usuarios y así incrementar sus ganancias, muchos basados en las mismas dinámicas que se utilizan en máquinas recreativas de azar o en casas de apuestas. Es la llamada “Economía de la atención”.

Estas técnicas de manipulación también están generando diversas patologías asociadas a la mente humana, por ejemplo, varios estudios vinculan el uso de mas de 3 horas al día en redes sociales por parte de adolescentes en EEUU, con un mayor riesgo de enfermedades mentales⁵. Otros indican que el uso de estas plataformas aumenta la probabilidad de sufrir trastorno de déficit de atención e hiperactividad ⁶, diógenes digital o depresión.

⁵ Kira, E. Kenneth, A. Kayla, N. (2019) Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth. *JAMA Psychiatry*, 76(12):1266-1273. Disponible en: <https://jamanetwork.com/journals/jamapsychiatry/fullarticle/2749480>

⁶ Chaelin, K. Junhan, C. Matthew, D. (2018) Association of Digital Media Use With Subsequent Symptoms of Attention-Deficit/Hyperactivity Disorder Among Adolescents. *JAMA Psychiatry*, 320(3):255-263. Disponible en: <https://jamanetwork.com/journals/jama/article-abstract/2687861>

Es por esto que se propone revisar la legislación vigente, con el fin de aplicar sobre estas plataformas, legislación similar a la utilizada en el sector del juego. Del mismo modo se insta a tratar de modificar los incentivos de estos modelos de negocio basados en la atención, con el fin de que estas técnicas de persuasión vean reducida su importancia.

También se propone trabajar en el sector de la educación para controlar el uso que se hace de la tecnología en el mismo. Del mismo modo se debe formar al alumnado y la comunidad educativa, acerca de los riesgos y las buenas prácticas en el uso de estas nuevas tecnologías. Actualmente tenemos tímidas iniciativas como el programa “Cibercooperantes” de INCIBE, pero el esfuerzo debe ser mayor, para que esta formación llegue a toda la comunidad educativa de manera efectiva.

Propuestas

- Posibilidad de aplicar legislación similar a la utilizada en el sector del juego sobre las plataformas de contenido digital.
- Modificar los incentivos de los modelos de negocio basados en la adicción para reducir su impacto sobre la sociedad.
- Limitar el uso de plataformas digitales adictivas en el entorno de la educación.
- Creación de programas de formación para alumnado y comunidad educativa acerca de los riesgos de estas plataformas.

Sobre el acceso a datos con fines de investigación científica, innovación y desarrollo

Usar conceptos imprecisos como “bien común” puede ser arriesgado a la hora de concretar ámbitos de aplicación que pueden ser contraproducentes en la protección de los datos personales.

La utilización del concepto de datos para el “bien común” puede dar lugar a ambigüedad, convirtiéndolo en un “cajón de sastre” con el que pervertir la utilización de datos por parte del sector público y privado. Es necesario replantearse el uso de datos para el bien común, no solo por la vaguedad del

concepto, sino por la potencial pérdida del derecho a la privacidad como ejercicio de la autonomía personal. Si existe una autoridad que puede determinar cuándo un uso de datos es por el bien común, estamos privando a los individuos del derecho a la privacidad que debería ser irrenunciable conforme al artículo 8 de la Carta Derechos Fundamentales de la Unión Europea. Actualmente ya existen bases legitimadoras del uso de datos personales para fines de interés general e investigación, por lo que la potencial intencionalidad de incluir el término “bien común” puede suscitar preocupaciones.

Propuestas

- Eliminar la idea ambigua del “bien común” como justificación para el uso de datos personales.

Sobre la herencia digital

Garantizar la herencia digital es una innovación jurídica que afecta directamente a la legislación en materia de propiedad intelectual que será necesario reformular para que los derechos de uso y disfrute de las licencias de las cuentas de uso de servicios sean susceptibles de transmisión.

Nos gustaría aplaudir en este apartado la iniciativa de la Carta de reconocer el derecho de los bienes y derechos de herederos cuando la persona titular de ellos fallezca.

Es especialmente importante aquí realizar una enmienda a la actual Ley de la Propiedad Intelectual que garantice que los derechos de uso y disfrute cedidos como parte de una licencia de uso y copia digitales. Por ejemplo, las que ocurren mediante servicios de compra de material digital, como libros electrónicos, audiolibros o música. La enmienda deberá de garantizar la capacidad de herencia mediante el uso de cuentas en el servicio, identificadas a nombre de los herederos, o bien mediante la capacidad legal de obrar en nombre de la persona fallecida, a través de su cuenta anterior, pudiendo reclamar el acceso a la misma los herederos.

En otro orden de cosas, se puede considerar también que los perfiles en redes sociales u otras plataformas digitales son también patrimonio e imagen pública de la persona fallecida, y es importante garantizar el acceso a los mismos a los herederos para poder disponer de este patrimonio, así como permitir la gestión de la imagen póstuma de la persona fallecida.

Además, sería necesario reconocer el derecho de las personas vivas a nombrar y repartir su legado digital en herencia así como la gestión de su imagen póstuma digital.

En la LOPDDD se describe parte del legado digital respecto a la gestión de los datos personales que ya obren en el poder de diferentes responsables de su tratamiento, pero resultaría conveniente articular también la capacidad y límites de, por ejemplo, actuar en nombre póstumo de esa persona de cara a su imagen y representación públicas.

Propuestas

- Para garantizar el derecho a la herencia digital deberá revisarse la legislación en materia de propiedad intelectual.
- Es necesario que los derechos de uso y disfrute de las licencias de las cuentas de uso de servicios sean susceptibles de transmisión.
- Los perfiles de plataformas digitales deben ser considerados patrimonio e imagen pública del fallecido y, por lo tanto, ser susceptibles de transmisión con todos los derechos asociados que ello conlleva.

Sobre los derechos de igualdad

La brecha digital en todas sus manifestaciones cuenta con una serie de componentes educativos, sociales y económicos que hay que comprender y atacar con políticas públicas. No se puede pensar la brecha digital de una manera unitaria, sino que hay que dirigir actividades transversales más allá del mundo digital.

Además de políticas socioeconómicas, hay que buscar mecanismos de corregulación y regulación estatal para garantizar la inclusión en la brecha de habilidades y de accesibilidad para personas con discapacidad.

¿Igualdad para quién?

Reconociendo la importancia de garantizar la igualdad efectiva en el entorno digital, se señala la necesidad de reconocer otros ejes de discriminación y colectivos vulnerables que se están viendo especialmente afectados por el impacto tecnológico más allá del género. Las condiciones raciales y económicas

son factores de discriminación en el seno de algunas tecnologías como la inteligencia artificial, el reconocimiento facial o la automatización algorítmica.⁷

De este modo se insta a contar con una regulación, independientemente de la fórmula escogida, que pueda garantizar la igualdad efectiva y la no discriminación en el entorno digital.

Entre otras, se propone que los proyectos de analítica de datos tanto en el sector público como privado, deben acogerse a una regulación -ya sea regulación estatutaria, co-regulación o autorregulación- que establezca criterios proactivos de igualdad que deberán ser auditables - sobre auditabilidad, transparencia y análisis de datos Véase *Derechos ante la inteligencia artificial*.

Algunos de estos criterios proactivos de igualdad pueden ser:

- Conocer el entorno explorado por el análisis de datos
- Analizar el contexto previo al análisis de datos
- Incluir equipos diversos en el proyecto, no solo en cuanto a edad, género y raza. Es necesario incluir integrantes de otras disciplinas que ayuden a dar contexto al análisis de datos, ayudando a evitar potenciales consecuencias negativas sobre la población estudiada.

Acabar con las brechas digitales

Atacar la brecha digital en todas sus manifestaciones y, en particular, en aquellas tres señaladas por la literatura: brecha de acceso, de habilidades y de resultados, requerirá de políticas públicas transversales que no se centren únicamente en el componente tecnológico. En este sentido, los condicionantes socioeconómicos y educativos son determinantes en el desarrollo de la brecha digital⁸, por lo que se insta al desarrollo de políticas públicas económicas, sociales y culturales que ayuden a paliar esa brecha. Del mismo modo, felicitando las propuestas concretas en materia de educación digital, es necesario incluir y desarrollar el aspecto social de las habilidades digitales, fomentando políticas públicas para el crecimiento de la participación por parte de la sociedad civil.

Asimismo, se señala la necesidad de incluir a las empresas en las obligaciones y responsabilidades de hacer la tecnología de un modo más abierto e inclusivo. Las empresas tienen un papel crucial en el desarrollo de la alfabetización tecnológica, por lo que se insta a la utilización de instrumentos de co-regulación que llamen a las buenas prácticas y adopción de estándares en el desarrollo de contenido y la experiencia de usuario.

⁷ Eubanks, V. (2018) "Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor". St. Martin's Press.

⁸ Helsper, E. (2015). Survey on the use of information and communication technologies in Brazilian households: ICT households 2015. São Paulo, Brasil: Comitê Gestor da Internet no Brasil. 175-185; Van Dijk, J. & Van Deursen, A. (2014) Digital Skills. Unlocking the Information Society. Palgrave Macmillan; Van Deursen A. & Helsper, E. J. (2015). The third-level digital divide: Who benefits most from being online? Emerald Studies in Media and Communications, 10

El uso de buenas prácticas y programas de *user experience*, gestión de contenidos y desarrollo de aplicaciones adaptables a dispositivos móviles puede hacer el uso de aplicaciones más accesibles a aquellos grupos vulnerables. Así, los sectores socio-económicamente vulnerables tienen una mayor posibilidad de acceder a un dispositivo móvil antes que a un ordenador. Así mismo, realizar aplicaciones de mayor calidad y páginas web adaptables a dispositivos móviles puede fomentar el acceso de estos grupos a otro tipo de contenido. Del mismo modo, se insta a que se adopten buenas prácticas de accesibilidad en el sector privado.

Es importante definir qué es una conexión de calidad. La obligación de servicio universal ya establece un mínimo de conexión de 1mbps; sin embargo, este tipo de conexión no es capaz de soportar las necesidades de consumo mínimas para el libre desarrollo de la persona en internet.

Propuestas

- Fomento de la sociedad civil, programas y financiación para promover mecanismos de alfabetización digital en el seno de la sociedad civil de manera local, pudiendo alcanzar a grupos más vulnerables.
- Promover mejoras en la experiencia de usuario y la gestión de contenidos mediante instrumentos de co-regulación que ayudarán a incentivar el uso de las tecnologías en colectivos de baja alfabetización digital.
- Fomentar colaboración público-privada para la investigación en experiencia de usuario y human-computer interaction. Fomentar esta línea de investigación en universidades públicas de cara a obtener datos, pruebas empíricas y mejoras en la experiencia de usuario para el fomento de la inclusión digital.
- Dotar de un plan de implantación, seguimiento e indicadores de evaluación para las propuestas de la Agenda Digital en este ámbito para garantizar su cumplimiento y efectividad; en particular, a los programa de formación digital para la ciudadanía; programa de digitalización y desarrollo de competencias digitales en educación; programa de competencias digitales para empleados y desempleados; y programa de especialistas en tecnologías digitales básicas y avanzadas.

Sobre la igualdad de las personas con discapacidad en el entorno digital

Se necesitan mecanismos que garanticen condiciones de accesibilidad para personas con discapacidad más allá de la posible comprensión de su información y de las condiciones legales. Independientemente del mecanismo elegido, será necesario desarrollar obligaciones para que los prestadores de servicio incluyan medidas accesibles para diferentes tipos de discapacidad.

Accesibilidad implica, por tanto, que las personas discapacitadas puedan beneficiarse del entorno digital del mismo o modo que lo hacen las personas sin discapacidad. Excluir a las personas con discapacidad del contenido existente en Internet, da lugar a su exclusión de un potencial tejido productivo, social y educativo. Si bien actualmente el Real Decreto 1112/2018 impone obligaciones en materia de accesibilidad web para el sector público, sería necesario trasladar esas mismas obligaciones al sector privado.

Las tecnologías de la información son una herramienta muy potente para garantizar la inclusión de las personas con discapacidad en el entorno digital -la inteligencia artificial, por ejemplo puede usarse para la descripción automática de imágenes o la generación de subtítulos-, pero las empresas no suelen tener incentivos para invertir en ellas de cara a generar entornos accesibles.

Por otra parte, no existen datos para analizar empíricamente cómo atacar los problemas de accesibilidad debido a la falta de incentivos. Es por ello que se proponen medidas como:

Propuestas

- Incentivar programas de colaboración público-privada para analizar problemas y soluciones en el diseño de aplicaciones y mejorar la accesibilidad y experiencia de usuario.
- Fomento de las buenas prácticas en materia de accesibilidad mediante instrumentos de co-regulación o imposiciones legales. Algunas buenas prácticas de accesibilidad se encuentran en normativas ISO ya existentes, el W3C o The Ally Project.
- Repensar la aplicación de la ley de propiedad intelectual para reducir las barreras en materia de propiedad intelectual con el fin de facilitar la adaptación de contenidos para personas con discapacidad mediante el uso de las tecnologías de la información. Del mismo modo que el Tratado de Marrakesh facilita la adaptación del libros al braille, es necesario formular un mecanismo que facilite que la tecnología pueda usarse para promover la accesibilidad sin problemas de propiedad intelectual.
- Elevar la categoría del actual Artículo 100.3 de la Ley de Propiedad Intelectual a Derecho digital, e incluir para los propósitos de accesibilidad, el derecho a poder utilizar APIs y servicios en línea de formas que puedan modificar el servicio original, por ejemplo, mediante “WebExtensions”, “plugins” u otros mecanismos de interceptación de la capa de presentación de los servicios, para poder adaptarlos a las circunstancias de accesibilidad necesarias, incluso sin el permiso de los titulares de los derechos de explotación.

Protección de menores en el entorno digital

Siendo conscientes y proclamando la libertad de educación que tienen los padres para con sus hijos, la actual redacción de la carta pone la responsabilidad exclusivamente en el lado de los padres. El relato de que el usuario es siempre el eslabón más débil y el único responsable de sus actos en Internet no funciona cuando su capacidad para maniobrar en Internet viene predeterminada por desigualdades socio-económicas preexistentes (Véase Brechas Digitales).

Determinar la exclusiva responsabilidad de los padres sobre lo que sus hijos hacen en el entorno digital puede dejar desahuciados a menores en entornos más vulnerables, así como a sus familias. No es posible reclamar la misma responsabilidad a familias que están condicionadas, imposibilitando el desarrollo de sus capacidades digitales. En este sentido, el fenómeno de

“servicio premium” o servicios de tarificación adicional es un problema del que los menores han sido especialmente partícipes⁹. La posibilidad de suscripciones mediante pago a un “click” son una práctica habitual que convierte a los menores en un objetivo fácil para los prestadores de servicios.

Si bien no se puede pretender poner exclusivamente la responsabilidad en los proveedores de servicios, no se puede exigir responsabilidad a la parte débil de la relación asimétrica: el consumidor y, en este caso, el menor. Construir ese relato de manera institucional puede acentuar la asimetría de poder, especialmente en grupos vulnerables.

Por último, y estrechamente relacionado con el relato institucional que deja la carta, llama poderosamente la atención que se prohíba “*las prácticas de perfilado susceptibles de manipular o perturbar la voluntad de los menores*”, dando lugar al permiso para utilizar técnicas de perfilado con fines de manipulación en mayores de edad.

Propuestas

- Se insta a reflexionar sobre que la responsabilidad de la protección de menores en el entorno digital recaiga exclusivamente sobre los padres.
- El hecho de prohibir explícitamente el perfilado y la manipulación de menores genera dudas sobre si esto lo habilita en mayores de edad.

Sobre la libertad de creación y acceso a la cultura en el entorno digital

Se deben desarrollar leyes para adaptar la producción y difusión científica, artística y cultural a las nuevas tecnologías, y limitar en la medida de lo posible los obstáculos a la creación cultural y su acceso.

⁹ Blog Comisión Nacional de Mercados y Competencia (7 agosto, 2015): “Más protección para los usuarios en los servicios telefónicos de tarificación adicional”. Disponible en: <https://blog.cnmc.es/2015/08/07/mas-proteccion-para-los-usuarios-en-los-servicios-telefonicos-de-tarificacion-adicional/>

El acceso a la cultura en Internet

Los objetos culturales lo son en tanto que objetos sociales. En palabras del proyecto Free Cultural Works *"Cuanto más fácil es reutilizar y derivar obras, más ricas se vuelven nuestras culturas"*¹⁰.

La UNESCO, en la Declaración de México Sobre las Políticas Culturales¹¹, define a la cultura como *"el conjunto de los rasgos distintivos, espirituales y materiales, intelectuales y afectivos que caracterizan a una sociedad o un grupo social. Ella engloba, además de las artes y las letras, los modos de vida, los derechos fundamentales al ser humano, los sistemas de valores, las tradiciones y las creencias"*.

El entorno digital ofrece oportunidades tanto en el disfrute a la cultura como en la creación artística e intelectual proveyendo herramientas para el acceso, difusión, producción, trabajo colaborativo, etc. Es deber de las instituciones públicas garantizar el acceso de toda la sociedad a estas herramientas, así como dotar a la ciudadanía de las garantías legales para permitir su participación.

Acceso a la cultura y neutralidad de la red

Los proveedores de servicios digitales deben tratar de igual forma a todo tráfico de datos en la red, sin discriminar en función del tipo de información, su origen o su destino. Las instituciones deben velar para que el acceso de los ciudadanos a la información y al uso de las comunicaciones no esté supeditado al criterio o los intereses de estas empresas. Para ello, se debe garantizar la neutralidad de la red, de modo que no se discrimine ni excluya a los ciudadanos en función de su capacidad de acceso a la información.

Promoción de la cultura libre y democratización del contenido para garantizar una ciudadanía libre

Se debe promocionar e incentivar la producción de obras artísticas y culturales con licencias abiertas que permitan su copia, reutilización, remezcla y, en general, la producción de obras derivadas según el artículo 11 de la Ley de Propiedad Intelectual¹², así como la distribución de estas. Organizaciones como Creative Commons¹³ llevan años trabajando en adaptar este tipo de licencias a la legislación de cada país, replicando en gran medida los logros de las licencias

¹⁰ Freedom Defined. "Free Cultural Works. Definition". Disponible en: <https://freedomdefined.org/Definition>

¹¹ Conferencia mundial sobre las políticas culturales. Declaración de México sobre las Políticas Culturales. Ago. 1982. Disponible en: https://culturalrights.net/descargas/drets_culturals400.pdf

¹² Real Decreto Legislativo 1/1996, de 12 de abril por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. Boletín Oficial del Estado núm. 97, de 22 de abril de 1996. Disponible en: <https://www.boe.es/eli/es/rdlg/1996/04/12/1/con>

¹³ Creative Commons Disponible en: <https://creativecommons.org/>

de software Libre y de fuentes abiertas, en las que se inspiran. Otras iniciativas como la Open Knowledge Foundation¹⁴ o el proyecto Free Cultural Works¹⁵ contribuyen a la promoción de la cultura abierta con definiciones y herramientas tecnológicas. Del mismo modo, el conocimiento abierto no solo promueve un sistema cultural abierto, sino que promueve el libre desarrollo de la persona. Así lo explica Yochai Benkler, uno de los principales teóricos de la cultura libre. Así, la cultura libre e interconectada mejora las capacidades de los individuos y su autonomía individual: mejora sus habilidades para hacer más por sí mismos y para sí mismos y enriquece el sistema democrático al poder conectar libremente con otros, contribuyendo a una mejora de la esfera pública.¹⁶

El uso de estas licencias abiertas permite el libre desarrollo de un ecosistema cultural vivo, diverso y fluido. Para ello es indispensable proporcionar el marco legal que respalde y proteja tanto a los autores de las obras originales como a los autores de las obras derivadas y que garantice de oficio la tutela judicial efectiva recogida en el artículo 24.1 de la Constitución Española.

La actuación directa de la Administración sin tutela judicial efectiva ante reclamaciones de propiedad intelectual para limitar la distribución de contenidos, en ocasiones abusadas de forma ilícita, crea una situación de indefensión en los actores que alojan contenido. Esto ocurre porque se invierte la carga de la prueba y pone el esfuerzo administrativo de parte del acusado y no del demandante. Por esto, la decisión de actuar ante reclamaciones de propiedad intelectual debería de requerir la actuación judicial antes de ponerse en manos de la Administración.

La protección de los derechos de explotación debe estar supeditada al interés general del acceso a la cultura y de la ciencia recogidos en el artículo 44.1-2 de la Constitución Española, y no debe ser un impedimento para este acceso ni para la producción cultural.

Una obra tarda en torno a dos generaciones en pasar al dominio público. Limitar la promoción del acceso a la cultura a las obras en dominio público supone un freno a la educación, a la creación y al desarrollo cultural de toda la sociedad.

El acceso abierto promueve la democratización de los contenidos educativos, su producción y mejora colaborativa, su actualización, verificación y corrección continuas, la adaptación a la idiosincrasia y el entrono de la realidad educativa de cada circunstancia y reduce el riesgo de exclusión. En sintonía con iniciativas internacionales como Open Education Consortium¹⁷, se debe incentivar la producción de material docente e investigador con licencias abiertas que permita su uso, modificación, libre distribución y reutilización, así como su producción colaborativa. Para ello, se deben desarrollar políticas públicas que

¹⁴ Open Knowledge Foundation. Disponible en: <https://okfn.org/>

¹⁵ loc. cit. Freedom Defined, <https://freedomdefined.org>

¹⁶ Benkler, Y (2006): *The wealth of networks: How social production transforms markets and freedom*. Yale University Press.

¹⁷ Véase en <https://www.oeconsortium.org/>

promuevan la colaboración entre docentes para el desarrollo y la publicación de material docente con licencias libres.

Con el objetivo de promover la cultura y dotar de herramientas al sistema educativo, Se debe respaldar legalmente el uso de las obras culturales, científicas o artísticas en el ámbito de la educación y la docencia.

La contratación pública debe priorizar el material docente que disponga de licencias libres que permitan su copia, reutilización, remezcla y, en general, la producción de obras derivadas, así como la distribución de estas, en sintonía con la Cape Town Open Education Declaration¹⁸. Así mismo, se debe incentivar la investigación científica en abierto (Open Access¹⁹) por medio de leyes que promuevan la publicación, distribución y publicidad de estudios y publicaciones científicas, así como de los datos en los que se basan. La evaluación del personal docente e investigador por parte de las instituciones públicas debe valorar positivamente los artículos en publicaciones Open Access.

La publicación en abierto de los resultado de las investigaciones y sus datos, defendida internacionalmente por iniciativas como la Declaración De Berlín Sobre el Libre Acceso a la Literatura Científica²⁰ o la Budapest Open Access Initiative²¹, agiliza y abarata costes en la investigación científica, facilitando el acceso a los estudios, sus datos y sus resultados y contribuyendo a una ciencia mejor. En consonancia con la recomendación sobre el acceso y la conservación de la información científica de la Comisión Europa 2020 de 17 de julio de 2012²², toda investigación que reciba fondos públicos debe publicar en abierto y lo antes posible, tanto las publicaciones realizadas como de los propios datos de la investigación, de forma que se logre el objetivo de proporcionar acceso a los lectores a publicaciones científicas y datos de investigación revisados por pares de forma gratuita, y se permita el uso y la reutilización de los resultados de la investigación.

Los algoritmos y herramientas de software destinados a coartar o limitar las posibilidades de acceder a contenidos digitales o producir copias de estos, conocidos como Digital Rights Management o DRM, constituyen una vulneración de los derechos de los ciudadanos y una vulneración de la legislación, dado que impiden la copia o el acceso incluso en los supuestos legítimos reconocidos por las leyes españolas e internacionales. Campañas como "Defective by Design"²³, impulsada por la Free Software Foundation²⁴, son indicativas de la oposición de la ciudadanía a estas tecnologías en todo el mundo. Los criterios de en qué supuestos legales se puede o no copiar un contenido están recogidos en las

¹⁸ Véase en https://www.budapestopenaccessinitiative.org/open_education/read-the-declaration/

¹⁹ UNESCO. "¿Qué es el acceso abierto?". Disponible en: <https://es.unesco.org/open-access/%C2%BFqu%C3%A9-es-acceso-abierto>

²⁰ Véase en: <https://openaccess.mpg.de/Berlin-Declaration>

²¹ Véase en: <https://budapestopenaccessinitiative.org/>

²² Comisión Europea. Recomendación de 17 de julio de 2012 relativa al acceso a la información científica y a su preservación (2012/417/UE) DOUE 194/39. Disponibe en: <http://www.boe.es/doue/2012/194/L00039-00043.pdf>

²³ Véase en: <https://www.defectivebydesign.org/>

²⁴ Véase en: <https://www.fsf.org/>

leyes, y es una decisión que no debe ser usurpada por unos algoritmos ideados por las empresas productoras o distribuidoras de estos contenidos. Por lo tanto, el uso de estas herramientas debe ser regulado por leyes que garanticen que estos sistemas no limitan ni el derecho de copia en los supuestos recogidos por los artículo 31, 31bis, 31ter, 32, 33, 34, 35, 37 y 37bis de la Ley de Propiedad Intelectual ni el acceso a la cultura y la ciencia descrito en la Constitución Española, de forma que estos derechos también sean derechos digitales con la misma efectividad.

Propuestas

- Asegurar la disponibilidad y garantía legal de herramientas que permitan el acceso y creación sobre la cultura.
- Proteger la neutralidad de la red para que no se discrimine a la población según su capacidad de acceso a la información.
- Promocionar la producción de obras artísticas y culturales con licencias abiertas que protejan a la ciudadanía para conseguir acceso a la cultura y la ciencia de interés general recogido en la Constitución Española.
- Priorizar la contratación pública de material docente que disponga de licencias libres y permitan la difusión y reutilización de las mismas.
- Incentivar la investigación científica en abierto para promover la publicación de estudios y publicaciones científicas, al igual que los datos en los que se basan; como puede ser evaluando positivamente al PDI que realice sus publicaciones en abierto.
- Regular que los algoritmos y herramientas destinados a limitar el acceso a contenidos digitales garanticen que no limiten el derecho de copia recogido en la Ley de Propiedad Intelectual ni el acceso a la cultura y la ciencia descrito en la Constitución Española.

Sobre los derechos ante la inteligencia artificial

El uso de inteligencia artificial debe pasar por un proceso que permita conocer los promotores, razones y objetivos de su aplicación para asegurar justicia y equidad. Debe también asegurar la transparencia de su algoritmo y dataset para prevenir la discriminación de determinados sectores, siguiendo la ley de antidiscriminación europea.

Para evitar la manipulación de los usuarios a través de manipulación con Inteligencia Artificial, debe definirse con más exactitud la implicación de ésta en el proceso de perfilado y sugestión del usuario.

Así mismo, el uso de inteligencia artificial en reconocimiento facial y biométrico supone un nuevo reto en el campo de la privacidad y requiere una revisión técnica y jurídica.

La rendición de cuentas en la inteligencia artificial

Acogiendo con agrado las propuestas sobre los derechos frente a la inteligencia artificial, es necesario plantearse tanto las diferentes posibles implementaciones legislativas, como las consecuencias que se deriven de su implementación. Como indica el propio apartado de la Carta existen criterios fundamentales para garantizar el uso de la inteligencia artificial con un enfoque humano. Si bien transparencia, auditabilidad, explicabilidad y fiabilidad son condiciones básicas para un uso de la inteligencia artificial, la actual redacción de la Carta está obviando la rendición de cuentas en el uso de la inteligencia artificial.

No se puede entender un uso de la inteligencia artificial justo, transparente e igualitario sin la rendición de cuentas. Definiendo rendición de cuentas como el proceso por el cual entendemos las finalidades, justificaciones y propósitos para los cuales se está utilizando una decisión automatizada o inteligencia artificial en un determinado proyecto, plataforma o servicio.

“Algorithmic accountability concerns a networked account for a socio-technical algorithmic system, following the various stages of the system’s life cycle. In this accountability-relationship, multiple actors have the obligation to explain and justify their use, design and/or decisions of/concerning the system and the subsequent effects of that conduct”²⁵.

²⁵ Wieringa, M (2020): “What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability”. *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. 1-18 <https://doi.org/10.1145/3351095.3372833>

"La rendición de cuentas se refiere a la red de responsabilidades socio-técnicas del sistema algorítmico, siguiendo las diversas etapas del ciclo de vida del sistema. En esta relación de responsabilidad, múltiples actores tienen la obligación de explicar y justificar su uso, diseño y/o decisiones con respecto al sistema y los efectos posteriores de esa conducta".

Conocer al promotor del proyecto, sus razones y objetivos para los que quiere usar la inteligencia artificial, así como como los recursos, metodología, perfiles en el proyecto, y de dónde provienen los datos utilizados, es fundamental para evitar potenciales discriminaciones. La rendición de cuentas, por supuesto, debe acompañarse de transparencia.

Algunos criterios que deben ser tenidos en cuenta para evaluar la rendición de cuentas, que deben ser transparentes para los usuarios y cualquier actor externo, son:

- ¿Quién es al promotor del proyecto? ¿Es un decisor público o una empresa privada?
- ¿Para quién va dirigido el proyecto? ¿Cuál es el foro? ¿Es político, legal, social o profesional?
- ¿Cuál es la relación con el sistema de decisiones? ¿Cuál es la perspectiva de la rendición de cuentas? ¿Es con un fin democrático? ¿Es un proyecto piloto?
- ¿Cuáles son los criterios elegidos en el ciclo de desarrollo de software? ¿Cómo funciona el sistema? ¿Cómo se están probando los desarrollos para evitar consecuencias no deseadas?
- ¿Cuál es el resultado que proyecto espera? ¿Cuál ha sido el resultado real?

Documentar todos estos criterios de manera transparente debería ser la norma en todos los proyectos relacionados con las decisiones automatizadas. Para ello, un sistema de co-regulación, así como una legislación nacional o supranacional, pueden ser una buena solución.

En el punto número dos de este apartado, que está referido al derecho a no ser objeto de decisiones automatizadas y recogido actualmente en el Reglamento Europeo de Protección de Datos, hay que tener en cuenta que ha sido fuente de críticas por la academia. Así, este derecho no recoge el derecho a que se explique el algoritmo, sino que solo prevé la posibilidad de oponerte a la decisión.²⁶

Transparencia, rendición de cuentas y explicabilidad se vuelven cruciales para evitar la discriminación, incluyendo la discriminación indirecta. Actualmente el uso de la algorítmica puede estar vulnerando las normas antidiscriminación de la Unión Europea²⁷ al utilizar datos de carácter no personal para realizar perfilados. Esto se conoce como discriminación indirecta. Un ejemplo de ello es

²⁶ Wachter, S., Mittelstadt, B. and Floridi, L. (2017) "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", International Data Privacy Law. 7 (2) 76-99

el uso de datos no personales ni sensibles para dirigir una oferta de empleo mediante un algoritmo. Si yo decido que el algoritmo debe dirigirse a gente con el atributo “pelo corto”, al tener de media las mujeres el pelo más largo que los hombres estaré discriminando indirectamente a este colectivo. Es por esto que la rendición de cuentas, explicabilidad y transparencia son tan necesarias. Por supuesto, estos criterios deben ser cumplidos de la misma manera en el ámbito del sector público.

Algunas propuestas para lograr de manera efectiva los objetivos de transparencia, explicabilidad y rendición de cuentas son las siguientes:

- Realización de Evaluaciones de Impacto Éticas por parte de cualquier actor que quiera utilizar sistemas con decisiones automatizadas e inteligencia artificial.²⁸
- Establecer requisitos para conocer a la población que se va a impactar, incluyendo sus circunstancias sociales.²⁹
- Uso de equipos multidisciplinares y diversos.

Transparencia y control

Para garantizar la no discriminación ante decisiones automatizadas -no sólo de inteligencia artificial- se requiere control y transparencia sobre el algoritmo y su *dataset*, es decir sobre los datos de aprendizaje, por lo que el tanto el uso de software libre como la publicación de los datos utilizados como open data, son necesidades fundamentales -Véase apartado Open Data.

Debe también garantizarse al usuario final el acceso a la lista de motivos por los cuales determinada decisión ha sido tomada y facilitar los mecanismos que permitan pedir una revisión humana en caso de desacuerdo o error.

Propuestas

- Publicar datasets y algoritmos bajo licencias libres para dar transparencia real.
- Añadir mecanismos de oposición y rectificación ante decisiones automatizadas.

²⁷ Wachter, S. (2019) "Affinity Profiling and Discrimination by Association in Online Behavioural Advertising", Berkeley Technology Law Journal

²⁸ Mantelero, Alessandro. "AI and Big Data: A blueprint for a human right, social and ethical impact assessment." Computer Law & Security Review. 34(2018) 754-772.

²⁹ D'Ignazio, C. and Klein, L. F (2020): Data feminism. MIT Press.

Accesibilidad, usabilidad y fiabilidad

La inteligencia artificial es un sistema de aproximación y predicción inexacto que sirve para apoyar otras tecnologías o hacer simulaciones teóricas, en ningún caso debe ser considerado como una decisión completamente irreprochable. En todo caso, se puede hablar de un porcentaje de exactitud aproximado basado en el tamaño del *dataset*, la cantidad de pruebas realizadas y los resultados obtenidos. Todo ello debe plantearse de una forma transparente, clara y legible para el usuario.

Para asegurar la accesibilidad habría que asegurarse también de que en el *dataset* y la interfaz, se han tenido en cuenta las diversas necesidades de grupos de usuarios diversos.

Propuestas

- Plantear de forma transparente que la IA no es exacta, es una aproximación, y hacérselo saber al usuario.

Prohibición de sistemas IA dirigidos a manipular la voluntad de las personas

Este punto de la Carta suscita muchas dudas respecto a su interpretación y aplicación. Esto podría implicar que los sistemas de anuncios basados en perfiles y huella digital no estarían permitidos, al igual que cualquier campaña no requerida por parte del usuario que haga uso de la información tanto pública como privada de dicho usuario. En tal caso habría de definirse con más exactitud qué se considera dirigido a manipular o perturbar la voluntad de las personas.

También habría de revisarse la implicación de la Inteligencia Artificial en dicho proceso, para evitar que sí se contemple la posibilidad de utilizar Inteligencia Artificial de asistencia con otro objetivo inicial pero cuyo objetivo final sea la manipulación y perturbación del usuario.

Para todo ello vuelven a ser fundamentales los requisitos de explicabilidad, transparencia y, sobre todo, rendición de cuentas.

Propuestas

- Definir qué se considera "dirigido a manipular o perturbar la voluntad de las personas", al tratarse de un texto muy amplio.

Tecnologías de reconocimiento biométrico y facial

La implantación de las nuevas tecnologías relacionadas con el reconocimiento biométrico y en concreto facial, suponen una oportunidad en el campo de la vigilancia y la seguridad pero, sobre todo, un enorme reto a afrontar en el campo de la privacidad.

Actualmente estas tecnologías se encuentran cuestionadas por la eficacia de su funcionamiento en casos como la detección de ciudadanos con mascarillas³⁰ y generan dudas al ser desplegadas en espacios públicos y privados, permitiendo recabar datos biométricos altamente protegidos sin apenas requerir la aceptación consciente de la cesión de dichos datos por parte de la población, que se ve afectada por dichas tecnologías simplemente al pasear por un espacio público³¹.

La necesidad de estas tecnologías también está siendo puesta en duda por sus sesgos a la hora de tratar datos de personas de color, mujeres o niños³², acentuando la discriminación de estos grupos, así como de minorías infrarepresentadas que habitualmente son las personas de mayor vulnerabilidad social.

Así mismo, el hecho de recabar toda esta información biométrica de gran valor, se convierte también en un reclamo para posibles atacantes informáticos que podrían utilizar estos datos para suplantar a las víctimas o utilizar dicha información en su contra.

Por todo esto se plantea la necesidad de crear un espacio propio en el que incluir derechos de los ciudadanos con respecto a estas tecnologías de reconocimiento biométrico.

Al ser unas tecnologías accesorias y prescindibles para la provisión de muchos de los servicios en los que se están utilizando, como en el acceso al transporte público, check-in en aeropuertos o en eventos deportivos y culturales, se insta a proveer de un derecho que permita a la población acceder a estos servicios evitando el tratado de sus datos por algoritmos de reconocimiento biométrico.

Se señala también la necesidad de crear una regulación concreta y estricta para el uso de esta tecnología, que podría incluir la prohibición de su uso en menores de edad, en espacios públicos como hospitales, colegios, estaciones de tren o vías públicas, así como impedir su uso en el sector de la vigilancia, tanto por parte de las fuerzas y cuerpos de seguridad del estado, como por empresas privadas.

Es por esto que se insta a abrir un amplio debate entre administraciones, empresas y sociedad civil acerca del peligro que la implementación de esta

³⁰ National Institute of Standards and Technology. "FRVT Face Mask Effects". Disponible en : https://pages.nist.gov/frvt/html/frvt_facemask.html.

³¹ BELLIO, N (11 agosto, 2020) : "Spain's largest bus terminal deployed live face recognition four years ago, but few noticed". Disponible en: <https://algorithmwatch.org/en/story/spain-mendez-alvaro-face-recognition/>

³² National Institute of Standards and Technology. "Face Recognition Vendor Test (FRVT) Ongoing". Disponible en: <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing>

tecnología supone, y si su uso debe ser totalmente prohibido, como ya está sucediendo en múltiples lugares como Boston³³ o San Francisco³⁴, y como demandan múltiples asociaciones y colectivos^{35 36 37}.

En nuestro país ya hemos visto varios casos sobre el tema en los que la Agencia de Protección de Datos ha indicado, que en concreto el reconocimiento facial para su uso en seguridad privada está, en principio, prohibido en la legislación española ya que debe existir un "interés público esencial" para su uso, al tratarse de una tecnología enormemente intrusiva, por lo que no se puede justificarse su utilización en base al interés legítimo. Su uso no es proporcional.

Se insta en definitiva a impulsar y endurecer la legislación al respecto de la identificación biométrica y la protección de datos, así como a dar mas peso y financiación a la autoridad independiente encargada de que se cumpla dicha legislación, la Agencia Española de Protección de Datos (AEPD). La AEPD debe disponer de más medios para poder iniciar un mayor número de investigaciones al respecto, así como disponer de nuevos canales más ágiles para poder actuar.

Propuestas

- Crear un espacio propio en la Carta para incluir los derechos de los ciudadanos con respecto al reconocimiento biométrico.
- Añadir el derecho a que el ciudadano pueda acceder a servicios públicos sin tener que ceder sus datos biométricos.
- Abrir el debate sobre la prohibición de esta tecnología y crear una regulación muy estricta para el uso de la misma.
- Aumentar la financiación de la AEPD y conferirle más medios y canales para luchar contra las infracciones de protección de datos.

³³ Boston City Council (24 junio, 2020). Committee on Government Operations. "Report of Committee Chair". Disponible en: <https://www.documentcloud.org/documents/6956465-Boston-City-Council-face-surveillance-ban.html>

³⁴ Electronic Frontier Foundation (6 mayo 2019). "Stop Secret Surveillance Ordinance". Disponible en: <https://www.eff.org/document/stop-secret-surveillance-ordinance-05062019>

³⁵ Véase en: <https://www.banfacialrecognition.com/>

³⁶ Véase en: <https://reclaimyourface.eu/>

³⁷ Véase en: <https://bigbrotherwatch.org.uk/>

Sobre los derechos digitales en el empleo de las neurotecnologías

Las neurotecnologías pueden suponer un gran cambio en la sociedad humana tal y cómo la conocemos en los próximos años, por eso es importante poner atención en reducir las desigualdades que potencialmente generen y en profundizar en la protección del individuo que las utilice.

Con respecto a los derechos digitales en el empleo de neurotecnologías, resulta manifiesta una falta de intencionalidad con respecto a los objetivos de estos derechos, más allá de los estipulados en el primer punto. Por otra parte, este primer punto, según la lectura de los autores de este documento, creemos que habría de formar parte de las salvaguardas éticas del código deontológico de la medicina y la salud pública.

Se percibe en falta una definición más exhaustiva sobre las neurotecnologías, ya que en un sentido restringido podrían aplicarse solamente a aquellos implantes o productos que puedan incrustarse en el sistema nervioso del cuerpo humano. Sin embargo, creemos que esta definición deja fuera una discusión más importante sobre la percepción misma del transhumanismo, al abordar solamente una de las verticales en las que se encuadra la posibilidad de entre las modificaciones corporales ex-vivo posibles hoy, y en el futuro.

Antecedentes

Las extensiones humanas tecnológicas llevan entre nosotros desde la invención de las gafas, o de las prótesis para miembros perdidos. Sin embargo, en los últimos años la tecnología ha progresado a pasos agigantados, hasta el punto en que disponemos de procedimientos médicos que nos permiten alterar partes mucho más intrínsecas a lo que es nuestra identidad. Anteriormente, esto podía no parecer un problema ya que, mayoritariamente, la pretensión solía quedar restringida a permitir una equiparación con estados anteriores de la propia persona (principalmente, por la pérdida de miembros, piezas dentales, o sentidos). Sin embargo, hoy en día tenemos ya tratamientos que son, por ejemplo, capaces de alterar no solo el estado del ánimo³⁸, sino también la personalidad de quien está bajo tratamiento, como ocurre con ciertos tratamientos para el Parkinson³⁹.

³⁸ González-Hernando, C.; Souza -deAlmeida, M.; Martín-Villamor, P.; Cao-Torija, M.J. y Castro-Alija, M.J. (2013) La píldora anticonceptiva a debate. *Enfermería Universitaria*. Vol. 10, Núm 3. Disponible en: [https://doi.org/10.1016/S1665-7063\(13\)72635-6](https://doi.org/10.1016/S1665-7063(13)72635-6) (Open Access)

³⁹ Aguilar O, Soto C, Esguerra M.(2011): Cambios neuropsicológicos asociados a estimulación cerebral profunda en enfermedad de Parkinson: Revisión teórica. *Suma Psicológica*, Vol. 18, Nº 2, 89-98. Pontificia Universidad Javeriana, Colombia. Disponible en: <http://www.scielo.org.co/pdf/sumps/v18n2/v18n2a07.pdf>

No solo se están realizando más investigaciones, sino que también se está hablando en el entorno académico de los límites éticos de estas modificaciones. Por lo tanto, un sector de la población ya cree que será cuestión de tiempo que acaben ocurriendo, no solamente mediante modificaciones corporales, sino también mediante recodificaciones genéticas in-vivo (o in-vitro), mediante técnicas como, por ejemplo, CRISPR-Cas9.⁴⁰

Bajo esta perspectiva, podría caber considerar no solamente la identidad de nuestros ciudadanos, sino también de garantizar la salvaguarda de la identidad de su progenie, legislando en consideración con los beneficios, riesgos, y límites de la percepción de identidad compartida con sus progenitores.

Otro sector de la población se sitúa en contra de estas modificaciones y cree que un debate de la sociedad civil todavía es necesario y que podría ser razonable prohibir o limitar las modificaciones de las capacidades humanas de forma directa, mediante derecho nacional y/o internacional.

Consideraciones

El debate está abierto, pero esta Carta no parece establecer ninguna posición clara al respecto y se hecha en falta en el texto una intencionalidad y una hoja de ruta al respecto.

En cualquier caso, proponemos que esta cuestión forme parte del debate público y que la sociedad civil pueda pronunciarse al respecto de tecnologías que, en definitiva, podrían tener la capacidad de cambiar nuestra propia identidad colectiva.

No obstante, es de agradecer que se haya motivado la inclusión de esta nueva realidad en el debate público, y que esto permita a la sociedad civil añadir estas preocupaciones al desarrollo social y político si bien creemos que el resultado final es insuficiente, por falta de pronunciación en cuanto a la dirección a tomar.

En particular, nos parece importante definir una serie de intenciones con respecto a estas posibilidades de aumentaciones, tanto en el desarrollo, investigación e innovación, como en la disposición de fondos públicos para tales objetivos y de cara a proporcionar un acceso no discriminatorio a la tecnología.

Nuestra proposición

Es evidente que esta tecnología todavía es altamente novedosa y, por lo tanto, difícilmente legible o garantizable, mientras no sepamos a qué nos estamos realmente enfrentando. Por una parte, es posible aventurar que tendremos una sociedad en la que el acceso a ciertos trabajos quede restringido, *de facto*, a personas con capacidades aumentadas. En este ámbito, parece prudente

⁴⁰ Song, G.; Chen, K.; Kong, X.; Khattak, B.; Xie, C.; Li, A. y Mao, L. (2016): CRISPR/Cas9: A powerful tool for crop genome editing. *The Crop Journal*. Vol. 4(2), pp. 75-82. Disponible en: <https://doi.org/10.1016/j.cj.2015.12.002>

establecer unas bases mínimas sociales en estas situaciones como las que se proponen a continuación.

Se garantizará la dignidad de la persona, la igualdad y la no discriminación en el empleo de las neurotecnologías y otras tecnologías que permitan el aumento cognitivo o la potenciación de otras capacidades de las personas.

El Estado promoverá un plan público de acceso a tecnologías para el aumento y la gestión de habilidades que permita a personas elegibles por motivos económicos y en concurrencia competitiva, acceder a estas tecnologías.

En particular, y conforme a la normativa vigente y la jurisprudencia, se garantizarán los medios necesarios para el acceso en igualdad de condiciones a la educación, incluyendo la educación superior y senior. Esto podrá regularse en el futuro, o bien mediante la limitación de mejoras, o bien mediante un sistema de becas, dependiendo de la voluntad social a largo plazo.

En complementación al derecho al trabajo⁴¹, se garantizará el acceso a puestos sin discriminar respecto de la existencia de implantes cognitivos. Será ilegal discriminar en una oferta de trabajo por la existencia de implantes, junto al resto de motivos, siempre que esto no proporcione ventajas injustas.

El Gobierno elaborará un plan que garantice, cuando se requiera el uso de neurotecnologías para el trabajo, en qué condiciones puede ser esto posible para la empresa, velando de no limitar el acceso al trabajo en igualdad de condiciones.

En vista de la creciente importancia de la tecnología y dada la capacidad de las neurotecnologías del incremento de productividad social, se promoverá la investigación y desarrollo público y privado en las mismas a través del plan nacional de investigación

Dados los inherentes riesgos derivados del tratamiento de datos personales, así como de la potestad y agencia sobre los mismos por parte de terceros al utilizar tecnologías que permitan el aumento cognitivo o la potenciación o limitación de otras capacidades de las personas, se promoverá la transparencia respecto a los usuarios en cuanto a la tecnología utilizada, de forma que en caso de que la empresa que proporciona un determinado producto pueda garantizar que, incluso si fuese a la quiebra, pueden garantizarse la vida de las personas previamente sometidas a esta tecnología, así como una transición posible a otro estado, o bien utilizando tecnología alternativa, o bien permitiendo el cese del uso de la misma.

En cualquier caso, la persona sometida al uso de esta tecnología será informada respecto a la información que pueda obtenerse de ella.

El consentimiento nunca será una base legitimadora del tratamiento de datos en este caso, sino que solamente podrán utilizarse las bases relativas al uso efectivo de la tecnología y nunca para ningún otro propósito, incluyendo el de

⁴¹ Artículo 35.1, Constitución Española; Artículo 23.1 Declaración Universal de los Derechos Humanos

archivo o fines históricos (salvo información agregada que garantice cumplir el secreto estadístico), según el Reglamento de Protección de Datos.

El acceso a neurotecnología y otras tecnologías que permitan el aumento cognitivo o la potenciación o limitación de otras capacidades de las personas será regulado por Ley, y España velará por la armonización internacional de este Derecho, en particular, a nivel Europeo y las Naciones Unidas.

Por último se insta a abrir un amplio debate público acerca del peligro que puede suponer la utilización de este tipo de tecnologías, así como a analizar la posibilidad de incluir una regulación estricta en su uso o incluso una prohibición si así se considera.

Propuestas

- No discriminación en el uso de neurotecnologías y en concreto en el acceso a la educación y en el trabajo.
- Definir un plan público de acceso a tecnologías para el aumento de habilidades con el fin de reducir posibles desigualdades.
- Definir un plan público de investigación en neurotecnologías.
- Crear medidas para garantizar la mantenibilidad de las tecnologías y la transparencia en su funcionamiento y en la información que generen.
- Crear regulación para una limitación estricta del tratamiento de los datos generados a únicamente el uso efectivo de la tecnología y para ningún otro propósito.
- Abrir un amplio debate público sobre la regulación estricta o incluso prohibición de estas tecnologías.

Derechos relacionados con entidades públicas y privadas

Sobre el derecho a la seguridad digital

La Seguridad Digital es un tema amplio y complejo que debe ser definido con claridad, diferenciando sus características específicas en distintos ámbitos y a distintos niveles, y para el que quizás ya existan herramientas jurídicas e institucionales adecuadas.

Para hablar del derecho a la seguridad digital es importante definir este concepto que en la carta no ha sido concretado por lo que comenzaremos estableciendo las posibles interpretaciones y caminos de la definición de seguridad digital.

También describiremos las potenciales implicaciones de la seguridad digital (en el sentido de la definición de entorno digital que ofrece la Carta). Partiendo de esa definición, debemos entender que a efectos de gobernanza, el entorno digital está dividido en tres capas: física, lógica y de contenido. Por lo tanto, garantizar la seguridad digital va a implicar garantizar la seguridad en esas tres capas, lo que va a conllevar la interacción de diferentes bienes jurídicos protegidos y derechos colindantes en cada una de esas tres capas.



Necesidad de definición de la seguridad digital

La alusión directa en el apartado VI a *“siempre en colaboración con las empresa tecnológicas”* sobre cómo garantizar la seguridad digital plantea ciertas cuestiones. En primer lugar, podría interpretarse como una intención de privatizar la seguridad digital.

En este sentido es importante saber qué se entiende como seguridad digital, y definirlo como tal. Si lo que se pretende con esta carta es trasladar la misma garantía de derechos que existe en el mundo *offline* al mundo *online* debemos tener en cuenta que la “seguridad pública” es una competencia reservada a las Fuerzas y Cuerpos de Seguridad del Estado⁴². Actualmente existen ya los mecanismos en los cuerpos de seguridad del Estado en lo que se refiere a delitos relacionados con el entorno digital.

Es necesario desarrollar el concepto de seguridad digital desde un punto de vista del derecho constitucional si se pretende desligar de la rama de la seguridad pública y de la competencia existente de los cuerpos y fuerzas de seguridad, así como terminar de encajarla con la actual Ley de Seguridad Privada. Es por ello que es necesario establecer una definición unívoca de seguridad digital para entender qué rol pueden tener las empresas tecnológicas en una función que es meramente pública.

En este sentido, si se quiere hablar de la seguridad desde un punto de vista preventivo y no solo punitivo, será necesario plantearse diferentes modelos.

En primer lugar, para que se garantice la seguridad desde el punto de vista preventivo, primero tiene que existir una obligación que actualmente no existe. En segundo lugar, debe garantizarse que ese mecanismo y obligación se cumple, no solo desde un punto de vista sancionador, sino desde un punto de vista de soporte y colaboración que son los pilares en los que se basa la legislación europea en ciberseguridad⁴³.

Como potencial modelo al que aspirar, sería óptimo plantear la existencia de una agencia pública o semipública que pueda garantizar el cumplimiento con la norma en seguridad digital, no solo mediante auditoría y revisión, sino desde un punto de vista colaborativo, de formación, apoyo y concienciación. En este sentido, la Agencia Española de Protección de Datos ya tiene actualmente esa competencia reconocida en el artículo 57 del Reglamento Europeo de Protección de Datos cuando dota a las autoridades de control con la potestad de velar por el cumplimiento del reglamento y, por lo tanto, con la obligación de garantizar la seguridad desde el diseño.

Con esto quiere plantearse, primero, que es necesario explicar qué se va a entender como “seguridad digital” y, segundo, que no es necesario, según nuestro punto de vista, reinventar la rueda para llevar estas garantías a cabo. Centrarse en las actuales medidas y competencias que nos otorga el ordenamiento jurídico puede ser positivo para adaptarnos a nuevos retos. Por lo tanto, entendemos que garantizar la seguridad digital es un problema de inversión, financiación y medios materiales más que de innovación jurídica.

⁴² Congreso de los Diputados. Sinopsis del artículo 104. Disponibel en: https://app.congreso.es/consti/constitucion/indice/imprimir/sinopsis_pr.jsp?art=104&tipo=2

⁴³ Dirección de Seguridad Nacional. “Visión global de los instrumentos de la UE en ciberseguridad”. Disponible en: <https://www.dsn.gob.es/es/actualidad/sala-prensa/vision-global-instrumentos-ue-ciberseguridad>

Seguridad digital más allá del ámbito público

Si hablamos de seguridad en el entorno digital a los efectos de la definición de esta Carta es necesario garantizar la seguridad tanto de activos tangibles como intangibles de la ciudadanía. Como explicamos antes, la seguridad digital irá dirigida a la protección de las tres capas. Para ello es necesario garantizar en todas estas capas, todas las dimensiones de la seguridad: disponibilidad, integridad y confidencialidad.

De este modo, cabe preguntarse por la necesidad de imponer obligaciones de seguridad a las empresas que desarrollen tecnología de cualquier ámbito. Actualmente las administraciones públicas tienen qué cumplir el Esquema Nacional de Seguridad (ENS), pero ¿de qué manera vamos a conseguir garantizar el derecho a la seguridad digital?

En el sector privado no existe ninguna obligación de garantizar la seguridad, salvo que se traten datos de carácter personal que caen bajo las obligaciones de seguridad desde el diseño que impone el reglamento de protección de datos. En este sentido es necesario plantearse la viabilidad de un instrumento jurídico que imponga obligaciones en materia de seguridad informática y de la información, del mismo modo que existen requisitos en el sector eléctrico o energético para la venta de productos de manera segura. Así, algunas de las vías más rápidas y flexibles para determinar requisitos regulatorios en una materia tan cambiante son los instrumentos de co-regulación como la obligación de adherirse a códigos de conducta y/o certificaciones, como ya sucede en otros ámbitos.

Propuestas

- Crear una regulación que imponga obligaciones en materia de seguridad informática y de la información tanto al sector público como al privado.

Seguridad en contenido

En lo que se refiere a la seguridad digital en la capa de contenido y sus problemas asociados se plantean varias dudas y cuestiones.

¿Cómo se va a garantizar este derecho de manera que no exista un sesgo económico en la persecución de delitos tecnológicos relacionados con la persona, su identidad digital o con la empresa en el entorno digital? Las actividades relacionadas con la seguridad digital tienen costes muy altos para los usuarios por requerir de conocimiento muy especializado. Conseguir contactar con una empresa o solicitar un peritaje de parte, tiene una fuerte barrera de entrada económica y educativa. Del mismo modo, muchas empresas pequeñas que son víctimas de este tipo de delitos, no pueden permitirse acceder a estos mecanismos. Por lo tanto, hay que plantearse no solo

diferentes teorías jurídicas respecto a lo que consideramos seguridad digital, sino también las diferentes maneras de implantarlas de una manera igualitaria.

Por otra parte, si entendemos la seguridad digital dentro del monopolio de la seguridad pública, dada la extensión del entorno digital habría que plantearse una posible extensión de medios a las administraciones competentes, o incluso plantear la necesidad de un nuevo orden jurisdiccional especializado que esté a la altura de procedimientos ágiles, dada la volatilidad de la información en el entorno digital.

Propuestas

- Se invita a la reflexión sobre cómo garantizar la seguridad en contenido sin crear un sesgo económico a pequeñas empresas o individuos.
- Se insta a aumentar los medios disponibles o a plantear un nuevo orden jurisdiccional especializado y más ágil en el campo de la seguridad digital.

Derecho al cifrado, a la integridad y la privacidad de las comunicaciones

Se señala también la necesidad de introducir el derecho a la integridad de las comunicaciones privadas así como el derecho a que dichas comunicaciones se puedan realizar a través de mecanismos que garanticen la privacidad de las mismas.

En concreto el cifrado de la información, que debería también ser referido como un derecho, permite garantizar, no solo la privacidad, sino también la seguridad de la información.

Es importante que se garantice que dicho cifrado pueda realizarse de extremo a extremo evitando puertas traseras y la existencia de claves de cifrado maestras que permitan acceder a toda información almacenada, como propone EDRI (European Digital Rights)⁴⁴.

Aunque podría parecer útil para proveer de información al poder judicial ante investigaciones en curso, la mera existencia de estas llaves maestras abre la puerta a grandes brechas de seguridad que potencialmente podrían dar acceso a la totalidad de las comunicaciones privadas almacenadas.

⁴⁴ Bits of Freedom, "Position paper on encryption" (25 Ene. 2016) EDRI. Disponible en: <https://www.edri.org/files/20160125-edri-crypto-position-paper.pdf>

Al mismo tiempo, introducir mecanismos que permitan descifrar comunicaciones, incluso con una potencial base legal, es totalmente ineficaz. El acceso a herramientas criptográficas y de comunicación cifrada en el mundo del software (es decir aquellas que nos permitan mantener la integridad y secreto de las comunicaciones) no está bajo control de uno o varios países⁴⁵, sino que implica tecnologías desarrolladas y distribuidas a lo largo de todo el mundo, como indica el criptógrafo Bruce Schneier en su estudio "A Worldwide Survey of Encryption Products"⁴⁶. Es por esto que criminales y terroristas podrían acceder de forma sencilla a herramientas de cifrado que se encuentren fuera del control de los estados legisladores de forma sencilla.

En definitiva, la posibilidad de introducir métodos que debiliten el cifrado o permitan acceder a dicho contenido, no solo se ha demostrado ser una medida ineficaz sino que genera un problema mucho mayor al crear un punto único de acceso y control sobre toda la información. Una vulnerabilidad crítica que nos dejaría totalmente expuestos frente atacantes externos.

Propuestas

- Se debería introducir el derecho a la integridad de las comunicaciones privadas y el derecho al uso de herramientas criptográficas.
- Se debería garantizar concretamente el derecho a utilizar cifrado de extremo a extremo.
- Se debería garantizar la no existencia de puertas traseras o llaves maestras que permitan acceder al contenido de las comunicaciones.

⁴⁵ En su libro, Schneier recuerda que aunque el software esté sujeto a legislación en la jurisdicción que lo origine, la naturaleza de la información (y del software) hacen muy difícil el control de su exportación.

⁴⁶ Schneier, B.; Seidel, K.; y Vijayakumar, S (11 febrero, 2016): "A Worldwide Survey of Encryption Products" 11 Feb. 2016. Berkman Center Research Publication No. 2016-2, <http://dx.doi.org/10.2139/ssrn.2731160>

Sobre los derechos del individuo en relación con la Administración Pública

La administración pública debe garantizar los principios de igualdad y transparencia hacia al ciudadano. Por esto es importante reforzar la publicación de información y el uso de tecnologías libres y estándares interoperables para que cualquier ciudadano se pueda relacionar libremente con ella.

Software libre

Los avances tecnológicos y el crecimiento de la industria, en concreto del desarrollo software, permiten un rápido avance en la digitalización de la sociedad y de la administración pública. Aún así, cabe preguntarse por los detalles de esta digitalización y la pérdida de soberanía que puede traer consigo el utilizar tecnologías privativas con código no auditable o no alojadas en equipamiento informático propio.

La iniciativa "Public money, public code!"⁴⁷ busca promover en la administración pública la utilización de software libre, tecnologías con código público cuya licencia permita su uso, estudio, compartición y posibilidad de mejora para cualquier fin, lo cual favorece la innovación y la competencia, reduce la dependencia de terceros y permite colaborar para crear mejores aplicaciones reduciendo costes.

Se insta a promover de forma clara y directa una regulación que obligue a que todo nuevo desarrollo tecnológico contratado por la administración pública, y por tanto con dinero público, sea desarrollada bajo una licencia libre, permitiendo su auditabilidad y su reutilización.

Así mismo se señala la necesidad de fomentar que en todo contrato público de provisión de software como servicio (SaaS) se incluyan cláusulas que obliguen, o al menos puntúen positivamente, el contratar servicios basados en software libre.

Esta apuesta por el fomento de tecnologías con licencias libres podría ir enmarcada en una estrategia nacional o europea que permitiría mejorar y fomentar la participación ciudadana en el desarrollo y la revisión de los proyectos financiados con dinero público, siguiendo el ejemplo iniciado con la aplicación RadarCOVID donde la ciudadanía ha colaborado proponiendo mejoras y reportando errores a corregir.

Del mismo modo se insta a colocar al Centro de Transferencia de Tecnología (CTT) como el organismo encargado de promover y coordinar el desarrollo de

⁴⁷ Véase en: <https://publiccode.eu/es/>

proyectos libres para la administración. Para ello es necesario dotarlo de recursos para su modernización, con el fin de avanzar en la digitalización de la administración pública en base a compartir el desarrollo de plataformas de código libre entre administraciones con las mismas necesidades, como ayuntamientos, universidades o comunidades autónomas.

Todo nuevo desarrollo debería estar obligado a comprobar si existe ya una solución que cubra sus necesidades en la forja pública de proyectos del CTT, así como a justificar la necesidad de crear un nuevo software en lugar de utilizar las soluciones ya existentes. Por último, todo nuevo desarrollo debería realizarse íntegramente en abierto en dicha forja, asegurando de esta forma que el código sea publicado desde el primer momento.

Cabe destacar el ahorro de costes que esto supondría al eliminar duplicidades en el desarrollo de software, el crecimiento que implicaría en los niveles de transparencia y el grado de auditabilidad del código de la administración pública, Todo ello permitiendo a la administración concentrarse en la innovación en lugar de reinventar la rueda en cada una de sus instituciones individuales. En este sentido se ha pronunciado recientemente la Comisión Europea con la Estrategia de Código Abierto.⁴⁸

De hecho, nuestra legislación ya recoge la necesidad de que las Administraciones Públicas, antes de promover una iniciativa, reutilicen las que ya están previstas en el Catálogo del Centro de Transferencia Tecnológica en aras, no solo de promover la transparencia, sino de evitar duplicidades y gastos para la Administración. Sin embargo, dicho catálogo que recoge todo tipo de soluciones, no necesariamente tecnológicas, parece estar infrautilizado. En el año 2019 solo tenía registradas 351 soluciones y es difícil valorar la eficacia de este catálogo al no existir indicadores eficientes para comparar.

De cara a los futuros desarrollos y presentes aplicaciones, especialmente en el ámbito de las decisiones automatizadas que afectan a los usuarios, es muy necesario que el paso por este registro se haga de manera obligatoria para (i) registrar las soluciones, algoritmos y/o desarrollo de cualquier índole con el fin de hacerlos lo más transparentes posibles, y para (ii) promover la interoperabilidad, la cooperación y evitar la duplicidad de desarrollo en el seno de las diferentes administraciones públicas.

⁴⁸ Comisión Europea (21 octubre, 2020) C(2020)7149. “Open source software strategy 2020-2023. Think open”. Disponible en: https://ec.europa.eu/info/sites/info/files/en_ec_open_source_strategy_2020-2023.pdf

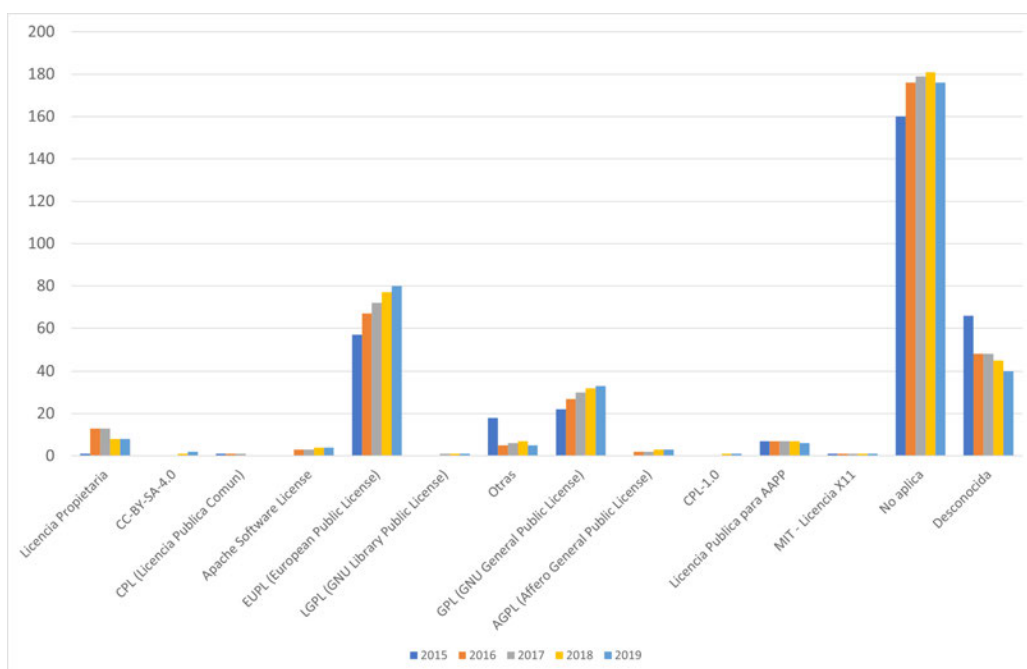


Gráfico: Número de soluciones dadas de alta en el Centro de Transferencia Tecnológica entre 2015 y 2019 (Fuente: CTT)

Aunque el Esquema Nacional de Interoperabilidad (ENI) establece la posibilidad de realizar proyectos de manera abierta, siempre que la unidad los declare proyectos “de fuentes abiertas” y cuenten con licencias que garanticen su desarrollo de manera libre -y no solo abierta-⁴⁹, no existe una obligatoriedad de hacerlo. Esto deja al administrado en una situación de potencial indefensión cuando las decisiones que toma el sistema tienen efecto en una resolución de la administración. Así, de las soluciones registradas en el catálogo entre 2015 y 2019, a la mayoría de ellas no se les aplica una licencia, probablemente por no ser software o sistemas de información. Es decir, parece que con lo que menos cuenta el catálogo es con software.

Por todo esto se insta a aplicar la transparencia por defecto en el desarrollo de código y a publicar con licencias libres, todo código de software anteriormente desarrollado y que esté funcionando como mecanismo automático de decisión o de filtrado para la concesión de ayudas públicas, como es el caso del software BOSCO que determina la concesión del bono social de electricidad. Se señala la posibilidad de que el organismo anteriormente propuesto para la coordinación de desarrollos de código libre, pueda ser el encargado de responder y actuar ante las peticiones de la ciudadanía para conocer el código de dichas tecnologías.

⁴⁹ Según el artículo 16.2 del ENI los principios que deben cumplir las licencias de proyectos de “fuentes abiertas en la Administración Pública son los siguientes: *a) Pueden ejecutarse para cualquier propósito; b) Permiten conocer su código fuente; c) Pueden modificarse o mejorarse; d) Pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas mismas cuatro garantías.*”. Estos principios son aquellos que definen a una tecnología como “libre” tal y como establece el Movimiento de Software Libre.

Propuestas

- Establecer una regulación que obligue a que todo nuevo desarrollo de la administración pública se publique bajo licencias libres.
- Puntuar positivamente el uso de plataformas basadas en software libre al contratar software como servicio (SaaS).
- Desarrollar una “Estrategia nacional para el desarrollo de la administración pública con software libre”.
- Aumentar las competencias y la financiación al Centro de Transferencia de Tecnología (CTT) para fomentar el desarrollo colaborativo de herramientas entre administraciones.
- Obligar a la reutilización o a la adaptación de herramientas ya desarrolladas en la forja del CTT salvo justificación clara.
- Publicar y desarrollar nuevas herramientas de la administración directamente en abierto y en la forja pública del CTT.

Open data

Al igual que el software, los datos generados con dinero público también deberían ser accesibles de forma libre por la sociedad, siempre y cuando sean totalmente anonimizados y/o agrupados, siendo muy estrictos con respecto a aquellos datos que puedan ser relacionados de forma inequívoca con un individuo. Las relaciones con la administración pública deben tener en cuenta el derecho de transparencia y acceso a los datos mediante open data.

Es por esto que se propone añadir en las licitaciones técnicas que incluyan nuevos desarrollos y que generen datos útiles para el ciudadano, la obligación de que estos datos sean publicados con licencias libres por defecto. En concreto se insta a fomentar proyectos de colaboración entre instituciones similares a la “*Plataforma de gobierno abierto, colaborativa e interoperable*”⁵⁰ iniciada por las ciudades de A Coruña, Santiago de Compostela, Zaragoza y Madrid, con la idea de estandarizar el intercambio y la publicación de información en los campos de la participación, la transparencia y los portales de datos abiertos.

Es importante que el intercambio de este tipo de datos se realice de forma estructurada ya que la publicación de información como los presupuestos generales del estado o los datos de incidencia del COVID-19 en formato PDF, ve su utilidad reducida a meramente cumplir con la obligación de información por parte de la Administración. Poder compartir esta información en formatos

⁵⁰ Ciudades e Islas Inteligentes. Agenda Digital para España. Disponible en: http://ondemand2.redes.ondemand.flumotion.com/redes/ondemand2/Portal_DSN/Marzo_2017/Coruna_Madrid_Santiago_Zaragoza.pdf

procesables por algoritmos permitiría que el coste económico que supone el agrupar y generar esta información, pudiera ser sobradamente compensando gracias a la reutilización de la misma, y permitiendo a actores de la sociedad civil realizar también su labor de información, divulgación y auditoría del Gobierno, para mantener una democracia sana en la que la soberanía parta del pueblo.

Del mismo modo, se insta a que la información solicitada y ofrecida por el Consejo de Transparencia, sea recopilada y almacenada de forma pública y accesible por cualquiera una vez es entregada. Es importante que una vez se ha entregado esa información, no sea necesario volver a solicitarla y cualquier ciudadano pueda acceder a la misma y descargarla de forma automática.

Propuestas

- Incluir en los nuevos desarrollos que generen datos útiles para el ciudadano, que estos sean publicados por defecto con licencias libres.
- Fomentar que se publiquen todos los datos posibles generados por la administración en formatos consumibles por algoritmos, no solo en PDF.
- Publicar los datos solicitados y entregados por el Consejo de Transparencia, para que cualquiera pueda acceder a ellos.

Garantizar la igualdad y el principio de neutralidad tecnológica

Reconocer la igualdad de acceso a los servicios públicos y en las relaciones digitales con la Administración no solo implica incluir a los ciudadanos vulnerables en los procesos digitales de la administración. ¡Solo el 60% se relaciona con la administración de este modo!⁵¹⁾ -véase *Acabar con las brechas digitales*-; también implica reconocer distintas realidades tecnológicas garantizando siempre el principio de neutralidad tecnológica.

El principio de neutralidad tecnológica proclama que los ciudadanos no pueden quedar discriminados ni excluidos en sus relaciones con la administración en función de su elección tecnológica, tal y como reconoce el Esquema Nacional de Interoperabilidad. De este modo, el acceso a la administración pública mediante tecnologías libres no debe ser un impedimento en el acceso al mismo. Es por ello que dicha vertiente de la igualdad y neutralidad tecnológica en las relaciones con la administración no solo debe verse reflejada en la Carta, sino que además debe garantizarse.

⁵¹ Instituto Nacional de Estadística. Encuesta sobre equipamiento y uso de Tecnologías de la Información y Comunicación en los hogares 2020.

Es necesario, por lo tanto, generar indicadores eficientes que permitan evaluar de manera eficaz la implantación del Esquema Nacional de Interoperabilidad.

Si bien actualmente existen datos en abierto sobre la digitalización de la administración, estos no son indicadores fiables ni efectivos para analizar ni el estado de la administración digital ni la aplicación del ENS. Los datos aportados se presentan en términos absolutos, y sin posibilidad de establecer un análisis o comparativa que permita contextualizar esos datos.

Un ejemplo de este problema podría ser el número de organismos integrados en @Firma. A fecha 31 de octubre de 2020 un total de 917 estaban integrados en esta aplicación. Sin embargo, esto no permite saber si este es un buen dato o no, puesto que no nos es posible contextualizarlo. Considerando, por ejemplo, que en esa misma fecha había un total de 7.606 organismos registrados en @Clave, probablemente el número de organizaciones registradas en @Firma es bastante bajo. Sin embargo, esto no es contextualizable. Tampoco se conoce la metodología ni lo que se entiende por “organismo” en este contexto. Solo considerando las aproximadamente 19.000 administraciones públicas⁵² que hay en España, todos los datos de digitalización presentados en el Portal de Administración Pública son realmente bajos. Sin embargo, los datos presentados no aportan información relevante para estimar el grado de digitalización de la administración. Se acoge con agrado que existan datos comparables al estandarizarlos estableciendo indicadores para 10.000 habitantes. No obstante, una gran parte de los datos están vacíos.

Algunas propuestas

Es necesario por lo tanto incluir en la Carta el derecho del ciudadano a poder comunicarse con la administración pública, siempre utilizando estándares abiertos e interoperables así como permitir el acceso a cualquier procedimiento utilizando herramientas de código libre y por supuesto gratuitas, por lo que se insta a la aplicación del Esquema Nacional de Interoperabilidad (ENI)⁵³ en la contratación pública.

Se debe establecer un registro de indicadores eficiente y detallado que sea capaz de medir la aplicación del Esquema Nacional de Interoperabilidad. Los indicadores actuales, si bien mide ciertos aspectos de la digitalización de la administración, no son capaces de medir la aplicación del ENI.

Los indicadores deberán basarse, en todo caso, en el respeto al principio de neutralidad tecnológica y, por lo tanto, deberán medir, entre otros, las capacidades que tienen las Administraciones Públicas para integrarse con otros sistemas, formatos y modelos, incluyendo opciones basadas en software no propietario.

⁵² Francisco Nuñez (26 junio 2020). “España: Un Estado con un 'puzle' de 18.850 administraciones”. El Mundo. <https://www.elmundo.es/economia/2016/06/26/576ae93222601d985f8b45f0.html>

⁵³ <https://www.boe.es/eli/es/rd/2010/01/08/4/con>

Establecer procesos de evaluación de los indicadores y las políticas con el fin de dirigir medidas efectivas que garanticen la igualdad en las relaciones con la Administración. Es necesario indagar sobre las razones por las que las diferentes Administraciones Públicas no utilizan medios electrónicos de la manera en la que se espera.

Deberán establecerse procesos de manera coordinada con las diferentes Comunidades Autónomas para no caer en desigualdades regionales.

Propuestas

- Incluir en la Carta el derecho a comunicarse con la administración pública bajo estándares interoperables y utilizando herramientas de código libre.
- Establecer indicadores para medir la aplicación del Esquema Nacional de Interoperabilidad.
- Establecer procesos de evaluación de dichos indicadores y políticas públicas coordinadamente con las Comunidades Autónomas.

Garantizar la transparencia en el uso de decisiones automatizadas en las relaciones con la administración

La transparencia en la relación con los administrados es uno de los principios básicos del Derecho Público y por lo tanto las decisiones automatizadas que formen parte de una resolución administrativa, deben ser abiertas y públicas, además de documentadas de manera inteligible para el administrado.

Algunos autores como Boix Palop⁵⁴ se plantean la necesidad de interpretar el uso de algoritmos en la administración pública como reglamentos, extendiendo las garantías propias de las normas reglamentarias. Si bien la configuración jurídica de los algoritmos es aún muy discutida, lo que sí es seguro es que sean reglamentos o no, forman parte de norma jurídica que prevea su utilización. Es decir, un algoritmo no hace más que aplicar una norma, reglamento o decisión jurídica determinada y, por lo tanto, debe gozar de las mismas obligaciones de transparencia *ex ante* que la norma en sí que lo aplica. Así, Valero Torrijos⁵⁵ también entiende que los detalles del algoritmo deben ser notificados como parte del artículo 40 de la Ley 39/2015 en la resolución al interesado siendo, por tanto, una parte de la garantía *ex ante* que otorga la norma.

⁵⁴ Boix Palop, A (2020): Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones. *Revista de Derecho Público: Teoría y Método*. Vol. 1, pp.223-270.

⁵⁵ Valero Torrijos, J. (2019): Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración. *Revista Catalana de Dret Públic*, 58, pp. 82-96.

Si una resolución administrativa está basada en una decisión automatizada, esta tiene que ser abierta para que sus decisiones sean recurribles, extendiéndose el deber de motivación⁵⁶. De otra parte no podremos hablar de seguridad jurídica para con los Administrados.

Si las decisiones automatizadas forman parte del instrumento jurídico que las contempla, siguiendo los mismos criterios y principios básicos del procedimiento administrativo, significa que están sometidas a los mismos criterios de motivación y seguridad jurídica de las resoluciones administrativas. Por lo tanto, el resultado, los criterios, parámetros y flujos que utilizan las decisiones automatizadas, deben ser conocidos como parte de la resolución en sí, puesto que son la propia aplicación de la norma.

Sin el ejercicio de transparencia del algoritmo y el conocimiento previo de su funcionamiento, no podemos hablar de seguridad jurídica para el administrado, y se podría estar incurriendo en una falta adecuada de motivación de la resolución, dando lugar a una situación de indefensión, y en este sentido se está pronunciando la doctrina administrativa⁵⁷, llegando incluso a plantear la nulidad radical de las resoluciones⁵⁸.

Es decir; ya no solo hablamos del potencial impacto discriminatorio de una decisión automatizada por parte de la administración, sino que la consecuencia tiene un impacto en el propio proceso administrativo. No conocer el por qué de una decisión jurídica que se ha realizado mediante un algoritmo, va a impedir al administrado motivar antecedentes para interponer un potencial recurso a la resolución.

Para ilustrar esto, el Caso de Civio es bastante gráfico. Las asociación Civio lleva varios años intentando que los criterios de denegación y aceptación del bono social eléctrico mediante decisiones automatizadas sean públicos para poder conocer los motivos las resoluciones⁵⁹.

No conocer los criterios que está utilizando el algoritmo para realizar las decisiones automatizadas sitúa a los interesados en una situación de indefensión puesto que no tendrán las herramientas para recurrir, si no conocen sobre qué tienen que recurrir. Por lo tanto, no se les está motivando correctamente una resolución si no se muestra el comportamiento del algoritmo.

Por último, existen dudas concretas sobre especificaciones de la carta que no quedan claras ni dejan clara la intencionalidad:

⁵⁶ Reconocido en el Artículo 35 de la Ley 39/2015 <https://www.boe.es/eli/es/l/2015/10/01/39/con#a35>

⁵⁷ *Op cit* Valero Torrijos

⁵⁸ Ponce Solé, J. (2019). Inteligencia artificial. Derecho Administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico. *Revista Internacional de Transparencia e Integridad*, 6, citado en Valero Torrijos (2019).

⁵⁹ Elisa de la Nuez Sánchez-Cascado “Algoritmos y transparencia” 19 Feb. 2020. Expansión. <https://hayderecho.expansion.com/2020/02/19/algoritmos-y-transparencia-2/>

El párrafo XVI.6 habla de “actividades o decisiones digitales”. Es necesario, en primer lugar, definir qué es una actividad y una decisión digital para dar seguridad jurídica. En segundo lugar, si este apartado da lugar a reconocer una responsabilidad patrimonial de la administración pública respecto al uso de algoritmos, es fundamental reformar las leyes 39/2015 y 40/2015, reconociendo un auténtico estatuto para los algoritmos dentro de la administración como parte del procedimiento administrativo y, por tanto, con todas las garantías que ello conlleva.

Si el párrafo XVI.6 afirma la existencia de una responsabilidad patrimonial de la Administración, habría que plantearse la necesidad de regular la responsabilidad de los algoritmos en el sector privado.

El párrafo XVI.7 reconoce el buen gobierno en el uso de decisiones “en el entorno digital”, pero esto debería implicar una discusión pública de los algoritmos previa a su utilización y una potencial nulidad, en caso de no fundamentarse su uso con la debida transparencia.

Propuestas

- Establecer esquemas y directrices de transparencia en las Administraciones Públicas para la consecución de este objetivo.
- Instar a la utilización del software como código libre, o al menos abierto, para que pueda ser auditable.
- Crear un marco de transparencia y rendición de cuentas para el uso de decisiones automatizadas en la administración pública.
- Llevar a cabo actividades de concienciación social respecto al funcionamiento del uso de algoritmos y a la toma de decisiones automatizadas.
- Reconocer un estatuto para los algoritmos dentro de la administración como parte del procedimiento administrativo y regular su responsabilidad patrimonial en los sectores público y privado.

Sobre la empresa en el entorno digital

Una Carta de Derechos dirigida a las personas físicas no parece la herramienta adecuada para definir las pautas de transformación digital de las empresas.

Creemos que los procesos de transformación digital son imprescindibles para mantener un ecosistema empresarial saludable y, aunque sea mera transposición de un derecho ya existente, aprobamos la inclusión de la libertad de empresa de forma explícita y haciendo mención a su subordinación a los derechos digitales de las personas físicas. Se echa en falta la mención explícita a personas físicas, ya que las empresas, pudiendo ser entidades con personalidad jurídica, podrían reclamar derechos adicionales a los que el espíritu de esta carta pretendiere otorgarles.

Respecto a las condiciones de espacios de pruebas, o “sandbox”, si bien defendemos que puede ser una opción para el desarrollo de negocios en ciertas condiciones, creemos que estipularlo como un derecho del empresario podría ser problemático.

Dada una Carta de Derechos, nos parece un lugar inapropiado establecer acuerdos que pudieran resultar o parecer partidistas o descritos ad-hoc para actores específicos en nuestra sociedad, y preferiríamos que, en este caso, se estableciese normativa mediante una disposición con rango de Ley, pero sin garantizar su existencia como un derecho digital.

Entre otras cosas, la propia definición de un “espacio de pruebas” es problemática al establecerla como un derecho, ya que los límites de dónde terminan y empiezan los derechos de personas y empresas son difusos, y parte del éxito del modelo radica en esta propiedad.

Sin embargo, esto significa que una vez establecidas ciertas condiciones de base, podrían intentar dibujarse líneas más claras de los límites de diferentes derechos contrapuestos en un lugar (y, en particular, los referidos a los datos personales y a la capacidad de empresas de realizar con ellos operaciones que fuera del espacio de pruebas hubieran de ser evitadas).

En este caso, podría verse en el futuro un sector minoritario en cuanto a personas físicas pero mayor en cuanto a poder económico, que pudiese pretender activamente que estas líneas se dibujasen de forma más clara en contra de las personas físicas aún con la redacción actual. Por lo tanto, nos gustaría que esta mención fuese eliminada por completo y, si esto fuese impracticable, realizar una redacción final más cuidada, que redujese su eficacia como garantía de un derecho futuro.

No significa esto que estemos en contra de la existencia de campos de pruebas, sino que creemos que no debería de garantizarse su existencia, ya que la forma en la que se garanticen los primeros, informará y sentará pretensiones sobre derechos futuros ya adquiridos.

Propuestas

- Los derechos reconocidos a las personas físicas deberían aludir a estas explícitamente, evitando que se pueda entender que se conceden esos derechos a las empresas.
- La mención en la carta a los “sandbox” debería eliminarse, o redactarse de modo que no pueda interpretarse como un derecho.

Conclusiones

Desde Interferencias y Trackula agradecemos de nuevo la existencia de esta Carta de Derechos Digitales y sobre todo de la consulta pública de la misma.

En general interpretamos la Carta como un vehículo para atraer el cambio en la legislación y la creación y defensa de derechos civiles en el ámbito digital.

En este sentido, en nuestra alegación describimos las partes de la Carta que más nos preocupan para generar este cambio y las razones para que esto sea así. También incluimos propuestas para, con un espíritu constructivo, tratar de elevar la Carta y con carácter general, las actuaciones en materia de la Agenda Digital, a un grado de innovación puntero. Todo bajo el objetivo de posicionarnos como país en la vanguardia respecto a los derechos digitales y al liderazgo tecnológico en general que, tal y como reconoce la Agenda Digital, será una parte importante de la economía del país y, por lo tanto, debería de centrar nuestra atención para garantizar nuestra prosperidad.

Para aquellas partes que no hemos comentado de la carta, lo hemos hecho con la intención de minimizar el espacio en el documento y maximizar su valor. Respecto a estas, o bien consideramos que es una buena idea, o bien que su definición no causa situaciones tan destacables como los que describimos.

La extensión de este documento se justifica por la necesidad de incluir contexto suficiente para poder argumentar en dónde creemos que el texto propuesto se queda corto, o bien de intención, o bien de definición o claridad. Así mismo hemos tratado de incluir medidas que podrían tomarse para llevarlo más allá y ofrecer unas garantías más robustas en cuanto a la dirección en la que puedan implementarse estos derechos.

Tratamos los derechos propuestos y algunos que echamos en falta desde dos orígenes: los referidos a personas físicas y aquellos en los que intervienen otras entidades.

Por no reiterar aquí las propuestas y conclusiones de cada apartado, nos referimos al final de cada uno, y concluimos con el humilde deseo de que estas propuestas puedan tenerse en cuenta de forma constructiva tanto para la redacción final de la Carta como en el desarrollo de la Agenda Digital a futuro.

En cualquier caso, quedamos a su disposición para cualquier aclaración, duda, consulta o comentario en nuestras direcciones de contacto.

Para más información pueden contactar con nosotros en: info@trackula.org y en info@interferencias.tech

Firmado:

Lorena Sánchez

Ángel Pablo
Hinojosa

Pablo Castro

Santiago Saavedra
Sofía Prósper

Germán Martínez

Paula de la Hoz