EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

Respuesta de CCBE a la consulta sobre el Libro Blanco de la Comisión Europea sobre Inteligencia Artificial

05/06/2020

Introducción

El Consejo de la Abogacía Europea (CCBE) representa a las Abogacías de 45 países y, a través de ellas, a más de un millón de abogados europeos. CCBE responde regularmente en nombre de sus miembros sobre cuestiones políticas que afectan a los ciudadanos y abogados europeos.

En el presente documento, CCBE tiene la intención de explicar con más detalle varias de sus respuestas al cuestionario general relativo a la consulta sobre el Libro Blanco sobre la Inteligencia Artificial - Un enfoque europeo de la excelencia y la confianza (que se copia en el ANEXO de la página 12-22), y de ofrecer sugerencias más detalladas sobre las cuestiones de mayor relevancia desde el punto de vista de los abogados. Este documento se inspira en gran medida en las Consideraciones de CCBE sobre los aspectos jurídicos de la inteligencia artificial (IA), recientemente publicadas.

En primer lugar, CCBE expresa su preocupación por la forma en que se ha redactado el cuestionario de consulta. En particular, el cuestionario no se ha adaptado a sectores y casos de uso específicos, y no ofrece a los encuestados la oportunidad de indicar por pregunta desde qué perspectiva se da la respuesta. En consecuencia, será muy difícil interpretar las distintas respuestas sin información adicional sobre el modo en que los respectivos encuestados han enfocado las distintas preguntas. Además, muchas de las preguntas son preguntas capciosas que sólo ofrecen un conjunto cerrado de opciones, por lo que es imposible expresar una opinión significativa.[1]

Por estas razones, CCBE desea aclarar que el alcance de su respuesta a esta consulta se limita principalmente a los aspectos relacionados con el Estado de Derecho, la administración de justicia y los derechos fundamentales. Por otra parte, CCBE también aborda ciertas cuestiones de responsabilidad, así como las necesidades de formación de los abogados y los bufetes en relación con el uso de la IA en la práctica jurídica. Las partes que se presentan a continuación están estructuradas según los temas abordados en el cuestionario de la consulta y abordan los siguientes aspectos principales.

[1] Se hace referencia a las observaciones de CCBE en relación con la consulta de la Comisión sobre el "Balance del enfoque "Legislar mejor" de la Comisión", donde CCBE pidió a la Comisión que revisara su metodología de diseño de cuestionarios. Véanse los párrafos 3-6 en este enlace.

- ***Un ecosistema de excelencia***:

- Debe ponerse a disposición de los reguladores sectoriales -incluidos los colegios de abogados- financiación a nivel de la UE para formar a los abogados en temas como el uso de las nuevas tecnologías y la IA en el ámbito de la justicia, respetando los principios éticos y los requisitos de protección de datos.
- La interacción entre todos los sectores, privados y públicos, es esencial para garantizar que los valores éticos que guían a los distintos actores se diseñen en los propios sistemas de IA.
- Los abogados deben tener acceso a las instalaciones de prueba y de referencia para poder ejercer plenamente su papel y sus responsabilidades a la hora de garantizar el despliegue y la revisión adecuados de las herramientas de IA.

- ***Un ecosistema de confianza***:

- Inteligencia artificial y derechos humanos: prácticamente todos los derechos humanos pueden verse afectados por el uso de sistemas de IA. Por lo tanto, son necesarias varias acciones, entre ellas: evaluaciones exhaustivas del efecto de los sistemas de IA; un escrutinio independiente y experto; transparencia en el uso de la IA; garantizar la disponibilidad de recursos; nuevos marcos legales para codificar los principios y requisitos que rigen el uso de la IA, junto con códigos éticos voluntarios que comprometan a los desarrolladores de IA a actuar de forma responsable.
- Como alternativa al enfoque basado en el riesgo propuesto, CCBE pide un enfoque más específico que establezca requisitos legales adaptados a las necesidades de los sectores y circunstancias específicas tras una evaluación más detallada de los riesgos y la valoración de las medidas legales u otras medidas apropiadas.
- El uso de la IA por parte de los tribunales y en los sistemas de justicia penal supone un alto riesgo, ya que socava muchos de los fundamentos en los que se basa la justicia. Por lo tanto, cualquier despliegue de este tipo de herramientas debe ir precedido de una evaluación en profundidad y de evaluaciones de impacto con la participación de todos los actores y partes interesadas pertinentes, y estar estrictamente regulado teniendo en cuenta la arquitectura procesal que sustenta los procedimientos judiciales. En cualquier caso, debería garantizarse el derecho a un juez humano en cualquier fase del procedimiento.
- Es necesaria una combinación de mecanismos de cumplimiento ex-ante y ex-post sobre la base de un conjunto de requisitos obligatorios

- ***Implicaciones de la seguridad y la responsabilidad de la IA, la IO y la robótica***

- Será necesario introducir algunos cambios importantes en el marco legislativo actual, teniendo en cuenta las diferencias fundamentales que existen entre los productos tradicionales y la IA, en particular, en lo que respecta a las nociones de producto, culpa y defecto.
- CCBE optaría por un instrumento independiente sobre las cuestiones de responsabilidad de la IA en lugar de modificar la Directiva sobre responsabilidad por productos. Aspectos como la indemnización por daños y perjuicios y la atribución de la responsabilidad, así como las normas sobre la carga de la prueba, deberían regularse a nivel de la UE.
- Entre las cuestiones que deben tenerse en cuenta a la hora de modificar el marco legislativo actual se encuentran: la noción de producto; la falta de previsibilidad en el funcionamiento de los sistemas de IA; el destinatario de la responsabilidad; las defensas; el tipo de daños y las

víctimas; el régimen de pruebas y la inversión de la carga de la prueba en determinadas situaciones; y la cuestión del seguro obligatorio.

Sección 1 - Un ecosistema de excelencia

Con el auge de la IA y la llegada de la tecnología jurídica, la práctica jurídica se ha vuelto cada vez más compleja debido a las nuevas cuestiones jurídicas que plantea la IA y al desarrollo de herramientas digitales muy sofisticadas que los abogados deben dominar y comprender. También es necesario que los abogados hagan un uso consciente y responsable de estas nuevas tecnologías para desarrollar su actividad de la mejor manera posible, protegiendo la relación de confianza entre el abogado y el cliente y asegurando el cumplimiento de las obligaciones profesionales. En este sentido, los principios más evidentes a respetar en el uso de las herramientas de IA se refieren a: el deber de competencia, el deber de información al cliente, el mantenimiento de la independencia de los abogados en materia de defensa y asesoramiento, el deber de preservar el secreto profesional/privilegio profesional del abogado y la obligación de proteger la confidencialidad de los datos de los clientes. Por lo tanto, es necesaria una formación que amplíe la competencia general de los abogados para comprender el entorno tecnológico en el que probablemente trabajarán en el futuro.

Por lo tanto, CCBE apoya firmemente la idea de que la financiación a nivel de la UE se ponga a disposición de los reguladores sectoriales -incluidos los colegios y consejos de abogados-, ya que son los que están mejor posicionados para comprender y abordar las necesidades de formación de sus respectivos sectores -como el de los abogados-, en particular en lo que respecta a la forma en que la IA puede utilizarse de manera compatible con sus códigos éticos y deberes profesionales. En este sentido, se hace referencia a la contribución de CCBE para la próxima política de la UE en materia de formación judicial[2], que también destaca la necesidad de formar a los abogados en temas como el uso de las nuevas tecnologías y la inteligencia artificial en el ámbito de la justicia, respetando los principios éticos y los requisitos de protección de datos.

Otro aspecto esencial es la interacción entre todos los sectores, privados y públicos, para garantizar que los valores éticos que guían a los distintos actores se diseñen en los propios sistemas de IA. No basta con confiar en la experiencia de los especialistas técnicos que operan en el ámbito de los sistemas informáticos. Hay que construir nuevos puentes de confianza teniendo en cuenta la experiencia y las funciones específicas de los actores y especialistas de los distintos sectores y profesiones. A este respecto, CCBE desea destacar que los abogados desempeñan un papel importante para garantizar el acceso a la justicia, la defensa del Estado de Derecho y la protección de los valores democráticos, y como tales tienen un papel particular que desempeñar cuando se trata de seguir desarrollando y desplegando herramientas de IA, especialmente en aquellos ámbitos en los que están en juego el acceso a la justicia y el debido proceso.

Por lo tanto, los abogados también deben tener acceso a las instalaciones de prueba y referencia para poder ejercer plenamente su papel y sus responsabilidades a la hora de garantizar el despliegue y la revisión adecuados de las herramientas de IA. Esto es especialmente importante cuando las herramientas de IA pueden llegar a ser impugnadas en los procedimientos judiciales y deben ser revisadas por las partes.

[2] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/TRAINING/TR_Position_papers/EN_TR_20200427_CCBE-contribution-for-the-next-EU-policy-on-judicial-training.pdf

Sección 2 – Un ecosistema de confianza

I. Inteligencia artificial y Derechos Humanos

En general, el uso de la IA en los procesos automatizados de toma de decisiones puede reconfigurar la interacción entre los ciudadanos y los responsables públicos y privados. Esto puede socavar la capacidad de los ciudadanos para buscar asesoramiento, o para impugnar o tratar de revertir las decisiones. Por lo tanto, es necesario garantizar unos mecanismos de recurso sólidos, así como una estrecha participación de los actores que tienen una función de protección de los derechos de los ciudadanos (por ejemplo, abogados y jueces).

Además, prácticamente todos los derechos humanos pueden verse afectados por el uso de sistemas de IA. CCBE subraya en particular lo siguiente:

Desde el punto de vista de CCBE, el derecho a un juicio justo es un punto clave de preocupación. Aunque más adelante se identificarán las cuestiones relativas al uso de la IA en los tribunales y en los procesos penales, también el derecho a un juez humano forma parte del derecho a un juicio justo.

Además, el posible sesgo de los conjuntos de datos que la IA utiliza para aprender es también un claro ejemplo de una cuestión que afecta a la imparcialidad de un juicio. Los sistemas de IA no comprenden todo el contexto de nuestras complejas sociedades. Sus datos de entrada son el único contexto en el que operan y si los datos proporcionados para entrenar a la IA son incompletos o incluyen un sesgo (incluso no intencionado), es de esperar que el resultado de la IA sea también incompleto y sesgado. Además, en la fase actual de desarrollo, los sistemas de IA suelen carecer de transparencia en sus conclusiones. Carecen de explicación, es decir, de la capacidad de explicar tanto los procesos técnicos de un sistema de IA como las decisiones humanas relacionadas (por ejemplo, las áreas de aplicación de un sistema). Por lo tanto, los humanos no entienden o tienen dudas sobre cómo los sistemas de IA llegan a las conclusiones.

Estas conclusiones pueden ser inofensivas en su uso ordinario, pero cuando se utilizan ante un tribunal, las conclusiones pueden interferir con la imparcialidad del proceso.

En aras de la transparencia y con el fin de permitir a los individuos defender sus derechos, parece apropiado que las personas afectadas por el uso de un sistema de IA sean debidamente informadas de que se está utilizando la IA y de que los datos relativos al asunto planteado por él o ella pueden ser considerados por un sistema automatizado. Esto se corresponde con los principios actuales de protección de datos, que en general deben seguirse cuando se utiliza la IA, al igual que cualquier otra norma legal aplicable. Como es habitual en otros lugares, garantizar la disponibilidad de recursos será probablemente la medida adecuada para abordar los casos de uso indebido de los sistemas de IA.

El derecho a la libertad de expresión e información también puede verse afectado: la IA permitirá un mayor escrutinio y control de la forma en que las personas pueden expresarse tanto en línea como fuera de ella. Aunque se pueden ver usos positivos en la lucha contra la incitación al odio y las noticias falsas, la línea entre el uso beneficioso de la IA y su mal uso parece ser tenue.

Del mismo modo, el derecho a la libertad de reunión y de asociación entra en consideración cuando se utiliza la IA para identificar a los participantes en asambleas, protestas o cualquier otra reunión multitudinaria. Aunque son útiles en algunas situaciones para proteger el orden público, estas herramientas pueden ser fácilmente utilizadas de forma indebida contra los opositores políticos. Ya existen sistemas capaces de reconocer automáticamente a las personas (reconocimiento de rostros o movimientos) y analizar su comportamiento. Es muy posible que estas herramientas influyan en la

participación de las personas en las reuniones, atenuando así el derecho a la libertad de reunión y asociación.

El derecho a una vida protegida, en el contexto de las armas inteligentes y los drones operados algorítmicamente, también se verá afectado por la IA. El derecho a la protección contra la discriminación puede verse afectado cuando los empresarios utilicen la IA para automatizar partes de los procesos de contratación de empleados.

Incluso hoy en día existen sistemas capaces de preseleccionar a los candidatos al puesto de trabajo. En nuestra era digital, la cantidad de datos que los humanos proporcionan sobre sí mismos es enorme. Ya sean metadatos o datos de contenido, proporcionan muchos detalles de su vida personal o detalles que simplemente son privados en general. La IA vive de los datos y su capacidad para trabajar con ellos y combinarlos es inmensa. Por lo tanto, el derecho a la privacidad y a la protección de datos está claramente en juego.

Los principios democráticos y el Estado de Derecho están estrechamente vinculados a los derechos humanos, ya que se complementan entre sí. Al observar el derecho a la intimidad, la recopilación de información de los perfiles de las redes sociales de las personas sobre sus opiniones políticas y su posterior uso (erróneo) para afectar a las preferencias de voto y a las elecciones, no sólo atenta contra el derecho a la intimidad, sino que también puede considerarse una injerencia en uno de los principios de la sociedad democrática que tiene un impacto directo en el orden público.

Teniendo en cuenta estas consideraciones, CCBE recomienda que se tomen las siguientes medidas:

- En general, y sobre la base de las recomendaciones[3] disponibles actualmente3 en este ámbito, las evaluaciones exhaustivas del efecto de los sistemas de IA sobre diversos derechos humanos, principios democráticos y el Estado de Derecho es una de las medidas clave que deberían utilizarse para evitar conflictos no deseados con estos derechos, principios y normas. Dichas evaluaciones deberían llevarse a cabo tan pronto como sea posible, incluso en la fase inicial de desarrollo, evaluando el impacto potencial que los sistemas de IA pueden tener sobre los derechos humanos a lo largo de todo su ciclo de vida.
- También es necesario que los sistemas de IA se sometan a un escrutinio independiente y experto, especialmente cuando se pretende su uso público. Poner a disposición del público los resultados de este examen no sólo reducirá la posibilidad de sesgos intencionados y no intencionados, sino que también aumentará la fiabilidad de los sistemas de IA. La apertura de los sistemas de IA para su examen por parte de cualquier interesado puede aumentar aún más su fiabilidad; sin embargo, esto no será posible sin interferencias proporcionadas con los secretos comerciales y otros derechos de propiedad intelectual de los desarrolladores de IA.
- En aras de la transparencia y para que los individuos puedan defender sus derechos, las personas afectadas por el uso de un sistema de IA deben ser debidamente informadas de que se está utilizando la IA y de que los datos que les conciernen pueden ser considerados por un sistema automatizado. Esto se corresponde con los actuales principios de protección de datos, que en general deben seguirse cuando se utiliza la IA, al igual que cualquier otra norma legal aplicable.
- Como es habitual en otros lugares, garantizar la disponibilidad de recursos será probablemente la medida adecuada para abordar los casos de uso indebido de los sistemas de IA o los daños causados por ellos.

[3] https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

- Es necesario evaluar si los marcos jurídicos actualmente disponibles son adecuados o deben adaptarse para garantizar que los sistemas de IA se utilicen respetando los derechos humanos. Posiblemente, sea necesario establecer algunos marcos jurídicos nuevos para codificar determinados principios y requisitos junto con códigos éticos voluntarios que comprometan a los desarrolladores de IA a actuar de forma responsable. Dado que la tecnología (incluida la IA) es extranacional, cuando se puede apoyar la necesidad de un marco jurídico que no se limite a una jurisdicción, el desarrollo de un marco de este tipo podría ser deseable y parecería estar en consonancia con la evolución actual[4].

II. Posibles ajustes del actual marco legislativo de la UE en materia de IA

A. Enfoque basado en el riesgo

CCBE le preocupa que un ejercicio de categorización del riesgo como "alto" o "bajo" sobre la base de criterios abstractos sea demasiado simplista y conduzca a una regulación estructuralmente defectuosa. Es necesario un enfoque más específico.

En particular, los factores que hay que tener en cuenta para determinar el riesgo son muchos y complejos, y dependen de los casos de uso específicos, las circunstancias de su utilización, la complejidad de la tarea, el riesgo que plantea un posible mal funcionamiento de la IA y su naturaleza técnica. Por ejemplo, la IA para un sistema de gestión de casos utilizado por los tribunales plantea menos riesgo que la IA para la evaluación de la probabilidad de reincidencia de un acusado.

En estas circunstancias, en primer lugar, no conviene dar el mismo tratamiento jurídico a cosas que son técnicamente diferentes, por ejemplo, la inteligencia artificial, el internet de las cosas y otras tecnologías digitales, aunque a veces compartan características comunes. En realidad, se requiere un enfoque más matizado, que tenga en cuenta los nuevos y complejos retos que plantea la IA.

En segundo lugar, en el Libro Blanco se reconoce que el nivel de riesgo puede ser muy diferente incluso dentro de un mismo "sector", como la sanidad. Por lo tanto, la regulación que pretende neutralizar los riesgos sólo puede ser eficaz si se dirige a riesgos muy específicos en circunstancias concretas, como el riesgo de discriminación en los sistemas de vigilancia de las fuerzas de seguridad, o el riesgo de un juicio injusto si las partes en un caso no tienen la oportunidad de evaluar, debatir y plantear objeciones contra una herramienta de IA que se utilizó en el proceso de toma de decisiones judiciales.

Por ello, CCBE reclama un enfoque más específico basado en las siguientes acciones:

- Evaluación de los riesgos y daños específicos que el uso de herramientas de IA puede causar en sectores y circunstancias concretas.
- Evaluación del tipo de medidas legales o de otro tipo apropiadas que podrían adoptarse para hacer frente a los riesgos y daños identificados en sectores y circunstancias específicas, teniendo en cuenta que, en un sector determinado, puede haber niveles de

[4] Vea las actividades del Consejo de Europa en este ámbito y su Comité Ad Hoc sobre Inteligencia Artificial que se ha creado el 11 de septiembre de 2019 para evaluar la necesidad de dicho marco jurídico: https://www.coe.int/en/web/artificial-intelligence/-/the-council-of-europe-established-an-ad-hoc-committee-on-artificial-intelligence-cahai

riesgo muy diferentes en función del uso preciso que se haga de la IA. En este contexto, también es necesario evaluar en qué medida es necesario adaptar o ajustar las normas comunitarias existentes.

- Establecimiento de requisitos legales adaptados a las necesidades de los sectores y circunstancias específicas. En este contexto, es importante considerar cómo se aplican los principios generales, como la no discriminación y el derecho a un juicio justo, y cómo deben cumplirse.

B. Aplicación de alto riesgo de la IA: el uso de la IA por los tribunales

Cuando examinamos los diferentes usos posibles de la IA en el proceso judicial, vemos inmediatamente que su introducción en los sistemas judiciales podría socavar muchos de los fundamentos en los que se basa la justicia (véase el cuadro siguiente).

En el ámbito de la justicia, podría haber fuertes incentivos para utilizar la IA. Las autoridades públicas ya han identificado los supuestos beneficios presupuestarios que podrían obtenerse al sustituir parte del personal judicial por sistemas automatizados. El uso potencial de las herramientas de IA también podría verse como un medio para permitir a los jueces dictar sentencias más coherentes y de mayor calidad de forma más rápida, racional y eficiente. Por lo tanto, no cabe duda de que habrá intentos de desplegar la voluntad de la IA en el ámbito de la justicia, lo que plantea la cuestión de las condiciones para dicho uso.

La necesidad de un marco ético en relación con el uso de la IA por parte de los tribunales es, por tanto, claramente evidente y, por ello, CCBE apoya la iniciativa de la Comisión Europea para la Eficiencia de la Justicia (CEPEJ) del Consejo de Europa, que ha adoptado una "carta ética sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno"[5]

Pero la reflexión ética por sí sola no será suficiente, y también es necesario identificar normas y principios operativos eficaces y normas y principios operativos eficaces y vinculantes que puedan regir, en la práctica, el uso de las herramientas de IA por parte de los tribunales. En particular, el uso de herramientas de IA debe conciliarse con los principios fundamentales que rigen el proceso judicial y garantizar un juicio justo, por ejemplo: igualdad de armas, imparcialidad, procedimientos contradictorios etc. Aunque la tentación de sacrificar todo por la eficacia pueda estar presente, estos derechos fundamentales tienen que deben seguir estando garantizados para todas las partes que buscan justicia.

[5] Véase la Carta Ética Europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno, aprobada por la CEPEJ durante su asamblea plenaria de los días 3 y 4 de diciembre de 2018, y que está disponible en línea en: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

Tabla: Identificación de los posibles usos de la IA en los sistemas judiciales y los peligros inminentes para los derechos fundamentales y el Estado de Derecho

Principales usos del Tribunal

Pasos	Gestión de casos	Fase prejudicial	Juicio	Deliberación del Juez	Fase posterior a la sentencia
Potenciales aplicadores IA	* Sistemas de gestión de casos * Plataformas de comunicación accesibles para los abogados * Monitoreo automático de procedimientos * Monitoreo automático de dilaciones en el proceso * Sistemas automáticos para cumplir con itos formales del proceso * Decisiones automáticas en la vida del proceso * Diferenciación automática entre casos apelables y no apelables.	Base de datos del demandante y sus peticiones	*Conferencias. *Transcripción automática. *Presentación automatizada de evidencias. * IA que detecte las emociones	*Herramientas de jurisprudencia *Herramientas de búsqueda autónoma *Análisis automático del riesgo *Sistema de toma de decisiones *Asistencia inteligente	*Análisis de riesgos, probabilidad de reincidencia

Principales problemas y riesgos que tener en cuenta

Principios	*Procedimientos contenciosos * Estado de derecho y proceso debido * No restricciones en el acceso a la justicia * Igualdad de armas * Acceso a datos por parte de los abogados	*Procedimientos contenciosos * Igualdad de armas * Acceso a datos por parte de los abogados * Protección de datos	*Procedimientos contenciosos * Juicio justo * Transparencia *Neutralidad	*Procedimientos contenciosos * Juicio justo * Transparencia *Responsabilidad en caso de error *Acceso a la prueba *Derecho a solicitar la intervención de un juez humano	*Procedimientos contenciosos * Juicio justo * Transparencia *Derecho a recurrir

El cuadro anterior muestra que se puede imaginar el uso de herramientas de IA en la gestión o el seguimiento de los expedientes; durante las audiencias (ya sea en la fase de juicio o de instrucción); para facilitar la toma de decisiones del juez (la fase de deliberación); y en el seguimiento de la ejecución de las decisiones.

El cuadro anterior también indica los principios que podrían verse afectados por el uso de herramientas de IA debido a una multitud de realidades negativas que podrían producirse, por ejemplo:

- La utilización de datos y elementos que no han sido objeto de un debate contradictorio.

- La explotación de conclusiones (incluso parciales) que no han sido obtenidas mediante el razonamiento del juez.

- La falta de transparencia del proceso, ya que resulta imposible saber qué debe atribuirse al juez y qué procede de una máquina.

- La ausencia de un campo de juego (igualdad de armas).

- La vulneración del principio de imparcialidad por la imposibilidad de neutralizar y conocer los sesgos de los diseñadores del sistema.

- La vulneración del principio de lógica debido a la existencia de resultados que escapan al razonamiento humano y no pueden ser rastreados.

Por lo tanto, el uso de herramientas de IA por parte de los tribunales podría socavar gravemente la actual arquitectura procesal de los procedimientos judiciales, especialmente si se acepta que el juez pueda acceder a dichas herramientas solo durante el proceso de deliberación.

La actual arquitectura general de un juicio se explica por la necesidad de garantizar el cumplimiento de una serie de una serie de principios y de producir decisiones que provienen del propio juez, a la luz de los argumentos y las pruebas aportadas por las partes. El juez es imparcial y sus decisiones contienen explicaciones que permiten comprender qué disposiciones legales y precedentes pueden justificarlas.

Normas y principios operativos

Por lo tanto, es importante que las herramientas de IA se adapten adecuadamente al entorno de la justicia, teniendo en cuenta los principios y la arquitectura procesal que sustentan los procedimientos judiciales. Antes de implantar las herramientas de IA en los sistemas judiciales, debe definirse y adoptarse un conjunto de normas y principios que regulen el uso de la IA. En particular, deberían mantenerse las siguientes garantías mínimas:

- La posibilidad de identificar el uso de la IA: todas las partes implicadas en un proceso judicial deben poder identificar siempre, dentro de una decisión judicial, los elementos resultantes de la aplicación de una herramienta de IA.

- No delegación del poder de decisión del juez: en ningún caso el juez debe delegar todo o parte de su poder de decisión en una herramienta de IA. En cualquier caso, debe garantizarse el derecho a un juez humano en cualquier fase del procedimiento. - La posibilidad de que las partes verifiquen los datos introducidos y el razonamiento de la herramienta de IA.

- La posibilidad de que las partes discutan e impugnen los resultados de la IA de forma contradictoria fuera de la fase de deliberación y con un plazo razonable.

- El cumplimiento de los principios del GDPR.

- La neutralidad y la objetividad de las herramientas de IA utilizadas por el sistema judicial deben estar garantizadas y ser verificables

Como se ha demostrado anteriormente, todavía es necesario un gran debate crítico para evaluar el papel que deben desempeñar las herramientas de IA en nuestros sistemas judiciales, si es que lo hacen. El cambio debe ser aceptado cuando mejore o al menos no empeore la calidad de nuestros sistemas de justicia. Sin embargo, los derechos fundamentales y la adhesión a las normas éticas que sustentan las instituciones basadas en el Estado de Derecho no pueden subordinarse a meras ganancias de eficiencia o beneficios de ahorro de costes, ya sea para los usuarios de los tribunales o para las autoridades judiciales.

Por lo tanto, cualquier despliegue de estas herramientas debería estar estrictamente regulado y estar precedido de una evaluación en profundidad y de una valoración de su impacto con la participación de todos los actores y partes interesadas.

C. Aplicaciones de alto riesgo de la IA: el uso de la IA en los sistemas de justicia penal

Parte del trabajo de las fuerzas policiales en la prevención de delitos -incluyendo todas las formas de vigilancia técnica como la interceptación, la recopilación y el análisis de datos (texto, audio o vídeo) y el análisis de pruebas físicas (muestras de ADN, ciberdelincuencia, declaraciones de testigos, ...)- puede ser potencialmente apoyado técnicamente por el uso de la IA. Esto también da lugar a varios problemas; por ejemplo, el sesgo inherente a las herramientas utilizadas para predecir la delincuencia o evaluar el riesgo de reincidencia y herramientas como la tecnología de reconocimiento facial que son inexactas a la hora de identificar a personas de diferentes razas. Estas formas de discriminación suponen una amenaza para los derechos civiles. Además, el uso de la IA en el ámbito de la labor forense digital y la evaluación del riesgo de reincidencia se enfrenta a problemas, dado que el funcionamiento específico de los algoritmos no suele revelarse a las personas afectadas por el resultado de su uso. Esto hace que el acusado no pueda impugnar las predicciones realizadas por los algoritmos. Otra preocupación se refiere a la desigualdad de armas que puede surgir entre las capacidades más avanzadas de las que pueden disponer los fiscales y los recursos más limitados de los abogados.

En lo que respecta al uso de sistemas de identificación biométrica (por ejemplo, reconocimiento facial) en espacios de acceso público, CCBE considera que esto no debería tener lugar hasta que se establezcan directrices o legislación específicas a nivel de la UE que cumplan plenamente con la Carta de Derechos Fundamentales de la Unión Europea y el Convenio Europeo de Derechos Humanos, incluida la jurisprudencia pertinente.

La identificación biométrica suele tener graves defectos que ponen en peligro los derechos civiles. Se ha demostrado en múltiples estudios que es inexacta a la hora de identificar a personas de diferentes razas. Además, existe una gran preocupación por el hecho de que las palabras desencadenantes que utilizan las agencias de seguridad nacional no están suficientemente afinadas y, por tanto, las conversaciones telefónicas de millones de personas son vigiladas sin una base legal.

Además, el uso generalizado de los sistemas de identificación biométrica puede suponer graves riesgos para una sociedad abierta y pluralista si no se utiliza de forma proporcionada con un objetivo previsto como es garantizar la seguridad pública. En muchas situaciones, el anonimato es la salvaguarda más importante de la libertad, y las técnicas de identificación biométrica que abarcan grandes áreas del espacio público ponen en peligro esta libertad. Cuanto más precisas sean y más se extienda su uso, más peligrosas serán.

Por lo tanto, cuando se trata del uso de herramientas de IA en los sistemas de justicia penal, también se aplicarán la mayoría de las normas y principios expuestos en los apartados I y II.B. Por lo tanto, todo despliegue de estas herramientas debería estar estrictamente regulado y estar precedido de una evaluación en profundidad y de una valoración del impacto con la participación de todos los actores y partes interesadas pertinentes.

D. Requisitos obligatorios de un posible marco normativo futuro

CCBE está de acuerdo en que los siguientes requisitos obligatorios son importantes para el establecimiento de un futuro marco regulador de la IA:

- La calidad de los conjuntos de datos de formación
- La conservación de registros y datos
- Información sobre la finalidad y la naturaleza de los sistemas de IA
- Robustez y precisión de los sistemas de IA
- La supervisión humana
- Normas claras de responsabilidad y seguridad

Además, el CCBE también subraya que el requisito de explicabilidad es de especial importancia para el entorno de la justicia, es decir, la capacidad de explicar tanto los procesos técnicos de un sistema de IA como las decisiones humanas relacionadas.

Como se ha indicado en el punto II.A, es importante que los requisitos legales se adapten a las necesidades de sectores y circunstancias específicas.

E. Marco de cumplimiento

En cuanto a la cuestión de cómo garantizar que la IA sea digna de confianza, segura y respetuosa con los valores y las normas europeas, CCBE considera que es necesaria una combinación de mecanismos de cumplimiento ex-ante y de aplicación ex-post.

Sin embargo, en lugar de adherirse a un marco de cumplimiento muy genérico y abstracto, las medidas de cumplimiento apropiadas deben ser consideradas y adaptadas a las necesidades en sectores y circunstancias específicas.

Por lo tanto, los destinatarios del marco de cumplimiento también dependerán y diferirán según el ámbito exacto al que se dirijan las medidas de cumplimiento. También es importante garantizar que las herramientas de IA no se desplieguen, especialmente en el sector público, sin haber definido previamente el marco de cumplimiento.

Sección 3 - Implicaciones de seguridad y responsabilidad de la IA, el IoT y la robótica

I. Necesidad de modificar el actual marco legislativo de la UE en materia de responsabilidad

Al abordar la cuestión del modelo de responsabilidad para los sistemas de IA, algunos pueden tener la tentación de decir que la ley ya está bien desarrollada, especialmente en lo que respecta a la responsabilidad por productos, así como a otros regímenes de responsabilidad vigentes en los Estados miembros, y todo lo que se necesita para proteger a las víctimas potenciales es aplicarla. Por otro lado, dado que la IA es un nuevo desarrollo, algunos pueden querer reinventar el derecho de la responsabilidad para hacer frente a los problemas que plantea.

Si se observan los modelos de responsabilidad existentes, hay algunos enfoques posibles para abordar la cuestión de la responsabilidad civil con respecto a la IA: 1) un sistema de responsabilidad basado en el concepto de culpa o 2) un sistema de responsabilidad objetiva. Dentro de estas amplias categorías, puede haber margen para diferentes enfoques. Por ejemplo, en lo que respecta a este último, el sistema podría ser un régimen de responsabilidad estricta puro -en el que se responde tanto si hay un defecto como si no y en el que no se permiten defensas para excluir o reducir la responsabilidad- o un sistema de responsabilidad estricta que permita varias defensas, siguiendo el modelo de la Directiva 85/374/CEE27[6] (Directiva de la UE sobre responsabilidad por productos defectuosos). Por otra parte, podría ser conveniente considerar otros regímenes de responsabilidad en el contexto de la IA. Por ejemplo, el informe recientemente publicado del Grupo de Expertos en Responsabilidad y Nuevas Tecnologías creado por la Comisión Europea menciona la responsabilidad vicaria (responsabilidad derivada de las acciones de otros) en relación con la tecnología autónoma. Además, la responsabilidad contractual u otros regímenes de indemnización podrían aplicarse en algunos ecosistemas digitales junto con la responsabilidad extracontractual o en su lugar[7].

Los enfoques parecen diferir significativamente en cuanto al mejor régimen para abordar la cuestión de la responsabilidad con respecto a la IA, así como la decisión política que debería adoptarse al respecto. A pesar del enfoque que se adopte, está claro que habrá que introducir ciertos cambios importantes en el marco legislativo actual, teniendo en cuenta las diferencias fundamentales que existen entre los productos tradicionales y la IA, en particular, en lo que respecta a las nociones de producto, culpa y defecto. También habrá que reconsiderar las cuestiones de a quién puede extenderse la responsabilidad, la carga de la prueba y las defensas.

CCBE optaría por un instrumento separado sobre las cuestiones de responsabilidad de la IA, en lugar de modificar la Directiva sobre la responsabilidad de los productos, reconocida como eficaz respecto a los productos tradicionales. Tratar de introducir medidas adicionales en la Directiva de Responsabilidad por Productos para hacer frente a la IA afectaría necesariamente de forma negativa al proceso de investigación y desarrollo de otros productos, lo que no es deseable. En ese caso, los productos de la IA que actualmente entran en el ámbito de aplicación de la Directiva de

[6] Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos

[7] Comisión Europea: Informe del Grupo de Expertos en Responsabilidad y Nuevas Tecnologías - Formación en Nuevas Tecnologías: La responsabilidad por la inteligencia artificial y otras tecnologías digitales emergentes, diciembre de 2019, pp.36-37

Responsabilidad por Productos deberían salir del mismo e incorporarse al ámbito de aplicación de la nueva Directiva.

Sin embargo, la Comisión sólo parece estar considerando -al menos por el momento- los cambios que podrían ser necesarios en los instrumentos existentes de la UE, especialmente en la Directiva de Responsabilidad por Productos, así como en los regímenes nacionales de responsabilidad, y no la posibilidad de crear un nuevo instrumento. En cualquier caso, CCBE considera que aspectos como la indemnización por daños y perjuicios y la atribución de la responsabilidad, así como las normas sobre la carga de la prueba, deberían regularse a nivel de la UE. Otro enfoque podría llevar a una situación en la que las normas nacionales adaptadas diferirían significativamente entre los Estados miembros.

Más concretamente, la Comisión debería tener en cuenta las siguientes observaciones:

II. Cuestiones que deben tenerse en cuenta a la hora de modificar el marco legislativo actual

A. Noción de producto

Como ya se ha dicho, hay diferencias fundamentales entre los productos tradicionales y la IA. En primer lugar, en lo que respecta a la noción de producto, hay que tener en cuenta que los sistemas de IA son cada vez más cada vez más, no sólo como sistemas autónomos, que pueden funcionar en ordenadores de uso general, sino también como parte de productos más complejos de propósito general, sino también como parte de productos más complejos. Un ejemplo de lo primero es el software de diagnóstico médico que se utiliza para analizar las tomografías en busca de signos tempranos de cáncer, y de lo segundo son los vehículos de autoconducción. CCBE sostiene que la IA debe definirse a fondo en el nuevo instrumento legislativo.

B. Falta de previsibilidad en el funcionamiento de los sistemas de IA: impacto en las nociones de fallo y defecto

En segundo lugar, el atributo del autoaprendizaje y la toma de decisiones autónoma de los sistemas de IA va en contra del uso del razonamiento jurídico tradicional basado en el concepto de "previsibilidad" como base de la responsabilidad. En este contexto, un sistema de IA puede causar daños como resultado de un "defecto" tradicional, por ejemplo, en el software, pero también como consecuencia de sus "propias" acciones determinadas por datos y algoritmos, sin ningún "defecto" en el sentido tradicional. Así pues, la responsabilidad por daños no puede atribuirse fácilmente a la "culpa" de una persona (física o jurídica) ni a la existencia de un defecto en un producto, en el sentido de un mal funcionamiento específico de ese producto.

En estas condiciones, podría decirse que la responsabilidad por las acciones realizadas por un sistema de IA no debe vincularse necesariamente a la noción de culpa (en su sentido tradicional) o de "defecto" (en su sentido tradicional). A este respecto, también puede señalarse que la actual Directiva sobre responsabilidad por productos defectuosos, aunque se basa en la existencia de un "defecto", define "defecto" no en el sentido tradicional, sino en relación con el resultado, es decir, "un producto es defectuoso cuando no ofrece la seguridad que una persona tiene derecho a esperar, teniendo en cuenta todas las circunstancias..." (artículo 6, apartado 1).

C. Destinatario de la responsabilidad

En tercer lugar, está la cuestión de a quién se puede extender la responsabilidad. Esta puede ser una tarea difícil dada la opacidad de los sistemas de IA y teniendo en cuenta la multiplicidad de personas potencialmente implicadas, posiblemente en múltiples jurisdicciones, y en el caso de algunas personas, su trabajo podría ser utilizado posteriormente sin su conocimiento en un sistema de IA.

Hay varias posibilidades de identificar a los diferentes actores a los que se podría atribuir la responsabilidad. Por ejemplo, el informe del Grupo de Expertos sugiere que no sólo se considere responsable al productor, sino también al operador, dependiendo de las circunstancias[8].

La introducción de la noción de "operador" como la "persona que controla el riesgo relacionado con el funcionamiento de la IA y que se beneficia de su funcionamiento" es de agradecer a este respecto, con una distinción entre operador frontal y operador secundario. Dichos operadores, al igual que los productores, tendrían que cumplir con deberes específicos de cuidado, dando lugar a una responsabilidad en caso de incumplimiento de dichos deberes.

D. Defensas

Si el legislador de la UE instituye un régimen de responsabilidad objetiva para los productos de IA, lo que significa que, siempre que la IA haya causado un daño, el destinatario de la responsabilidad de esta IA debe ser responsable de cubrir el daño, debería estudiarse detalladamente la posibilidad de establecer defensas adecuadas.

No obstante, deberían reconsiderarse las exenciones específicas que se contemplan actualmente en la Directiva sobre responsabilidad por productos defectuosos. En particular, las excepciones establecidas en la letra b) del artículo 7 (el defecto no existía en el momento de la puesta en circulación del producto) y en la letra e) (la defensa del estado de la técnica) deberían rechazarse en relación con la IA. A este respecto, el CCBE está de acuerdo con la consideración expresada en el informe del grupo de expertos en el sentido de que la defensa por riesgo de desarrollo no debería aplicarse en el contexto de las tecnologías digitales emergentes: el productor debería ser estrictamente responsable de los defectos aunque éstos aparezcan después de la puesta en circulación del producto, siempre que el productor siguiera controlando las actualizaciones o mejoras de la tecnología.[9]

E. Tipo de daños y de victimas

En lo que respecta a los daños, es necesario considerar como pérdidas para las que se debe disponer de una indemnización en condiciones específicas no sólo los daños físicos y materiales, sino también la destrucción de los datos de la víctima.

Dado que los riesgos inherentes a la IA y los daños que ésta puede causar no son en sí mismos previsibles, los daños que se cubren no deben limitarse a los previsibles. Debe considerarse el nexo causal. Además, dado que los sistemas de IA están en constante desarrollo, no debería limitarse la responsabilidad a los daños que se demuestre que eran previsibles, siempre que, en un caso determinado, el uso que se haga de la IA entre en la categoría de razonable y se demuestre que el

[8] Comisión Europea: Informe del Grupo de Expertos en Responsabilidad y Nuevas Tecnologías - Formación en Nuevas Tecnologías: Liability for Artificial Intelligence and other emerging digital technologies, pp. 39-46
[9] Comisión Europea: Informe del Grupo de Expertos en Responsabilidad y Nuevas Tecnologías - Formación en Nuevas Tecnologías: Responsabilidad por inteligencia artificial y otras tecnologías digitales emergentes, p. 6

daño ha sido causado por ese uso de la IA (de acuerdo con las reglas de prueba que se explican más adelante).

Todos los perjudicados (ya sean personas físicas o jurídicas) deben poder reclamar una indemnización por daños y perjuicios, sin que haya ninguna restricción, por ejemplo, a los consumidores o a los que utilizan la IA en el marco de su actividad empresarial, comercial o profesional.

F. La regla de la prueba y la inversión de la carga de la prueba en determinadas situaciones

Las cuestiones relativas a la carga de la prueba también deben reconsiderarse en el contexto de los sistemas de IA, ya que las características de autoaprendizaje y aprendizaje profundo de la IA conducirán necesariamente a una disminución de la previsibilidad. Las conexiones causales entre la entrada y el comportamiento del sistema pueden ser difíciles de dilucidar[10]. En estas condiciones, no siempre se puede esperar que la víctima aporte pruebas sobre el mal funcionamiento interno que ha provocado los daños.

Las víctimas deben tener derecho a la facilitación de la prueba en aquellas situaciones en las que las dificultades para demostrar la existencia de un elemento de responsabilidad sean desproporcionadas, yendo más allá de lo que razonablemente se debería esperar. En algunos casos, la inversión de la carga de la prueba puede ser apropiada, como en el caso de la ausencia de información registrada sobre la tecnología de funcionamiento (registro por diseño) o la falta de acceso razonable de la víctima a esta información.

Cuando varias personas hayan cooperado para crear una unidad de IA y la víctima no pueda demostrar cuál de ellas ha creado el elemento que ha provocado el daño, estas normas de facilitación también deberían poder dar lugar a una responsabilidad conjunta de esas personas hacia la víctima. Las reclamaciones de reparación entre los causantes del daño deberían ser posibles.

G. La cuestión del seguro obligatorio

Por último, el seguro obligatorio de responsabilidad civil podría considerarse una solución para dar a las víctimas un mejor acceso a la indemnización en situaciones que exponen a terceros a un mayor riesgo de daño y también podría proteger a los posibles causantes de daños contra el riesgo de responsabilidad11. Por ejemplo, la conveniencia de garantizar, por un lado, que nadie que sufra pérdidas por el funcionamiento de un sistema de IA quede sin compensación, frente a la preocupación de que pueda haber un efecto de enfriamiento en la innovación o una interferencia no deseada en las relaciones entre empresas.

Además, hay otros factores que deben tenerse en cuenta en relación con un sistema de seguro obligatorio. Por ejemplo, en lo que respecta a la cuestión de qué actores deberían estar obligados a suscribir un seguro de este tipo, puede ocurrir que el número de personas que han contribuido -en distintos momentos y con distinta relevancia- a un sistema de IA sea muy grande. Los riesgos potenciales de los sistemas de IA también pueden ser muy diferentes en función de los sectores en los que se utilice el sistema de IA.

---

[10] Herbert Zech, Liability for autonomous systems: Tackling specific risks of modern IT; “Des voitures autonomes – Une offre de loi”, essai, juillet 2018, n°02.226

Por lo tanto, el CCBE invita a la Comisión a estudiar detenidamente todas estas cuestiones y a sopesar las ventajas e inconvenientes de estas posibilidades.

Puede encontrar las respuestas de CCBE a la consulta del Libro Blanco de la Comisión Europea sobre Inteligencia Artificial aquí.