Asociación Española de Compliance

Grupos ASCOM

Compliance en la Economía Digital

Inteligencia Artificicial aplicada. Desafios para el gobierno corporativo.

Noviembre 2024

www.asociacioncompliance.com

Inteligencia Artificial aplicada.

Desafíos para el gobierno corporativo.

ÍNDICE DE CONTENIDOS

1. Inteligencia Artificial aplicada. Desafíos para el gobierno corporativo

Cuando hablamos sobre Inteligencia Artificial ("IA")[1], es frecuente que surjan infinidad de dudas dada la complejidad técnica, así como la infinidad de retos y oportunidades que plantea. En mayor o menor medida las características de nuestra organización tales como el sector, su orientación a la innovación y los recursos disponibles, serán absolutamente determinantes para poder dar respuesta a esos retos y oportunidades que se derivan del uso de esta, así como determinarán nuestro nivel de confianza frente al abordaje de la IA. Lo cierto es que, con independencia del sector, tamaño y recursos, las herramientas de IA se están convirtiendo en elementos esenciales de los procesos organizacionales, si es que no lo son ya.

1.1. Conocimiento adecuado sobre la IA: oportunidades y riesgos

La IA es sinónimo de eficiencia y eficacia. Es una herramienta destinada a guiar la toma de decisiones y mejorar la productividad, siempre y cuando se construya de forma sólida, funcione correctamente (sin sesgos y con información clasificadora) y cumpla con la regulación. La IA supone una auténtica disrupción en cuanto a la disponibilidad que todos tenemos de hacer uso de ella. Por tanto, el riesgo no está en la tecnología per se, sino en el uso que desde las organizaciones se haga de dicha tecnología aplicada a la organización.

La respuesta a todas estas preguntas (y alguna más) se encuentra en la gobernanza de la IA, siendo éste el instrumento en las organizaciones para conseguir que la innovación proporcione beneficios sostenibles teniendo bajo control los riesgos, y es que mucho de lo que escuchamos sobre IA se focaliza en los riesgos.

Con razón o no, la IA es percibida como prometedora y a la vez intrínsecamente arriesgada (como la mayoría de novedades que la evolución natural del ser humano representa), siendo determinante una gobernanza sólida y pragmática de la IA en las organizaciones con el fin de proporcionar a todas las partes implicadas o "*stakeholders*" la tan ansiada seguridad de que, no solamente se mitigarán los riesgos, sino que la IA estará en consonancia con la cultura, ética y valores corporativos.

1 Definición de "sistema de IA de conformidad con el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de Inteligencia Artificial (RIA) (…): un sistema basado en máquinas que está diseñado para funcionar con diversos niveles de autonomía y que puede mostrar capacidad de adaptación tras su despliegue, y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales.

1.1.1. La importancia de un sistema de gobierno de IA multidimensional

A la hora de regular internamente la IA, surgen muchas preguntas: ¿Cuáles son los sistemas de IA que utilizamos? ¿Cuáles queremos utilizar? ¿Qué son prácticas prohibidas, riesgo alto, limitado, sistemas de IA de propósito general? ¿Cómo garantizamos ética, privacidad, seguridad de la información u otros derechos?

Nombrar a un responsable de IA es un primer paso, pero ¿Sería suficiente? Aquí la respuesta es clara. Aunque contemos con una cabeza responsable de la IA, ésta debe ser manejada de manera holística para abordar eficazmente los desafíos y oportunidades asociados con los sistemas de IA. Dicho enfoque multidimensional debe incluir, en todo caso:

1) **Tecnología y desarrollo**: encargados de la investigación, desarrollo e implementación de los modelos o sistemas de IA conforme a las necesidades de la organización.

2) **Ética y Compliance**: asegurando que los sistemas de IA se comporten de una manera ética y responsable, así como velando por el cumplimiento de leyes y regulaciones.

3) **Legal y regulatorio**: velando por la privacidad, propiedad intelectual y confidencialidad.

4) **Gestión del cambio**: fomentando la colaboración entre departamentos como parte esencial en la implementación de los sistemas de IA.

5) **Seguridad de la información:** protegiendo de los sistemas de IA y garantizando su integridad.

6) **Comunicación interna y externa**: en línea con el principio de transparencia, es clave gestionar la comunicación de iniciativas tanto dentro de la empresa como fuera, asegurando la confianza con las partes interesadas.

1.1.2. Coste, talento, integración en los procesos, ética y privacidad y resistencia al cambio

Implantar un modelo de gobernanza de la Inteligencia Artificial (IA) implica abordar factores críticos, cada uno con sus propios retos e implicaciones. La organización deberá enfrentarse al coste, talento, cómo integrar la IA en los procesos, el manejo de la ética y la privacidad, y la resistencia al cambio.

Montarse al carro de la IA de una manera segura requerirá inversiones significativas en la creación o implantación del sistema, así como el mantenimiento continuo y formación de los empleados. Una implantación exitosa del sistema de IA dependerá de unos profesionales cualificados en todos los ámbitos, debiendo basarse en un modelo escalable y adaptable a las necesidades, operaciones, así como a los cambios tecnológicos y normativos; y todo ello debe hacerse garantizando la ética y privacidad, esenciales para mantener la confianza de los *stakeholders*, buscando siempre disminuir o incluso anular los posibles daños legales o reputacionales en las personas y en la propia organización.

A todo esto, se le suma la resistencia cultural y el miedo que dentro de las organizaciones puede existir a sentirse desplazado por una tecnología que puede realizar muchas tareas básicas (y no tan básicas) desarrolladas por empleados. Aquí la organización también debe de realizar un buen trabajo de gestión del cambio y comunicación interna para abordar estos desafíos.

Para ello, un modelo de gobernanza sólido de la IA ayudará a despejar todas las dudas sobre las variables anteriores que podrían dificultar la puesta en marcha de IA como una herramienta fundamental para alcanzar la eficiencia operativa en la organización.

1.1.3. Transparencia: comunicación del uso de sistemas de IA a stakeholders

Los requisitos de transparencia de la IA encuentran su origen, entre otros, de la regulación en protección de datos[2] (“**GDPR**”) y otros esquemas regulatorios (principios de la OCDE) así como iniciativas privadas, que podrían ser tomadas como precedentes más inmediatos, sin perjuicio de ello, el Reglamento de Inteligencia Artificial (“**RIA**”) ha venido a introducir y disponer una amplia gama de requisitos de transparencia que aplican a los proveedores/implantadores de los sistemas de IA.

La transparencia ofrece claridad y comprensión a las partes interesadas. Internamente, establecer un sistema de gobernanza basado en la transparencia consolidará el propio sistema de IA, asegurando la responsabilidad, confianza y toma de decisiones informadas.

1.1.4. Responsable de IA. Ubicación en la organización

Como suele ocurrir siempre que una norma genera la obligatoriedad de crear una nueva figura dentro de las organizaciones, surge la necesidad de ubicar orgánicamente a esta nueva figura, surgiendo, innumerables debates sobre la compatibilidad o no de esta figura con otras preexistentes en la organización. El caso que nos ocupa no va a ser diferente.

En algunas organizaciones, los sistemas de IA podrían ser integrados en las funciones de Privacidad o Compliance, en otras en las de Tecnología e Innovación; en otras en la función de Compliance, atendiendo en todo caso a la estructura previa y a los requisitos de independencia y autonomía que se establecen en la regulación vigente, siendo necesario, en algunas organizaciones, la creación de un nuevo puesto.

Sin perjuicio de lo anterior, los sistemas de IA cuentan con infinidad de vértices que requieren de múltiples capacidades y conocimientos por lo que es necesario contar con roles con diferentes competencias dentro de la organización que participen en los procesos relacionados con la IA.

Para arquitecturar esta participación, muchas organizaciones están optando por la creación de un “Comité de IA”, que a su vez, podría culminar en un responsable último o no, reporta directamente a la alta dirección, asegurando que la estrategia e iniciativas de AI estén alineadas tanto con los objetivos tanto tecnológicos, como empresariales o en materia de ética y cumplimiento normativo de la entidad.

En todo caso, el papel del responsable de IA o del Comité de IA se encuentra ubicado en la conocida como segunda línea de defensa, pudiendo o no, ser compatibilizada con algunas de las figuras habituales que se encuentran en esa misma línea de defensa.

1.2. Requisitos para desarrollar un sistema de gobierno

El objetivo de la regulación sobre IA es promover la adopción de una Inteligencia Artificial centrada en el ser humano, fiable y confiable, garantizando un elevado nivel de protección de los derechos fundamentales.

Por tanto, la adopción de los nuevos requisitos del RIA y su total cumplimiento por parte de todas las organizaciones es un objetivo clave, para lo cual estas organizaciones están obligadas a implementar cambios técnicos y organizativos que garanticen que los sistemas de IA protegen los derechos fundamentales.

Las organizaciones, a través de la **Política de IA**, establecerán un marco único de definición del uso de IA, donde se comprometan a utilizar estos sistemas dentro de unos principios éticos, lícitos y robustos que garanticen la fiabilidad de los sistemas de IA que se utilizan en la compañía. Por otro lado, el modelo del Gobierno de la IA definirá las principales funciones para establecer los parámetros de estrategia, organización y gobierno en materia de IA.

Para poder diseñar un modelo de gobierno de IA, lo primero que debemos tener en cuenta son los parámetros que nos dimensionen el impacto de la IA en la organización, es decir, tendremos que atender a elementos como recurrencia, naturaleza, operaciones o actividades afectadas, volumen de sistemas, complejidad, rol de responsabilidad (proveedor/responsable del despliegue/distribuidor/importador), así como el impacto que, para el negocio de la organización, tiene la utilización de los sistemas de IA en el día a día.

En este punto, no todas las organizaciones utilizan sistemas de IA, hay otras que se apoyan en sistemas de IA generativa de manera muy residual para determinados procesos, otras que sí utilizan estos sistemas para su día a día de manera recurrente y otras, cuya estrategia de negocio pivota en estos sistemas.

Por tanto, como primer punto para tener en cuenta en la definición del modelo es que el **sistema de gobierno de IA debe ser proporcional al uso de los sistemas de IA** que se llevan a cabo dentro de la organización, por lo que siempre debe encontrarse contextualizada a la realidad concreta en la que nos encontramos.

Para abordar de forma exitosa una correcta y adecuada gestión del gobierno de IA en cualquier organización, todas las actividades realizadas deben establecerse de manera coordinada y en línea con la estrategia definida por la organización en la Política de IA, por lo que es necesario adoptar una división de trabajo que permita alcanzar los objetivos estratégicos propuestos de forma eficiente.

Para lograr esto, es necesario definir un sistema de planificación y gestión, integrado y balanceado, de forma vertical, mediante una estructura jerárquica, según las responsabilidades de decisión de cada integrante:

1) **Definir un nivel superior encargado de elaborar las políticas y estrategias de la organización**. Se basa en decidir los objetivos a largo plazo, definir los recursos que se usarán y las políticas para obtener y administrar dichos recursos:

   a) Establece la estrategia de IA de la organización mediante políticas globales y un marco general de referencia de gestión y aplicación a todos los componentes.

   b) Fija el gobierno y responsabilidad de la organización siguiendo la estrategia definida de IA requiere la implementación efectiva de una estructura organizacional sólida y multidisciplinaria. En este modelo de estructura, se deben organizar y delimitar adecuadamente los roles y responsabilidades de cada área y colaborador

2) **Definir un nivel medio que lleve a cabo control de la gestión y los riesgos de los sistemas de IA que se utilicen:**

   a) Modelo de gestión/cuadro de mando que permita la toma de decisiones.

   b) Políticas, procedimientos y gestión: alinearse con el negocio para garantizar que los datos estén protegidos y gestionados de acuerdo con la estrategia de la organización.

   c) Clasificación del sistema de IA y definición de los riesgos.

3) **Definir un tercer nivel operativo que plantea los sistemas de IA que se utilizarán:**

   a) Lleva a cabo las operaciones y procesos de IA soportados en las políticas y procedimientos

definidos, que dan soporte operativo al cumplimiento del RIA.

b) Realiza el inventario de sistemas de IA.

Para conseguir un efectivo control de los riesgos derivados en cada uno de dichos niveles es recomendable adoptar el **modelo de control de tres líneas de defensa**:

a) **Primera línea:** Áreas operativas.

b) **Segunda línea:** Áreas de control interno/cumplimiento.

c) **Tercera línea:** Órganos y entidades independientes, como auditoría interna o terceras partes.

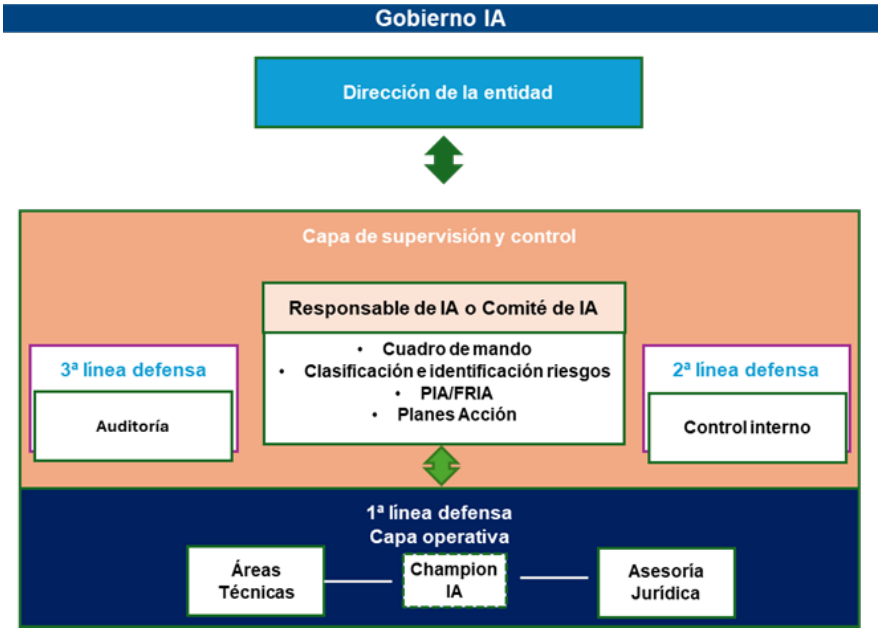
Adicionalmente, es necesario tener en cuenta la necesaria división en diferentes niveles de gestión y decisión:

1) **nivel superior** para la elaboración de la estrategia de IA dentro la organización;

2) **nivel medio** para el control de la gestión realizada y;

3) **nivel operativo** de utilización de los sistemas de IA;

Igualmente, será necesario definir los roles y responsabilidades específicos para la IA, siendo posible **replicar los modelos de gobierno de privacidad** que, en muchas corporaciones han sido muy exitosos desde el punto de vista de control. En estos modelos, se propone una persona responsable, "*Champion IA"*, a nivel operativo, que se encarga de velar el uso responsable de la IA en su área de influencia, y escala los riesgos identificados al también creado Comité de IA de la compañía tal y como figura en la siguiente ilustración:



Teniendo en cuenta el principio de proporcionalidad y como no los medios con los que cuente la organización, en función de la naturaleza, volumen, estrategia y complejidad de los sistemas de IA que utiliza una organización, la creación de un Comité de IA sería recomendable al aportar una estructura sólida y especializada para abordar cuestiones éticas en la implementación de IA, fortaleciendo la posición de la entidad en términos de responsabilidad y liderazgo ético en el uso de tecnologías digitales[2].

Si los tres componentes de una IA fiable son: (i) licitud, (ii) ética y (iii) robustez técnica, consideramos que los perfiles que deben formar parte de este Comité de IA deben ser expertos en dichas materias:

a) Técnicos, ingenieros, científicos de datos y expertos en estrategia IA.

b) Abogados expertos en derecho TIC (regulación IA, privacidad y propiedad intelectual).

c) Expertos en ética digital (entre otros, filósofos, psicólogos, humanistas).

El Comité de IA se encargaría de analizar que los sistemas de IA garanticen unos altos estándares éticos. En concreto, que dichos sistemas respeten la normativa aplicable (Tratados de la UE, normativa de protección de datos, propiedad intelectual y la normativa de IA), la autonomía humana, no provoquen daños o puedan perjudicar a personas, sean técnicamente robustos, sean especialmente cuidadosos con personas vulnerables, se aseguren que las personas no sufran sesgos injustos o cualquier tipo de discriminación, se cumpla con el principio de transparencia, explicabilidad y por último se garantice la supervisión humana de dichos sistemas.

2 Grandes compañías de telecomunicaciones, entidades de crédito, entidades tecnológicas, entidades del sector salud y entidades del sector energético, entre otras, donde el uso de IA está muy generalizado y su adopción es parte de decisiones estratégicas, deberían contar con este comité.

El éxito de la implementación de este modelo de gobierno de IA dependerá de la involucración de todas las áreas, desde el consejo de administración hasta el servicio de atención al cliente, y que éstas conozcan e integren en las funciones de su día a día, los principios éticos de IA basados en la solidez técnica, la supervisión, la transparencia, la gestión de la privacidad y la no discriminación.

2. Inteligencia Artificial y propiedad intelectual

2.1. La IA y su impacto en la Propiedad Intelectual

Cuando se hace referencia al concepto de "Propiedad Intelectual" se debe tener en consideración, tanto los derechos inherentes de autoría, como los derechos de explotación exclusiva sobre una obra susceptible de protección, siendo estas las obras literarias o artísticas, que la ley reconoce a su autor durante un cierto plazo temporal.

El Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual[3], determina en su artículo 2 que, la propiedad intelectual está integrada por derechos de carácter personal (derechos inherentes) y patrimoniales, que atribuyen al autor la plena disposición y el derecho exclusivo a la explotación de la obra, sin más limitaciones que las establecidas en la Ley.

La Propiedad Intelectual, protege los derechos de autor, y en este sentido **la IA ha logrado tener un gran impacto en lo que respecta a la protección de estos derechos de autor,** ya que, está transformando la creación y protección de activos intangibles, como patentes o marcas registradas (en Propiedad Industrial) o derechos de autor (en Propiedad Intelectual), de diversas maneras, por ejemplo:

1) En la **creación de contenido original**. La IA es una herramienta muy útil para crear contenidos inéditos y originales, dado que ayuda al autor con la ejecución de ciertos contenidos, como pueda ser música, diseño, arte o escritura, para que éstos sean mucho más rápidos y eficientes, y por lo tanto puedan crear más contenido en menos tiempo.

2) También nos ayuda en la **protección de los derechos de autor**, dado que la IA puede ser utilizada como herramienta para detectar infracciones de derechos de autor en línea, llegando incluso ciertas plataformas, a través de algoritmos, a poder detectar y bloquear la distribución ilegal de contenido protegido por derechos de autor.

3 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.

3) La IA nos ayuda también con la **gestión de los derechos de autor**, automatizando procesos, como puedan ser la licencia de contenido o la distribución de regalías.

Sin perjuicio de ello, la IA también, como no podía ser de otra forma, ha venido a plantear ciertos desafíos, como, por ejemplo:

1) La **determinación de la titularidad y autoría** de las creaciones generadas por algoritmos de la IA.
2) La adecuación jurídica de **llevar a cabo el "entrenamiento" de sistema de IA utilizando para ellos contenidos protegidos** por derechos de propiedad intelectual o industrial.
3) O los **requisitos** que son necesarios **para que una obra creada por IA sea protegida por derechos de autor,** si es que es posible. ¿Requiere un nivel determinado de intervención humana?

Por lo tanto, podemos afirmar que la IA ha transformado la creación y protección de la Propiedad Intelectual, mejorando la eficiencia en la producción de contenido y siendo una herramienta muy importante para detectar infracciones en los derechos de autor, facilitando, en resumen, la gestión y la protección de esta.

2.2. Propiedad intelectual. Riesgos derivados del uso de la Inteligencia Artificial

El reciente RIA, además del sometimiento a la legislación actual sobre propiedad intelectual europea, establece el denominado Requisito de Transparencia respecto de la IA generativa, no considerándola de alto riesgo por sí misma, pero obligándola a cumplir dicha transparencia respecto a la protección de los derechos de propiedad intelectual e industrial. Para ello se deberá:

1) Revelar qué contenido ha sido generado por IA;
2) Diseñar el modelo que evite la generación de contenido ilegales;

3) Publicar resúmenes de los datos protegidos por derechos de autor utilizados para el entrenamiento de los sistemas de IA.

4) Etiquetar todas aquellas imágenes, audios o vídeos que hayan sido generados y/o modificados con IA.

En general las legislaciones de la mayoría de los Estados y, particularmente la legislación de España exclusivamente reconoce la existencia de derechos de propiedad intelectual respecto a obras, siempre que en la elaboración de esta haya mediado intervención humana suficiente, por lo que, a aquellos contenidos generados de forma exclusiva por IA, no se les reconocerán derechos de autor. En este sentido, el artículo 5.1 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, es claro al determinar que *"Se considera autor a la persona natural que crea alguna obra literaria, artística o científica."*

A nivel Europeo, la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO), consciente de los retos que planteaba la IA para los derechos de propiedad intelectual, a principios de 2019, la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO) creó un Grupo de Expertos sobre el Impacto de la Tecnología de IA en los derechos de propiedad intelectual. Dicho grupo, que continúa aún vigente, se encuentra compuesto por expertos con conocimientos y experiencia práctica en el seguimiento del impacto de las nuevas tecnologías en los procesos de infracción de derechos de propiedad industrial.

Dicho Grupo de Trabajo sigue un enfoque específico basado en una adaptación de la teoría del «Código y otras leyes del ciberespacio» de Lawrence Lessig (la Teoría del Código), que describe cómo la actividad humana en línea está regulada por la ley, las normas sociales y el mercado, teniendo en cuenta la infraestructura técnica de Internet (denominada «código») llevándose a cabo un estudio publicado en el año 2022[4].

El propósito de este estudio es evaluar cómo las tecnologías de IA afectan tanto la violación como el respeto de los derechos de autor y de los modelos y diseños. Aunque estos presentan similitudes con la violación y el respeto de otros derechos de propiedad intelectual (como secretos comerciales, marcas y patentes) mediante el uso de IA, este análisis no abordará específicamente esos otros tipos de propiedad intelectual.

4 Study on the impact of artificial intelligence on the infringement and enforcement of copyright and designs: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs_FullR_en.pdf

Este estudio busca ser una herramienta práctica dirigida a profesionales, para facilitar la comprensión del impacto de la IA y contextualizarlo en un marco más amplio. Para ello, se han desarrollado 20 escenarios que ilustran el uso indebido actual o potencial de las tecnologías de IA para infringir los derechos de autor (y derechos conexos) y diseños, así como su uso para hacer cumplir dichos derechos. El enfoque principal es la aplicación de la IA en la observancia de la propiedad intelectual seleccionada. Sin embargo, hay y seguirá habiendo numerosas aplicaciones pertinentes de la IA que se entrelazan con medidas de observancia voluntaria, observancia civil y algunos aspectos de la observancia administrativa.

Si bien en España no se ha planteado hasta el momento ningún caso público en relación a este aspectos (al menos conocido), en Estados Unidos, en 2023, se dictó una resolución por parte de la oficina de propiedad intelectual (USCO - *U.S. Copyright Office*), relacionada con el comic *Zarya of the Dawm*, cuya inscripción había sido solicitada por la artista Kristina Kashtanova, en la que la USCO determinó que dar indicaciones a una IA para llevar a cabo la creación de un contenido, no convierte a quien realiza dichas indicaciones en autor de la obra resultante, denegando el registro de la obra a su nombre por no poder ser considerada autor.

Dada cuenta que la USCO cuenta ya con varias resoluciones en este sentido, siendo la más antigua del año 2018 y la más reciente del año 2023, la USCO publicó recientemente una guía estableciendo los criterios para el registro de obras que contengan material generado por el uso de la IA[5]. Entre los criterios que recoge están

5 Estas tecnologías se «entrenan» con grandes cantidades de obras preexistentes de autoría humana y utilizan las inferencias de ese entrenamiento para generar nuevos contenidos. Algunos sistemas funcionan en respuesta a una instrucción textual del usuario, llamada «prompt». El resultado puede ser textual, visual o sonoro, y lo determina la IA basándose en su diseño y en el material con el que ha sido entrenada. Estas tecnologías, a menudo descritas como «IA generativa», plantean cuestiones sobre si el material que producen está protegido por derechos de autor, si se pueden registrar obras

la creatividad y originalidad, así como la necesidad de contribución significativa de un creador humano.

Adicionalmente, a principios de 2023, la Oficina de Derechos de Autor puso en marcha una iniciativa para examinar la legislación de derechos de autor y las cuestiones políticas planteadas por la Inteligencia Artificial (IA), incluido el alcance de los derechos de autor en las obras generadas por IA y el uso de materiales protegidos por derechos de autor en la formación de IA. Tras organizar sesiones públicas de escucha y seminarios web, la Oficina publicó un aviso de investigación en el Registro Federal en agosto de 2023, que recibió más de 10.000 comentarios hasta diciembre de 2023. Derivado de dicho proceso la USCO está elaborando un informe, que va siendo publicado en varias partes en el que se analizan las cuestiones, habiéndose publicado hasta el momento la primera de las partes[6].

Por lo tanto, todo apunta a que, al menos hasta el momento, la tendencia legislativa y por parte de las autoridades es al **no reconocimiento de derechos de autor a las obras producidas por IA exclusivamente**, es decir, por robots, dado que se viene entendiendo que en este tipo de obras no está presente el principio de originalidad, tan unido a la persona física. Pero no deja de ser, por el momento, un tema no exento de controversia.

Adicionalmente a las posturas más o menos uniformes de Europa y Estados Unidos, en otros países, encontramos diferentes posturas sobre la atribución de la autoría en las obras generadas por la IA, así por ejemplo en China, donde la ley de derechos de autor no contemplan la propiedad *"no humana"* de los derechos de autor, en el caso de *Dreamwriter* de la compañía china *Tencent*, el Tribunal en 2019, vino a reconocer que, el artículo redactado por la IA *Dreamwriter*, no podría atribuirse exclusivamente a la IA, dado que todo el contenido del citado

compuestas tanto de material de autoría humana como de material generado por IA, y qué información deben proporcionar a la Oficina los solicitantes que pretendan registrarlas. Ya no se trata de cuestiones hipotéticas, puesto que la Oficina ya está recibiendo y examinando solicitudes de registro que reclaman derechos de autor sobre material generado por IA. Por ejemplo, en 2018 la Oficina recibió una solicitud para una obra visual que el solicitante describió como «creada de forma autónoma por un algoritmo informático que se ejecuta en una máquina.» La solicitud fue denegada porque, basándose en las representaciones del solicitante en la solicitud, el examinador consideró que la obra no contenía autoría humana. Tras una serie de recursos administrativos, la Junta de Revisión de la Oficina emitió una resolución final en la que afirmaba que la obra no podía registrarse porque se había realizado «sin ninguna contribución creativa de un actor humano.» Más recientemente, la Oficina revisó el registro de una obra que contenía elementos de autoría humana combinados con imágenes generadas por IA. En febrero de 2023, la Oficina concluyó que una novela gráfica compuesta por texto de autoría humana combinado con imágenes generadas por el servicio de IA Midjourney constituía una obra protegida por derechos de autor, pero que las imágenes individuales en sí mismas no podían ser protegidas por derechos de autor[10]. https://www.federalregister.gov/documents/2023/03/16/2023-05321/copyright-registration-guidance-works-containing-material-generated-by-artificial-intelligence.

6 El 31 de julio de 2024, la Oficina publicó la Parte 1 del Informe, que aborda el tema de las réplicas digitales. https://www.copyright.gov/ai/

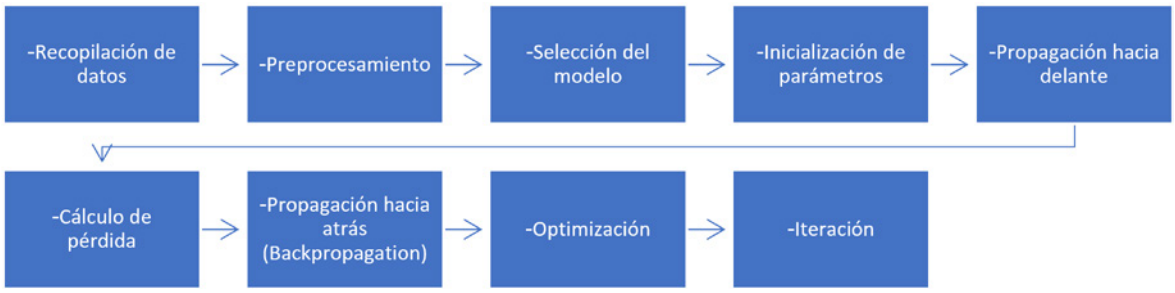
artículo era consecuencia de actividades intelectuales del equipo programador, y en ese sentido la Compañía Tencent estaría legitimada para defender derechos de autor, frente a reproducciones no consentidas del citado contenido.

Parece que la clave estará en distinguir, como ya lo ha hecho la OMPI (Organización Mundial de Propiedad Intelectual), entre obras generadas sin intervención humana, es decir generadas por la IA, y obras generadas con intervención y dirección material humana, es decir, asistidas por IA.

2.3. Entrenamiento de la IA

El entrenamiento de la Inteligencia Artificial podemos definirlo como el proceso por medio del cual un modelo de IA *"aprende"* a partir de los datos proporcionados de entrada, ajustando parámetros internos y realizando tareas específicas. Este entrenamiento tiene gran importancia para el funcionamiento de la IA, así como el hecho de que los datos sean de alta calidad. Podemos resumir los pasos del entrenamiento de la IA en los siguientes:

1) Recopilación de Datos.
2) Preprocesamiento.
3) Selección del Modelo.
4) Inicialización de Parámetros.
5) Propagación hacia delante.
6) Cálculo de pérdida.
7) Propagación hacia Atrás (Backpropagation)
8) Optimización
9) Iteración



El entrenamiento de la IA plantea ciertos desafíos legales en relación con la Propiedad Intelectual y los Derechos de autor. Los modelos de IA, durante el entrenamiento, ajustan sus parámetros para mejorar sus predicciones, y en este proceso utilizan conjuntos de datos que, en ocasiones, pueden contener obras protegidas por derechos de autor. El debate se centra en si el uso de esas obras para entrenar la IA es una infracción de Propiedad Intelectual o por el contrario se puede considerar un uso legítimo.

Son múltiples los casos en los que los autores y titulares originarios de las obras han emprendido acciones legales contra los titulares de los sistemas de IA reclamando sus derechos previos en relación al uso por parte de los segundos de los contenidos generados inicialmente por los primeros para entrenar sus sistemas de IA[7].

Cabe destacar el caso entre Thomson Reuters Enterprise Centre GmbH y otros contra ROSS Intelligence Inc en el que Thomson Reuters y West Publising demandaron a Ross Intelligence ante un tribunal federal de Delaware en mayo de 2020 por la supuesta infracción por parte de ROSS del sistema de números clave de Westlaw y de las notas de cabecera de Westlaw, dos herramientas propiedad de la popular herramienta de investigación jurídica de West, Westlaw, y destinadas a facilitar la investigación en la plataforma.

Más concretamente, Thomson Reuters/West considera que ROSS contrató a LegalEase (una plataforma de software de investigación y redacción jurídica) para que extrajera las Headnotes y los West Key Numbers de cientos de miles de documentos de la base de datos de Westlaw. ROSS tomó todos esos datos y los utilizó para entrenar su herramienta de búsqueda de «lenguaje natural» impulsada por IA para su propia herramienta de investigación jurídica.

Este caso es significativo porque es el primer caso de infracción de derechos de autor basado en IA que ha llegado a la fase de juicio y, por tanto, el primero en ser juzgado por un jurado y, al mismo tiempo, es el primer caso que pone a prueba

7 Acceso a la sentencia dictada por el Tribunal Federal de Delaware sobre el caso 20-613, Juez Judge Stephanos Bibas: https://www.ded.uscourts.gov/sites/ded/files/opinions/20-613_1.pdf

la teoría de que el entrenamiento de un modelo de aprendizaje de IA con material protegido por derechos de autor debe considerarse un uso legítimo.

Si alguien quiere utilizar material protegido por derechos de autor, debe obtener permiso (normalmente en forma de licencia) del propietario de los derechos. Pero hay límites a lo que puede estar protegido por derechos de autor: por ejemplo, las opiniones judiciales y los estatutos son de dominio público y no pueden ser propiedad exclusiva de nadie. En este caso, West afirma que sus Headnotes y Key Numbers constituyen material protegido por derechos de autor, lo que le da la capacidad de controlar el acceso a los casos, estatutos y otros documentos jurídicos de su base de datos.

Si alguien utiliza una obra protegida por derechos de autor sin permiso, o de un modo que excede el alcance de una licencia del titular de los derechos, esa conducta constituye una infracción de los derechos de autor, con independencia de que efectivamente quien utilice dichos sistemas sea un sistema de IA.

A medida que en los dos últimos años han ido apareciendo en el mercado unas tras otras herramientas de Inteligencia Artificial generativa, diversos grupos de titulares de derechos de autor han expresado su seria preocupación por el impacto que estas herramientas tendrán en los derechos de autor de los creadores. La Inteligencia Artificial generativa, capaz de crear textos, imágenes, vídeos y música originales, supone en teoría una amenaza directa para todas y cada una de las industrias que dependen de algún tipo de creatividad humana.

La amenaza proviene en gran parte del hecho de que estas herramientas de IA afectan a «ambas caras» de la moneda de los derechos de autor: la creación de nuevas obras que pueden no necesitar mucho más de la creatividad humana, y el uso sin licencia de material

preexistente protegido por derechos de autor en el entrenamiento de estas herramientas de IA. La primera cuestión ha suscitado encendidos debates, pero la segunda es la que más litigios ha generado hasta la fecha.

2.4. La Inteligencia Artificial como herramienta para facilitar el cumplimiento

Sin duda alguna el mayor reto que se plantea para las áreas de Compliance de las organizaciones, es el hecho de controlar desde la segunda línea de defensa que cada una de las áreas de trabajo de las organizaciones que utilicen la IA como herramienta para llevar a cabo sus procesos, utilicen dichas tecnologías evitando cometer infracciones como las descritas, teniendo en cuenta que, las líneas no están perfectamente definidas, y que nos movemos en un entorno que cambia vertiginosamente, pudiendo adoptar algunas medidas tales como:

1) La IA es capaz de analizar y rastrear multitud de datos y de contenido en línea, ya sean imágenes, textos, videos…etc, con el fin de poder identificar posibles infracciones. Un ejemplo de esto podría ser la búsqueda de similitudes entre obras ya existentes y otras generadas con IA. Con esto tendríamos lo que podríamos denominar un monitoreo automatizado.

2) La IA también puede servir a las empresas como filtro de determinados contenidos, para evitar publicar contenido que esté protegido por derechos de autor.

3) La IA puede aplicar marcas de agua digitales, que son invisibles, y permiten rastrear la autoría e identificar copias no autorizadas.

4) La IA también puede examinar patrones de uso en línea para identificar actividades que puedan considerarse sospechosas.

5) Puede generar informes sobre posibles infracciones, con pruebas y documentación.

6) La IA puede ayudar a las empresas a la gestión efectiva de sus activos digitales, etiquetando de forma automática contenido relevante, como derechos de autor, licencias, etc.

7) También en el análisis de casos similares, de cara a emprender acciones legales en defensa de derechos de autor.

3. Inteligencia artíficial y propiedad industrial

De conformidad con el Art. 4.1. Ley 24/2015 de Patentes[8] la normativa vigente *"Son patentables, en todos los campos de la tecnología, las invenciones que sean nuevas impliquen actividad inventiva y sean susceptibles de aplicación industrial"*.

Concretamente art 4 Ley 24/2015, de Patentes se infieren los principales requisitos de patentabilidad para obtener una patente en general, y también una patente en el ámbito de la IA:

1) **Novedad**: la invención no debe estar comprendida en el estado de la técnica, es decir, no debe haber sido accesible al público antes de la fecha de presentación de la solicitud de patente. En relación con este requisito, en la medida que mediante la IA se puede analizar grandes cantidades de datos para identificar soluciones, es cuestionable si estas invenciones pueden considerarse realmente "novedosas" o nuevas.

2) **Actividad inventiva**: la invención no debe resultar de una manera evidente para un experto en la materia a partir del estado de la técnica. Los algoritmos, el software o los modelos de IA *"per se"*, tienen la consideración de métodos matemáticos o programas de ordenador o modelos abstractos que, como tales, están excluidos en Europa de patentabilidad. Las invenciones implementadas por ordenador que utilizan IA pueden ser patentables si tienen carácter técnico y actividad inventiva no obvia, y en este sentido son patentables las invenciones que incorporan tecnología de IA, como los dispositivos de traducción que utilizan el Deep learning de IA o un dispositivo médico que utiliza IA para diagnosticar enfermedades[9]

8 Ley 24/2015, de 24 de julio, de Patentes: https://www.boe.es/buscar/act.php?id=BOE-A-2015-8328

9 Presentación del Webinario organizado por la OEPM sobre la patentabilidad de la Inteligencia Artificial y la utilización de la IA por las

3) **Intervención humana:** para que una invención generada por IA sea patentable, al menos un ser humano debe participar en el proceso inventivo.

De esta forma, la Inteligencia Artificial (IA), en conjunto con otros elementos, podría llegar a ser parte de un proceso objeto de patente, pero en la actualidad, no podría ser considerada, por sí misma, un invento propiamente patentable atendiendo a los requisitos normativamente exigidos para ello, en tanto existe un consenso general de que un inventor siempre debe ser un ser humano, ya que las máquinas no tienen personalidad jurídica[10].

Por otro lado, desde Estados Unidos, la USPTO (Oficina de Patentes y Marcas de los Estados Unidos) ha hecho público en Febrero del 2024 una RFC (Request for Comment) en torno a su guía con directrices para examinar invenciones en las que han intervenido sistemas de IA*, "Inventorship Guidance for AI-Assisted Inventions"*[11].

En esta Guía se contempla que un ser humano puede obtener una patente cuando se utiliza un sistema de Inteligencia Artificial (IA) como si se tratase de una herramienta, y aunque se expresa claramente que un sistema de IA no puede ser nombrado inventor o coinventor en una patente o solicitud de patente, siguiendo la jurisprudencia dominante, se indica en la Guía igualmente que "*un sistema de IA, al igual que otras herramientas, puede realizar actos que, si los realiza un ser humano, podrían constituir la invención según nuestras leyes.*"

El análisis de la invención debe centrarse en las contribuciones humanas, ya que las patentes funcionan para incentivar y recompensar el ingenio humano. La protección por patente deberá solicitarse para las invenciones respecto

---

oficinas de patentes: https://www.oepm.es/export/sites/oepm/comun/documentos_relacionados/Ponencias/152_00_Inteligencia_Artificial_y_PI.pdf

10 Resolución de la EPO en el caso DEBUS- J 0008/20 de 21 de diciembre de 2021 https://www.epo.org/en/boards-of-appeal/decisions/j200008eu1

11 De conformidad con la «Orden Ejecutiva sobre el Desarrollo y Uso Seguro y Confiable de la Inteligencia Artificial» (30 de octubre de 2023), la Oficina de Patentes y Marcas de los Estados Unidos (USPTO u Oficina) está publicando una guía de invención para las invenciones asistidas por Inteligencia Artificial (IA). La guía proporciona claridad a las partes interesadas y al personal de la USPTO, incluida la Unidad Central de Reexamen y la Junta de Juicios y Apelaciones de Patentes (PTAB o Junta), sobre cómo la USPTO analizará las cuestiones de invención a medida que los sistemas de IA, incluida la IA generativa, desempeñen un papel más importante en el proceso de innovación. Estas directrices explican que, si bien las invenciones asistidas por IA no son categóricamente no patentables, el análisis de la invención debe centrarse en las contribuciones humanas, ya que las patentes funcionan para incentivar y recompensar el ingenio humano. La protección por patente puede solicitarse para las invenciones en las que una persona física haya contribuido de forma significativa a la invención, y las orientaciones proporcionan procedimientos para determinarlo. Por último, la guía analiza el impacto que estos procedimientos tienen en otros aspectos de la práctica de patentes. La USPTO está recabando comentarios del público sobre estas orientaciones para las invenciones asistidas por IA. Accesible desde: https://www.federalregister.gov/documents/2024/02/13/2024-02623/inventorship-guidance-for-ai-assisted-inventions

de las cuales una persona física haya aportado una contribución significativa a la invención.

Actualmente hay 2 corrientes contrapuestas en relación con la capacidad de la IA para desarrollar invenciones de forma autónoma[12]:

Primera.- Algunas entidades, como la OEP, opinan que por ahora no es necesario ajustar la normativa de patentes para abordar la generación autónoma de invenciones por la IA. Consideran que, actualmente, el inventor será quien haya estado más cerca del proceso de invención: ya sea quien seleccionó los datos de entrenamiento de la IA, quien modificó el algoritmo o quien identificó el problema.

Segunda.- En contraste, otros autores y organismos, como la OMPI, creen que la IA con capacidad inventiva podría convertirse en una parte crucial de la investigación y el desarrollo a corto o medio plazo debido a la rápida evolución tecnológica. Cuando eso ocurra, se presentarán serios desafíos si no contamos con normas claras que determinen la posibilidad de proteger las invenciones generadas por IA, definir quiénes o qué deben figurar como inventores y establecer a quién pertenece la propiedad de estas invenciones, entre otras cuestiones.

12 En agosto de 2019, se reveló que se habían presentado dos solicitudes internacionales de patente para "invenciones generadas por IA", es decir, invenciones creadas de forma autónoma por una Inteligencia Artificial (IA) sin la intervención de una persona física, según una definición tradicional de inventor. En estas solicitudes, la IA figura como inventora, mientras que el propietario de la IA aparece como solicitante de la patente y posible titular de cualquier patente concedida. La Oficina Europea de Patentes (OEP) y la Oficina de Propiedad Intelectual del Reino Unido (UKIPO) ya han examinado estas solicitudes en cuanto al fondo. Ambas entidades consideraron que las solicitudes cumplían con los requisitos de patentabilidad hasta donde era posible antes de su publicación. Además, las solicitudes se presentaron bajo el Tratado de Cooperación en materia de Patentes, que facilita la obtención de una patente en más de 150 países, por lo que actualmente están pendientes de examen en un número creciente de oficinas de patentes. Accesible desde el siguiente link: https://www.wipo.int/wipo_magazine/es/2019/06/article_0002.html

Adicionalmente, la invención debe describirse de forma suficiente en la solicitud, de modo que un experto en la materia pueda ejecutarla con la información proporcionada, siendo quizá uno de los requisitos más complicados de cumplir dado que el *"black box thinking"* (pensamiento de caja negra) hace prácticamente imposible lograr determinar cómo se ha llegado a dicho resultado inventivo.

Según las directrices de la Oficina Europea de Patentes (OEP), las invenciones que utilizan herramientas de IA deben ofrecer información suficiente (entre otras, los tipos de datos y su tratamiento concreto por el algoritmo) para que el experto pueda comprender el efecto técnico producido. Proporcionar suficiente información sobre los datos, modelos y algoritmos de IA en las descripciones de patentes es básico para cumplir con este requisito.

En la Oficina Europea de Patentes, existen casos donde se rechazan solicitudes relativas a la definición de una Máquina de Aprendizaje Automático (MAA). La División de Examen ha determinado que la MAA soluciona el problema mediante el conjunto específico de datos usado en su entrenamiento, sin que la solicitud proporcione suficiente información sobre dichos datos. Se ha sugerido crear bases de datos de acceso público para subir los datos utilizados en el entrenamiento y que estos formen parte de la descripción de la solicitud de patente, como una manera de cumplir con el requisito de suficiencia en la descripción.

4) **Aplicación industrial:** la invención debe poder ser fabricada o utilizada en cualquier tipo de industria, incluyendo la agrícola, siendo más que evidente la aplicación industrial de las invenciones patentables que utilizan la IA.

Tampoco resulta extraño en el actual contexto, constatar que la industria de la tecnología la que más ha crecido en número de patentes de IA en los últimos 5 años, con un aumento del 28% anual y que China es el país con mayor número de patentes de IA actualmente publicadas.

Por sectores en la patentabilidad de soluciones con o mediante IA , destacan la industria médica /farmacéutica, la industria de la automoción y, paradójicamente, las propias oficinas de patentes, quienes utilizan la IA para mejorar la eficiencia y precisión en sus procesos de búsqueda y evaluación de patentes.

Al igual que con la propiedad intelectual, la función de Compliance en relación con la propiedad industrial se enfoca en supervisar desde la segunda línea de defensa para asegurar que todas las áreas de trabajo de las organizaciones que emplean

IA para sus invenciones no cometan infracciones similares. Es importante considerar que las fronteras no están claramente definidas y operamos en un entorno en constante cambio, por lo que las recomendaciones indicadas para la propiedad intelectual son igualmente aplicables aquí.

4. Ética, Inteligencia Artificial y neutralidad algorítmica. Por una IA sin sesgos

Ante el progreso, y las nuevas disciplinas que se derivan de la propia evolución de los sistemas de IA y de la aplicabilidad práctica de los mismos, se plantean nuevos dilemas éticos o morales que deben ser tenido en consideración, no sólo por los propios diseñadores que promueven y fabrican los sistemas de IA, sino también de las propias entidades usuarios de los mismos, siendo necesaria la presencia de unos principios éticos que, a modo de brújula, orienten el desarrollo y la aplicación de la IA.

Este análisis se centrará, en particular, en la IA generativa, cuya tarea es analizar cantidades ingentes de datos, establecer correlaciones entre ellos y realizar predicciones, recomendaciones y propuestas, centrándose en el cumplimiento por parte de éstos de los principios éticos y no en las obligaciones o prohibiciones legales. Tal y como señalan las Directrices éticas para una Inteligencia Artificial confiable[13] (en adelante las

13 El objetivo de las presentes directrices es promover una Inteligencia Artificial fiable. La fiabilidad de la Inteligencia Artificial (IA) se apoya en tres componentes que deben satisfacerse a lo largo de todo el ciclo de vida del sistema: a) la IA debe ser lícita, es decir, cumplir todas las leyes y reglamentos aplicables; b) ha de ser ética, de modo que se garantice el respeto de los principios y valores éticos; y c) debe ser robusta, tanto desde el punto de vista técnico como social, puesto que los sistemas de IA, incluso si las intenciones son buenas, pueden provocar daños accidentales. Cada uno de estos componentes es en sí mismo necesario pero no suficiente para el logro de una IA fiable. Lo ideal es que todos ellos actúen en armonía y de manera simultánea. En el caso de que surjan tensiones entre ellos en la práctica, la sociedad deberá esforzarse por resolverlas. ACCESIBLE DESDE: HTTPS://OP.EUROPA.EU/ES/PUBLICA-

Directrices) *"pese a que numerosas obligaciones legales reflejan principios éticos, el cumplimiento de estos últimos trasciende el mero cumplimiento de las leyes existentes*".

El recién aprobado Reglamento de la IA se enfoca en el riesgo, estableciendo un "semáforo" según el tipo de actividad y sus riesgos, entendiendo por riesgo será el resultado de la probabilidad de que se materialice un riesgo y el impacto derivado del mismo:

Existen cuatro niveles de riesgo para los sistemas de IA: inaceptable, alto, limitado y mínimo.

1) **Riesgo inaceptable**: están prohibidos, como por ej. manipular a la gente, a través de un sistema de IA, para que tome una decisión determinada que sin este sistema no hubiese tomado.

2) **Riesgo alto**: deben cumplir una serie de obligaciones antes de que puedan comercializarse.

3) **Riesgo limitado:** que se reduce a los riesgos asociados con la falta de transparencia, estableciéndose obligaciones específicas de transparencia, por ejemplo, cuando se utilizan sistemas de IA como chatbots, los seres humanos deben ser conscientes de que están interactuando con una máquina para que puedan decidir si continuar o no.

4) **Riesgo mínimo:** permitiéndose el uso libre. Esto incluye aplicaciones como videojuegos o filtros de spam. La gran mayoría de los sistemas de IA utilizados actualmente en la UE entran en esta categoría, siendo precisamente en este tipo de sistemas en los que debe extremarse el cuidado, dada cuenta que muchas muchas actuaciones en este tipo de entornos, sin suponer un incumplimiento legal directo, no puede considerarse adecuadas desde la perspectiva de la ética.

La presencia de los sistemas de IA ha adquirido una enorme presencia en nuestra cotidianidad, porque abarcan todos nuestros ámbitos de la vida, desde encontrar un trabajo, el amor de tu vida o invertir para la jubilación.

Es un cambio de paradigma y, como tal, debe ir acompañado de una vigilancia en la distancia, pues para distancias cortas ya está la normativa. Se trata de percibir la IA como una herramienta facilitadora, como una extensión de nuestra esfera de voluntad que resulta apoyada por sistemas de IA.

TION-DETAIL/-/PUBLICATION/D3988569-0434-11EA-8C1F-01AA75ED71A1

Se trata de una IA al servicio del ser humano y esto es en lo que se insiste en la regulación normativa. No obstante, algunas reflexiones actuales ponen de manifiesto un miedo a que la IA supere al ser humano, y este quede desplazado.

Se tiene miedo a la pérdida de puestos de trabajo, a problemas de protección de datos, de privacidad, a que genere mayores desigualdades, falta de transparencia o concentración de poder entre otros inconvenientes.

Ante esto, surge el debate acerca de si se deben limitar las capacidades de la IA o, por el contrario, estos miedos son muy optimistas, ya que suponen una gran confianza en la IA, dándole más capacidades de las que tiene o tendrá. Sea cual sea la opinión que tengamos al respecto, y aún sin saber a dónde puede llegar, conviene tener un posicionamiento firme desde las organizaciones y no dejar que la competencia nos aparte del camino a seguir respecto al uso de la IA: es una mejora para los seres humanos y debe ayudar a hacer el mundo un sitio con menos desigualdades. Y es ahí donde las organizaciones que lo tengan claro se pueden obtener ventaja, desterrando la anacrónica máxima de que si no está prohibido se puede hacer. Como dice el Reglamento se debe animar a los responsables del despliegue de sistemas y modelos de IA a aplicar de forma voluntaria elementos de las directrices éticas para una IA fiable, la sostenibilidad medioambiental, medidas de alfabetización en materia de IA, la inclusividad y la diversidad en el diseño y el desarrollo de los sistemas de IA, lo que incluye tener en cuenta a las personas vulnerables.

El avance tecnológico que supone la IA, debería ser el puente que nos acerque a una sociedad más eficaz y justa, además de ser el instrumento para crear nuevas formas cotidianas que mejorasen nuestra calidad de vida y la forma de relacionarnos con nuestra sociedad. Pero, no se puede negar, que puede ser también un

arma para incrementar la desigualdad, concentrar el poder en un pequeño número de grandes empresas y gobiernos. La concentración de poder se puede evitar con descentralización del desarrollo de la IA. En la otra cara de la moneda podemos sufrir una desaparición de los trabajos menos cualificados y de esta forma un incremento de la desigualdad y la falta de oportunidades para determinados sectores de la población.

Otro aspecto preocupante es la dependencia exagerada de la IA que genera una merma en las capacidades cognitivas del ser humano, especialmente la creatividad y el espíritu crítico. Resulta paradójico cómo la evolución tecnológica que nos brinda enorme cantidad de información está provocando que los mundos de las personas sean cada vez más pequeños. El algoritmo nos sugiere en base a lo que vemos y sólo vemos, al menos aplica para la mayoría de las personas, lo que el algoritmo nos sugiere[14].

En abril de 2023 Elon Musk, junto a más de mil investigadores, redactaron una carta pidiendo una pausa de seis meses en el desarrollo de la IA, en ella se afirma que *"Como se establece en los Principios de IA de Asilomar, ampliamente respaldados, la IA avanzada podría representar un cambio profundo en la historia de la vida en la Tierra y debe planificarse y gestionarse con el cuidado y los recursos correspondientes. Desafortunadamente, este nivel de planificación y gestión no se está produciendo, y en los últimos meses se ha visto a los laboratorios de IA atrapados en una carrera fuera de control para desarrollar e implementar mentes digitales cada vez más poderosas que nadie –ni siquiera sus creadores– puede entender. predecir o controlar de manera confiable. ….. La humanidad puede disfrutar de un futuro próspero con la IA. Habiendo logrado crear potentes sistemas de IA, ahora podemos disfrutar de un "verano de IA" en el que cosecharemos los frutos, diseñaremos estos sistemas para el claro beneficio de todos y daremos a la sociedad la oportunidad de adaptarse*"[15].

La presencia de la IA en nuestras vidas ha ocurrido a una velocidad de vértigo y eso es lo que hace difícil de predecir los problemas que podemos encontrarnos y valorar su impacto. Por ello, es más necesario que nunca tener claro el rumbo. Lo moral no consiste en mapas de carreteras, ya cerrados, sino en una brújula que señala el norte, como dice A. Cortina.

14 Resulta muy interesante la radiografía social que el filósofo Han, Byung-Chul realiza, especialmente en su libro "Infocracia. La digitalización y la crisis de la democracia". Es un campo de cultivo para la desinformación y la manipulación.

15 Pause Giant AI Experiments: An Open Letter - We call on all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4. https://futureoflife.org/open-letter/pause-giant-ai-experiments/

4.1. La esencial presencia de la ética en el proceso de desarrollo y uso de la IA

La IA avanza a una gran velocidad. Es portadora de grandes mejoras para la sociedad, pero también comporta riesgos y eso es algo que preocupa tanto a gobiernos, como a la propia industria.

La Unión Europea (UE) vio los posibles riesgos antes de que la IA se democratizará, y desde el año 2018 empezó a elaborar su estrategia en cuanto a la regulación de la IA. Ese año creó el grupo de expertos que se encargó de elaborar unas Directrices sobre la ética de la IA.

Este trabajo, presentado en abril de 2019, resultó una pieza fundamental para el desarrollo posterior de la regulación en materia de Inteligencia Artificial de Europa. Concretamente, el concepto de fiabilidad y los siete requisitos introducidos por las Directrices éticas han orientado las aproximaciones legislativas en materia de IA.

Antes del mismo, la Estrategia Europea en materia de IA lanzada en 2018[16] quedó reflejada en el Libro blanco de 2020[17], siendo el grupo de expertos de alto nivel sobre Inteligencia Artificial (High-Level Expert Group On Artificial Intelligence, AI HLEG)[18], grupo independiente de 52 expertos procedentes del mundo académico, empresarial y de la sociedad civil y que en su documento, expone los criterios para que desarrolladores y usuarios pueden asegurarse de que la IA respeta los derechos fundamentales, la normativa aplicable y los principios básicos de la Unión Europea, y cómo la tecnología puede ser técnicamente robusta y fiable en este contexto.

16 Estrategia Europa de Inteligencia Artificial. Accesible desde: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:237:FIN

17 Libro Blanco de Inteligencia Artificial de la Comisión Europea. Accesible desde: https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_es?filename=

18 European Comission - High-level expert group on artificial intelligence: https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

La idea de la UE no era otro crear un modelo de gobernanza integrador de los sistemas de IA común a todos los estados miembros que permitiera proteger los derechos y libertades de los ciudadanos, al mismo tiempo que se fomentará la investigación y la innovación industrial, pero garantizando la seguridad y los derechos fundamentales de todos los ciudadanos europeos, otorgando a los retos desde el punto de vista ético un papel central en el proceso de debate.

El 24 de enero de 2024, la Comisión Europea aprobó la creación de la nueva Oficina Europea de Inteligencia Artificial (IA)[19] que tiene por objeto supervisar el cumplimiento y la aplicación de esta nueva tecnología dentro de los 27 países. La oficina funciona desde el 21 de febrero de 2024 y está en Bruselas.

A lo largo de la regulación de los sistemas de IA, la ética ha tenido un papel fundamental. Según las Directrices, la ética puede ayudarnos a discernir lo que debemos hacer en lugar de solo enfocarnos en lo que se puede hacer con la tecnología actual. El objetivo de estas directrices es hacer de la ética una base primordial. Como se mencionó, las Directrices son la base sobre la que se construye la actual regulación de la IA en la UE. La UE reconoce que la IA avanza rápidamente y que la experimentación requiere un entorno controlado que promueva una innovación responsable y la implementación de controles éticos para mitigar los riesgos inherentes al desarrollo de la IA. Especial relevancia adquiere en áreas que no se consideran de alto riesgo.

Concretamente, según las Directrices, una IA confiable debería ser:

1) legal: respetando todas las leyes y regulaciones aplicables
2) ética: respetar los principios y valores éticos
3) robusta, tanto desde una perspectiva técnica como teniendo en cuenta su entorno social

En dichas directrices,

1) Con un enfoque basado en los derechos fundamentales, se identifican los principios éticos que deben respetarse en el desarrollo, despliegue y utilización de los sistemas de IA. Recogen cuatro principios éticos:
    a) Respeto de la autonomía humana.
    b) Prevención del daño.

19 La Oficina Europea de IA es el centro de la experiencia en IA en toda la UE. Desempeña un papel clave en la implementación de la Ley de IA, especialmente para la IA de propósito general, fomentando el desarrollo y el uso de IA confiable y la cooperación internacional. Accesible desde: https://digital-strategy.ec.europa.eu/es/policies/ai-office

c) Equidad.

d) Explicabilidad.

2) Estos principios se traducen posteriormente en siete requisitos concretos para hacer realidad una IA fiable que son aplicables a todos los que participan en algún momento del ciclo de vida de los sistemas de IA: desarrolladores, responsables del despliegue y usuarios finales, así como a la sociedad en su conjunto. Los sistemas deben cumplir esos requisitos para conseguir una IA fiable.

   Los siete principios son: acción y supervisión humanas; solidez técnica y seguridad; gestión de la privacidad y de los datos; transparencia; diversidad, no discriminación y equidad; bienestar social y ambiental, y rendición de cuentas[20].

3) Se dan una serie de orientaciones sobre cómo lograr una IA fiable

Concretamente, y de forma muy ejecutiva, los principios éticos en los que debe basarse el desarrollo de la IA, se concretan en los siguientes:

1) **Autonomía humana**: los sistemas de IA no deberían subordinar, coaccionar, engañar, manipular, condicionar o dirigir a los seres humanos. Por eso es tan importante garantizar la supervisión y el control humano sobre los sistemas de IA.

2) **Prevención del daño:** la IA no debe generar un perjuicio. Especialmente que no tengan usos malintencionados.

3) **Equidad:** tiene que haber un compromiso de garantizar una distribución justa e igualitaria de los beneficios y costes, y asegurar que las personas y grupos no sufran sesgos injustos, discriminación ni

20 https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=OJ:L_202401689

estigmatización. Además, conlleva la capacidad de oponerse a las decisiones adoptadas por los sistemas de IA y por las personas que los manejan. Poder identificar a la entidad responsable de la decisión y explicar los procesos de adopción de decisiones resultan imprescindibles.

4) **Explicabilidad**: tienen que ser procesos transparentes, cuyas decisiones deben poder explicarse a las partes afectadas por ellas. No obstante, hay veces que no se puede explicar por qué un modelo ha generado un resultado en concreto. En estos casos, se denominan algoritmos de «caja negra» y debe ser algo a extinguir. De hecho, ya existen proyectos en esta línea. Lamentablemente, hemos normalizado muchas veces este efecto, asumiendo la falta de transparencia como algo propio de la programación. En tales circunstancias, puede ser necesario incorporar otras medidas relacionadas con la explicabilidad (por ejemplo, la trazabilidad, la auditabilidad y la comunicación transparente sobre las prestaciones del sistema), siempre y cuando el sistema en su conjunto respete los derechos fundamentales.

   El grado de necesidad de explicabilidad dependerá mucho de la gravedad de las consecuencias derivadas de un resultado erróneo o inadecuado. Sin tener claro cómo el sistema de IA ha llegado a esa conclusión se rompe la confianza.

En esta misma línea, “AI 4People del Atomium European Institute”, señala cuatro principios clásicos, aplicados a entornos digitales, que son:

1) el de beneficencia, poner los progresos al servicio de todos los seres humanos y la sostenibilidad del planeta;

2) el de no-maleficencia, que ordenaría evitar los daños posibles, protegiendo a las personas en cuestiones de privacidad, mal uso de los datos, en la posible sumisión a decisiones tomadas por máquinas y no supervisadas por seres humanos;

3) el principio de autonomía de las personas, por lo que el control y las decisiones significativas deben estar en manos de los seres humanos.

4) El principio de justicia, que exige distribuir equitativamente los beneficios.

Vemos pues que todo ello nos lleva a pensar que estamos ante una regulación antropocéntricas, en la que la IA es una herramienta cuya función principal es mejorar la vida del ser humano y si bien éste tiene que confiar en la herramienta, siempre estará en la última fase del proceso, ejerciendo supervisión y control, asegurándose de que a través de la IA no se perjudica a nadie, que no se excluyen

a colectivos más vulnerables y que, en definitiva, los sistemas de IA mejoran la vida.

Por tanto, resulta imprescindible preservar la autonomía humana, siendo esta la capacidad de autorregularse, vinculada al reconocimiento de la dignidad humana, que podríamos considerar como el núcleo de la ética. Aunque se usen sistemas de IA, no son autónomos, son los seres humanos los que son responsables, puesto que ellos sí tienen la capacidad de ser autónomos, siendo los que han creado la propia IA de la que ahora hablamos. La autonomía comporta:

1) No puede ponerse en manos de una máquina cuestiones que afecten a la vida de una persona sin supervisión humana

2) La responsabilidad moral es humana.

3) El ser humano debe saber si está hablando con otra persona o con un robot. No debe dar lugar al engaño.

4) La ética debe ser la de los humanos aplicada a los entornos digitales, no dotar de una ética a los sistemas de IA. Aunque Cortina se plantea como objeto de reflexión si ¿una ética de la Inteligencia Artificial es la que deben practicar los sistemas inteligentes desde sus propios valores, o es la que los seres humanos deberíamos adoptar para servirnos de los sistemas inteligentes? Para Degli-Esposti (2) se podría plantear generar códigos morales para incluirlos en los propios sistemas de IA.

4.2. Una Inteligencia Artificial libre de sesgos humanos

Aunque los sesgos son objeto de numerosos estudios en el campo de la psicología, podemos simplificar el concepto a lo que todos entendemos por sesgo, definiéndolo como una orientación o tendencia al

analizar una información, pudiendo afirmar que las personas cuentan habitual e inconscientemente de multitud de sesgos que provienen de nuestros sistemas culturales y emocionales.

Cuando hablamos de *"sesgo algorítmico"* nos referimos a que determinadas predicciones de los sistemas, benefician recurrentemente a un grupo de individuos frente a otro, generando discriminaciones en dicha selección.

Una IA sin sesgos, neutra, fuerte, puede ayudar más a las personas, que los sistemas actuales gestionados por humanos. Las decisiones basadas exclusivamente en datos, objetivas, sin presencia de corrupción, nepotismo, o cualquier otra manifestación de parcialidad, dan seguridad y confianza al ciudadano, presumiendo que los sistemas de IA son infalibles, generando confort y por qué no decirlo, comodidad para el propio usuario y el propio sistema social, en la medida en que la decisión final adoptada por la IA es la mejor de todas las posibles atendiendo exclusivamente a datos objetivos.

Obviamente, si bien esto es técnicamente posible, atendiendo a los principios anteriormente expuestos, parece razonable pensar que el modelo adecuado no es un modelo en el que la IA tome las decisiones por sí misma, por muy basadas en criterios objetivos que sea, sino que las decisiones sean adoptadas por humanos, utilizando para ello sistemas de IA. Ese es, sin duda alguna, el camino adecuado.

Ello es así porque, en la medida en que los sistemas de IA han sido desarrollados por los seres humanos, los sistemas de IA cuentan con sesgos que han sido, inconscientemente, transmitidos por parte de éstos durante el desarrollo de estos.

En el documental *"Sesgo codificado"* la *"Liga por la Justicia Algorítimica"* (Algorithmic Justice League) deja claro que los sesgos siguen presentes en los modelos de tomas de decisiones automatizadas, tal y como se evidencia en el ejemplo de Amazon que utilizó un algoritmo para hacer el primer corte de los solicitantes de empleo en una posición técnica, descubriéndose que el sistema de selección básicamente sólo dejaba pasar a hombres blancos en detrimento de las mujeres y particularmente de otras razas, pero ¿por qué se producen los sesgos?

Primero, los sistemas de Inteligencia Artificial son desarrollados por personas que tienen sus propias perspectivas, prejuicios y valoraciones sobre diversos hechos, así como sesgos derivados de sus experiencias. Estos sesgos pueden influir en el diseño y los criterios de evaluación de estos modelos. Si los equipos de trabajo no son lo suficientemente diversos para representar una gran variedad de puntos de vista, es probable que no identifiquen la presencia de sesgos y, por ende, no los corrijan.

En segundo lugar, los sistemas actuales cuentan con la capacidad de aprendizaje automático, también conocido como machine learning. Al igual que los seres humanos aprendemos del entorno a nuestro alrededor, las máquinas aprenden a partir de los datos. Estos datos son un componente fundamental de la Inteligencia Artificial (IA). En realidad, el impresionante desarrollo de la IA se debe más a la disponibilidad de vastas fuentes de datos, tales como teléfonos móviles, redes sociales, digitalización de administraciones y bancos, que a avances técnicos propios.

Los sesgos surgen de los datos. Si existe una distorsión en la representatividad de los datos (sea por sobre- o subrepresentación), las conclusiones que generan los sistemas resultarán discriminatorias. En otras palabras, dado que los datos reflejan la realidad actual, si no se corrigen las inferencias obtenidas, se corre el riesgo de perpetuar o intensificar las desigualdades existentes.

La Inteligencia Artificial se fundamenta en patrones y correlaciones. Los sesgos se originan debido a problemas técnicos y sociales vinculados a diferentes perfiles de personas, ya sea por género, raza, o nivel cultural, y esto es exactamente lo que el algoritmo tiende a replicar. Por ejemplo, la falta de datos sobre mujeres se debe a que hay menos información disponible para describir la realidad femenina en comparación con la masculina. Las mujeres pasan menos tiempo en Internet que los hombres, generando así menos datos, y este desfase no es corregido por los desarrolladores de sistemas de IA.

En tercer lugar, puede darse lo que se denomina el sesgo de implementación que supone aplicar el modelo en un escenario diferente al que ha servido de base a lo datos, pudiendo dar resultados injustos[21].

21 R. González-Sendino, E. Serrano, J. Bajo, P. Novais. A Review of Bias and Fairness in Artificial Intelligence, International Journal of Interactive Multimedia and Artificial Intelligence, (2023), http://dx.doi.org/10.9781/ijimai.2023.11.001

Por ello, los sistemas de IA deben cumplir una serie de estándares éticos y estar sometidos a estrictas medidas de supervisión y control. De lo contrario, tendremos, inevitablemente, resultados discriminatorios.

Pero también podemos encontrarnos que el creador del algoritmo quiera, de forma manipulativa, generar una recomendación o tendencia.

Vemos pues, que es una prioridad eliminar los sesgos. ¿Cómo se puede lograr? Es imprescindible tener equipos representativos de la diversidad y aplicar perspectivas para corregir deformaciones propias de la sociedad y auditarlos. Los equipos heterogéneos transversales mitigan muchos de los sesgos injustos que pueden darse. Pero esta diversidad tiene que afectar a todos los niveles de jerarquía.

Asimismo, al igual que en las políticas públicas, los algoritmos deben incorporar perspectivas específicas para garantizar una protección especial, como puede ser la de género. Una posible estrategia sería equilibrar los datos para evitar que los modelos resulten discriminatorios o injustos, dependiendo de la situación que se está modelando. Otra opción podría consistir en inducir al sistema a utilizar representaciones no asociadas con características susceptibles de discriminación. Incluso, se podría requerir que el sistema ignore atributos protegidos, tales como género, etnia u otras características demográficas, al momento de tomar decisiones. No obstante, es fundamental proceder con cautela al diseñar estas soluciones, ya que, aunque ciertos atributos como género o grupo étnico sean ocultados al sistema, la correlación entre esos atributos y otras variables subsistirá.

Como señala De Zárate[22] algunos estudios del año 2018 demostraban que, mientras que casi el 100% de los hombres blancos eran reconocidos de manera exitosa por sistemas de reconocimiento facial, el éxito disminuía hasta un 35 % en el caso de las mujeres racializadas. Y es que es así como funciona la IA, buscando patrones de repetición, de ahí la importancia de nutrirla con muchos datos diversos y representativos.

El sistema identifica patrones con un grupo, bien porque funciona mejor con ellos al conocer mejor su realidad, su fisionomía, o porque al ser la muestra, mucho más grande, el algoritmo identifica supuestas relaciones causales que realmente no lo son. En algunos casos, ha sucedido que, a pesar de que un sistema de IA estaba entrenado con datos representativos, el algoritmo ha acabado encontrando patrones que permanecían ocultos y que no habían sido detectados anteriormente, reproduciendo así estereotipos por ejemplo de género.

22 DE ZÁRATE ALCARAZO, Lucía Ortiz. Sesgos de género en la Inteligencia Artificial. Revista de occidente, 2023, vol. 502, no 1.

Finalmente es muy importante realizar auditorías. La neutralidad que muchas veces predicamos de los sistemas de IA debe ser comprobada.

Para llegar a este punto queda un largo recorrido. Como indica Ferrante[23], los algoritmos tienen sesgos que amenazan con perpetuar e incluso profundizar las desigualdades del presente.

Si se pudieran evitar los sesgos injustos, los sistemas de IA podrían incluso aumentar la equidad social. La equidad algorítmica es un campo de estudio. Detectar sesgos y mitigarlos es esencial para garantizar decisiones justas y libres de discriminación. Los sistemas de IA pueden mantener o incluso incrementar inadvertidamente los prejuicios sociales.

4.3. El uso ético de la Inteligencia Artificial

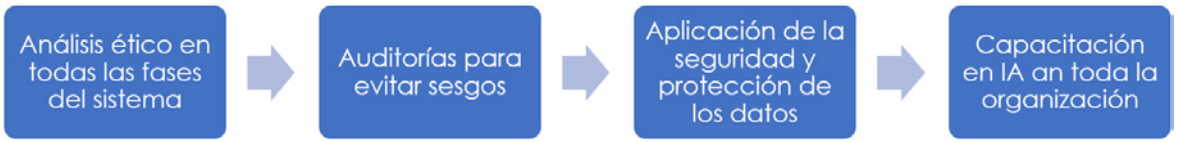
Es clave la existencia de una cultura ética tanto en los desarrolladores de sistema de IA, como en los usuarios de esta. Trasladar esta cultura ética es algo que corresponde a todos los implicados en la organización, desde la junta de accionistas ,los consejos de administración, CEO y todos los trabajadores, haciéndose extensivo a proveedores y clientes. De esta forma, estamos diseñando nuestra cultura ética que debemos dotar de herramientas para poder establecer actuaciones que sean conforme a ella. Antes de iniciar cualquier desarrollo o implementar algún procedimiento, se deben identificar posibles dilemas éticos y analizar cómo se van a tratar, qué camino seguir.

Las empresas que utilizan la IA en sus procesos deben implementar un marco ético en que se validen aspectos como los datos que se manejan, puesto que estamos, en muchos casos, hablando de información sensible y confidencial y transparencia. Deben ser procedimientos

23 FERRANTE, Enzo. Inteligencia Artificial y sesgos algorítmicos ¿Por qué deberían importarnos? Nueva sociedad, 2021, no 294, p. 27-36.

auditables y que establezcan sistema de resolución rápida en caso de detectar algún elemento que no se considere dentro del que el marco ético de la empresa ha establecido.

1) El análisis ético debe observarse en todas las fases de la implementación de un sistema de IA, desde su creación hasta el uso diario.
2) Auditar para evitar sesgos.
3) Tener siempre presente la seguridad y privacidad de los datos
4) Debe existir capacitación a todos los miembros de la organización sobre la IA responsable.



Aspectos esenciales a la hora de hacer efectiva la ética en materia de IA:

1) Analizar y valorar los riesgos éticos antes de empezar cualquier desarrollo o implementación. Para ello es deseable incorporar opiniones heterogéneas que puedan identificar posibles riesgos.
2) Auditar parámetros éticos de forma expresa. Sería interesante poder establecer sistemas mesurables, con métricas
3) Crear una figura / órgano especialista en ética como por ejemplo la Junta ética de IA de IBM que “se creó como organismo multidisciplinar central que apoya una cultura de IA ética, responsable y de confianza en todo IBM” tal como aparece en la presentación de la propia compañía.

Destacable es el Consejo de ética de la IA de Open AI que es un organismo interdisciplinario que quiere convertirse en líder de identificación, asesoramiento y tratamiento de las cuestiones éticas derivadas de la IA y el impacto en comunidades subrepresentadas o excluidas.

A partir de aquí la organización puede desarrollar con mayor grado de precisión la presencia de la ética en procedimientos relacionados con la IA.

Al igual que establece la normativa de la UE, las organizaciones deben poner en el centro de su universo al ser humano. Conviene recordar el grupo de expertos señala que una IA confiable debe garantizar un propósito ético y debe ser técnicamente robusta y fiable, ya que, incluso con buenas intenciones, la falta de dominio tecnológico puede causar daños involuntarios.

5. Responsabilidades derivadas del uso de sistemas de Inteligencia Artificial

5.1. Responsabilidad penal de la persona jurídica

Los modelos de Inteligencia Artificial buscan, según sus promotores, estar al servicio de la humanidad para mejorar nuestra calidad de vida, mediante la optimización de recursos, la automatización de procesos, y la mejora de cualquier actividad que realizamos en el día a día.

Pero, así como estarán presentes en todos los procesos productivos de las empresas, es probable que produzcan resultados lesivos para las personas, sea por diseño o uso incorrecto.

Van a ser tan peligrosos como lo es un coche diseñado con fallas de seguridad y conducido de forma temeraria, y tan seguro como el que cumple con estándares de seguridad y es conducido por una persona diligente.

El caso del *flash crash* ocurrido el 6 de mayo de 2010 en Estados Unidos, en el que hubo una variación de los durante un pequeño lapso que alteró el mercado de valores, es un ejemplo. De hecho, las autoridades que intervinieron resaltaron que "*la interacción entre los programas de ejecución automatizada y las estrategias de trading algorítmico puede erosionar rápidamente la liquidez y resultar en mercados desordenados*".

Desafortunadamente, como ocurrió con toda invención tecnológica, la Inteligencia Artificial también será utilizada para cometer delitos, tanto por personas físicas como jurídicas.

Desde 2010 las personas jurídicas pueden ser penalmente responsables por ciertos delitos cometidos en su nombre y en su beneficio. Esta responsabilidad puede surgir de dos maneras: por la conducta delictiva de sus representantes legales o por la falta de supervisión

adecuada que permita la comisión de delitos por sus subordinados.

Es decir, la forma de atribución puede ocurrir por vía vicarial o de transferencia, o por autorresponsabilidad, sea porque los delitos fueron cometidos por los representantes legales o personas con facultades similares de control -capaces de tomar decisiones, obligar o actuar en nombre de la empresa-, o por otras personas bajo su vigilancia siempre que ocurra un grave incumplimiento de los deberes de supervisión, vigilancia y control. La comisión del delito por parte de una persona física es presupuesto común a ambas.

Más allá de eso, la ley reconoce la "la responsabilidad autónoma de la persona jurídica por medio de la regulación de los programas de organización y gestión, a los que atribuye valor eximente bajo determinadas condiciones" (Circular 1/2016, Fiscalía General), es decir, la obligatoriedad de las personas jurídicas de controlar y vigilar sus procesos de producción para evitar que las personas que actúan a su servicio le generen beneficios -directos o indirectos- mediante la comisión de delitos. Los controles y defectos de organización son fundamentales a la hora de analizar la atribución de la responsabilidad penal de la persona jurídica.

Los delitos por los cuales las personas jurídicas pueden ser condenadas y las penas aplicables están expresamente previstos en el código penal, pudiendo beneficiarse de ciertas exenciones o atenuaciones en los casos en los que se acrediten las condiciones y requisitos de los modelos de organización y gestión y programas de compliance.

5.1.1. La Responsabilidad Penal de las Personas Jurídicas en el Uso de la Inteligencia Artificial

En el caso de la Inteligencia Artificial, si una persona jurídica —las personas físicas que la integran— utiliza la tecnología para cometer un delito y se demuestra que no se ejercieron correctamente los deberes de supervisión, vigilancia y control con relación a su uso, podría considerarse responsable penalmente, si se la acusa de los delitos por los que pueda ser condenada.

Según lo establecido por el art. 31 ter del Código Penal, aunque la persona responsable del diseño o uso ilícito de la Inteligencia Artificial no sea individualizada o no sea posible dirigir el procedimiento contra ella, la persona jurídica podría ser condenada y, en determinados casos, aunque concurra imprudencia (caso de los delitos previstos en los arts. 259.3, 331, 302.2, 576.5 CP).

También hay que considerar que las capacidades de independencia y autonomía de la Inteligencia Artificial no siempre serán opuestas, un discurso en el que se argumenta la dificultad de prever el comportamiento de determinados modelos de

Inteligencia Artificial. Dependiendo del sector en el que la empresa opere y especialmente en sectores regulados, podría ser rechazada sobre la base de la obligación de gestionar adecuadamente los riesgos inherentes al producto que se fabrica, distribuye o vende.

Esto significa, sobre todo después del lanzamiento del RIA, y en aquellos sectores regulados en los que la Inteligencia Artificial fue incorporada a los ordenamientos, que las personas jurídicas tienen la obligación de conocer el grado de peligrosidad del producto que se fabrica, distribuye o vende, es decir, conocer sus riesgos y gestionarlos mediante la implementación de controles y procedimientos adecuados. Justamente, la falta de previsibilidad causada por la ausencia de control es la que puede determinar la atribución de la responsabilidad penal de la persona jurídica.

En ese sentido, la omisión de los órganos de supervisión en la implementación de los controles y procesos necesarios para prever y evitar los riesgos derivados de la Inteligencia Artificial, para ahorrar recursos, disminuir costes, o aumentar ganancias, sería causal suficiente para atribuir responsabilidad penal a la persona jurídica.

Por lo tanto, la responsabilidad penal de la persona jurídica en el uso de la Inteligencia Artificial es posible, siempre que se den las condiciones previstas en el art. 31 bis, ter y siguientes del CP.

5.1.2. La importancia de los programas de compliance

En tales casos entran y cobran especial relevancia los programas de compliance y de gestión de riesgos. En el contexto del uso de la Inteligencia Artificial, las personas jurídicas deben asegurarse de implementar mecanismos de supervisión y control adecuados para prevenir la comisión de delitos y evitar así incurrir en responsabilidad penal.

Los programas de compliance penal deberán incorporar el análisis y evaluación de los riesgos derivados en el uso

de la Inteligencia Artificial y su posible impacto en los productos y servicios ofrecidos que, de una u otra forma, podrían derivar en la atribución de responsabilidad penal.

En este marco deberán asegurarse de que el modelo de Inteligencia Artificial utilizado o lanzado como producto sea seguro, es decir, que no represente un riesgo o sea mínimo, que pueda ser utilizado en condiciones de normalidad o razonablemente previsibles, de forma prolongada durante un lapso previsible.

Los equipos de compliance deben preguntarse; ¿El uso de la Inteligencia Artificial en el caso concreto es idóneo para lesionar bienes jurídicos? ¿El uso de la Inteligencia Artificial incrementa el riesgo en el producto específico? En tal caso, la identificación y propuesta de soluciones para prevenirlos es fundamental.

5.2. Responsabilidad administrativa

El uso de los sistemas de IA en la vertiente de responsabilidad administrativa se abordará desde una doble perspectiva: (i) El régimen sancionador establecido en la normativa vigente especialmente en el reciente RIA; y, (ii) La responsabilidad de las administraciones públicas derivada del uso de la IA.

5.2.1. El régimen sancionador establecido en RIA

Dicho régimen sancionador viene regulado en los artículos 99 a 101 del RIA, en el que se establecen sanciones a los distintos actores que intervienen en estos procesos (artículo 99), multas administrativas a instituciones, órganos y organismos de la Unión (artículo 100), y multas administrativas Multas a proveedores de modelos de IA de uso general (artículo 101).

5.2.1.1. Sanciones que se imponen por infracciones del ria que cometan los operadores[24]

Adoptarán todas las medidas necesarias para garantizar que se aplican de forma adecuada y efectiva y teniendo así en cuenta las directrices emitidas por la Comisión con arreglo al artículo 96 del Reglamento.

El no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 35 millones de euros o hasta el 7% de su volumen de negocios mundial total correspondiente al ejercicio anterior, si esta cuantía es superior.

A modo de resumen, entre estas prácticas estarían los sistemas de IA que manipulan las decisiones de las personas o explotan sus vulnerabilidades, aquellos que evalúan o

24 «operador»: un proveedor, fabricante del producto, responsable del despliegue, representante autorizado, importador o distribuidor;

clasifican a las personas en función de su comportamiento social o sus rasgos personales, y los sistemas que predicen el riesgo de que una persona cometa un delito. Asimismo, el RIA también prohíbe los sistemas de IA que extraigan imágenes faciales de Internet o de grabaciones de CCTV, infieran emociones en el lugar de trabajo o en instituciones educativas y clasifiquen a las personas en función de sus datos biométricos. Sin embargo, se hacen algunas excepciones con fines policiales, como la búsqueda de personas desaparecidas o la prevención de atentados terroristas.

El incumplimiento de otras disposiciones que constan a continuación, distintas de las reguladas en el artículo 5 del RIA estará sujeto a multas de hasta 15 millones de euros o hasta el 3% de su volumen de negocios mundial total correspondiente al ejercicio anterior, si esta cuantía es superior.

Esto incluye obligaciones de proveedores (art. 16), representantes autorizados (art. 22), importadores (art. 23), distribuidores (art. 24), responsables del despliegue (art. 26), organismos notificados (art. 31, 33 y 34), y la transparencia de proveedores y responsables del despliegue (art. 50).

La presentación de información inexacta, incompleta o engañosa a organismos notificados o a las autoridades nacionales competentes en respuesta a una solicitud estará sujeta a multas administrativas de hasta 75 millones de euros o, si el infractor es una empresa, de hasta el 1% del volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.

En cuanto a las sanciones a imponer a instituciones, órganos y organismos de la Unión, el RIA (artículo 100), establece los criterios de graduación de la multa, y distingue las cuantías en función de la infracción, según sean del artículo 5 o de las distintas previstas en dicho artículo.

5.2.1.2. Sanciones que se imponen a proveedores[25] de modelos de AI de uso general

La Comisión podrá imponer multas a los proveedores de modelos de IA de uso general que no superen el 3 % de su volumen de negocios mundial total anual correspondiente al ejercicio financiero anterior o de 15 millones de euros, si esta cifra es superior, cuando la Comisión considere que, de forma deliberada o por negligencia.

Dichas sanciones podrán imponerse cuando:

1) Se incumplan las disposiciones pertinentes del presente Reglamento;
2) No se atienda una solicitud de información o documentos con arreglo al artículo 91, o han facilitado información inexacta, incompleta infringieron o engañosa;
3) Se incumpla una medida solicitada en virtud del artículo 93.
4) No se otorgue acceso a la Comisión al modelo de IA de uso general o al modelo de IA de uso general con riesgo sistémico para que se lleve a cabo una evaluación con arreglo al artículo 92.

Asimismo, se toman en consideración que, además de la naturaleza, gravedad y duración de la infracción, se tendrán en cuenta los compromisos contraídos de conformidad con el artículo 93, apartado 3, y en los códigos de buenas prácticas pertinentes previstos en el artículo 56.

El referido artículo 56 (Código de buenas prácticas), promueve la elaboración de estas normas, tanto por todos los proveedores de modelos de IA de uso general, como a las autoridades nacionales competentes pertinentes, velando porque comprendan las obligaciones establecidas en los artículos 53 y 55.

5.2.2. La responsabilidad de las administraciones públicas derivada del uso de la IA

La responsabilidad administrativa desde la perspectiva de la administración pública como sujeto, tiene como fines y objetivos la subsanación de la actuación deficiente de las administraciones públicas en el ejercicio de su actividad y la satisfacción (resarcimiento), a los administrados de aquellos perjuicios que se les irrogan derivados del deficiente funcionamiento de las administraciones públicas en el

25 «proveedor»: una persona física o jurídica, autoridad, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente;

ejercicio de las actividades que le son propias o que éstas realizan.

Entre los requisitos que deben concurrir para poder exigir la responsabilidad administrativa (comprobación de la existencia de un hecho imputable a la Administración Pública como titular de la actividad; que dicho hecho produzca un daño de naturaleza patrimonial que pueda cuantificarse económicamente; existencia de nexo causal entre el hecho imputado a la Administración y el daño producido; y la ausencia de fuerza mayor), debe destacarse el parámetro de calidad en el uso por parte de la Administración Pública de los sistemas de Inteligencia Artificial.

Dicho parámetro puede traducirse en distintos principios:

1) El de transparencia en el diseño del software.

2) Que dicho diseño esté realizado con el objetivo de evitar sesgos y desigualdades.

3) El principio de personalización y proactividad [26].

4) Respeto al derecho fundamental a la protección de datos personales a través del diseño de las tecnologías de IA en base al principio de minimización de datos y el conocido como privacidad desde el diseño.

Además de los requisitos que deben cumplirse en;

1) Los procesos a través de los cuales la Administración Pública acceda a las tecnologías de IA (licitaciones, contratación, etc.), en materia de obtención de informes técnicos y verificación de la programación de los algoritmos, y en definitiva,

26 Establecido en la letra f) del artículo 2 del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. Definición: "la capacidad de las Administraciones Públicas para que, partiendo del conocimiento adquirido del usuario final del servicio, proporcione servicios precumplimentados y se anticipe a las posibles necesidades de los mismos".

que ha existido un control de legalidad necesario sobre los elementos que configuran el sistema y;

2) De los que deban cumplirse por la propia Administración Pública para desarrollar dichos productos que adquiera para el ejercicio de las actividades que tiene encomendadas; debemos resaltar aquellos supuestos y procedimientos administrativos en los que se adoptan decisiones a través del uso de tecnologías de Inteligencia Artificial, se garantice que dichas decisiones dispongan de motivación, que ésta sea adecuada y que el administrado tenga a su alcance conocer las razones en las que se ha sustentado la decisión adoptada.

Y es ahí donde entra el instrumento de la "responsabilidad" que garantiza o podrá garantizar al administrado que, si una decisión de la administración carece de motivación, o de una motivación adecuada y razonable con el empleo de tecnologías que apliquen la Inteligencia Artificial, generadora de un perjuicio pueda reclamar dicha responsabilidad.

La propia gestión documental realizada por la Administración Pública, entendida como una actividad que puede llevar a la desvinculación de los datos del documento original y procesarlos independientemente, con la posibilidad, dada la desvinculación del dato al documento, de otorgarles un tratamiento diferenciado, puede comportar o llevar a una toma de decisiones derivada a la aplicación de los correspondientes algoritmos por un sistema que pueda considerarse, per se, inteligente y ajeno (en lo que sería la adopción de la decisión), a la propia administración pública motivo por el cual, y con el fin de mitigar el riesgo de un resultado anormal, arbitrario o no motivado de la decisión adoptada que ponga fin al proceso aplicado por la administración pública, con las garantías necesarias para el administrado.

5.3. Responsabilidad civil

La responsabilidad civil o derecho de daños forma parte de la normativa civil y tiene por objeto determinar cómo compensar o resarcir a quien ha sufrido un daño, y quién y de qué forma hay que hacerlo.

Tiene una función reparadora y compensatoria y es de dos tipos, la responsabilidad civil contractual y la responsabilidad extracontractual.

La primera (contractual), tiene su origen en las relaciones contractuales y los perjuicios derivados de su incumplimiento o de un cumplimiento defectuoso, y la segunda (extracontractual), deriva de un hecho o un evento en el que, interviniendo culpa o negligencia, propia o de terceros, se produce un daño a una persona física o jurídica que debe ser resarcido.

Sus elementos esenciales son: (i) el daño, conceptuado como una lesión material o moral, que puede ser emergente (el perjuicio realmente sufrido), o por lucro cesante (la ganancia dejada de obtener); y (ii) la relación de causalidad entre la acción u omisión y el resultado perjudicial o dañoso.

Por su parte, los sujetos de la responsabilidad civil derivan de si el daño es por un hecho propio o por un hecho ajeno (los realizados por aquellas personas de quienes se debe responder).

En el plano normativo, cada estado de la UE tiene regulado o establecido su sistema de responsabilidad civil, que no es uniforme en todos los estados miembros, en elementos tales como el título de imputación (responsabilidad objetiva o subjetiva), el ejercicio de las acciones de reclamación o los plazos de prescripción.

En el contexto actual, se produce un incremento exponencial en el uso de sistemas de IA en numerosos ámbitos de la sociedad, lo cual va indisolublemente unido a la necesidad de establecer un sistema de responsabilidad que pueda aplicarse cuando dichos sistemas “fallan” o producen perjuicios para sus usuarios o destinatarios finales.

El legislador nacional y supranacional es consciente de los riesgos “tangibles” derivados del uso de dichos sistemas[27], de la probabilidad de que puedan producir

27 El REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, en su considerando (5), dispone que: Al mismo tiempo, dependiendo de las circunstancias relativas a su aplicación, utilización y nivel de desarrollo tecnológico concretos, la IA puede generar riesgos y menoscabar los intereses públicos y los derechos fundamentales que protege el Derecho de la Unión. Dicho menoscabo puede ser tangible o intangible e incluye los perjuicios físicos, psíquicos, sociales o económicos. Esta cuestión ya se mencionaba en el Libro Blanco de la UE de 2020 sobre la Inteligencia Artificial: (pág.14), como uno de los principales problemas que hacen necesaria una regulación de la IA: “Aunque la IA puede ofrecer muchas ventajas, por ejemplo, mejorando la seguridad de los productos y los procedimientos, también puede resultar nociva. Los daños pueden ser tanto materiales (para la seguridad y la salud de las personas, con consecuencias como la

daños de toda índole (económicos, morales, sicológicos, … etc.)[28] y de la necesidad de establecer un régimen que, en defensa del perjudicado, pueda aplicarse a proveedores, fabricantes, operadores, y resto de intervinientes con el fin de "resarcirle" de dichos daños[29].

Todo ello no es óbice para que existan distintas corrientes de opinión respecto de cómo debe regularse la responsabilidad civil con la irrupción de los sistemas de IA, como lo son aquellas que consideran que el sistema de tradicional de responsabilidad por daños y sus elementos, adaptado a la nueva realidad generada por estas nuevas tecnologías, es suficiente[30] y aquellas otras que postulan que debe construirse "ex novo", un nuevo sistema de responsabilidad, pues consideran que la complejidad y la autonomía e imprevisibilidad en la toma de decisiones de estos sistemas, desdibujan los sujetos intervinientes en la cadena de responsabilidad, los criterios tradicionales de imputación y, en definitiva, que *las herramientas vigentes no pueden enfrentar los problemas que plantean los daños originados por esos sistemas de Inteligencia Artificial fuerte"*[31].

Quienes son partidarios de regular un nuevo sistema de responsabilidad derivada del uso de la IA y de conferir personalidad jurídica a determinados sistemas inteligentes (personalidad electrónica), estarían más próximos a atribuir la condición de "responsables" a algunos de estos sistemas, mientras que los que postulan una adaptación de las instituciones tradicionales de la responsabilidad civil por daños, no ven la necesidad de atribuir personalidad jurídica a lo que consideran cosas,

muerte, y menoscabos al patrimonio) como inmateriales (pérdida de privacidad, limitaciones del derecho de libertad de expresión, dignidad humana, discriminación en el acceso al empleo, etc.) y pueden estar vinculados a una gran variedad de riesgos".

28 El REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, articulo 3, Definiciones, apartado 49) define como «incidente grave»: un incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga alguna de las siguientes consecuencias: a) el fallecimiento de una persona o un perjuicio grave para su salud; b) una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas; c) el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales; d) daños graves a la propiedad o al medio ambiente.

29 El REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, en su considerando (79), dispone que conviene que una persona física o jurídica concreta, definida como el proveedor, asuma la responsabilidad asociada a la introducción en el mercado o la puesta en servicio de un sistema de IA de alto riesgo, con independencia de si dicha persona física o jurídica es o no quien diseñó o desarrolló el sistema.

30 Vid. Derecho de contratos, responsabilidad extracontractual e Inteligencia Artificial. Obra colectiva. pág. 346 y ss., Capítulo VII. La responsabilidad civil causada por la IA, Mª Luisa Atienza Navarro (Asociación de profesoras y profesores de Derecho Civil. Editorial ARANZADI. 2024), citando a RUBI PUIG, A, en "retos de la Inteligencia Artificial y adaptabilidad del derecho de daños", en AA.VV. Retos jurídicos de la Inteligencia Artificial, Aranzadi, Navarra, 2020, pág. 63 y 64.

31 Vid. Derecho de contratos, responsabilidad extracontractual e Inteligencia Artificial. Obra colectiva. pág. 346 y ss., Capítulo VII. La responsabilidad civil causada por la IA, Mª Luisa Atienza Navarro (Asociación de profesoras y profesores de Derecho Civil. Editorial ARANZADI. 2024), página 361, citando, entre otros, a BOTELLO HERMOSA, SANTOS GONZALEZ y HERNAEZ ESTEBAN.

máquinas o sistemas que siempre son dependientes de los entes con personalidad (personas físicas o jurídicas).

La definición de IA establecida por el no resuelve (o al menos de dicha definición no se infiere), si debe conferírsele personalidad jurídica, o no, a determinados sistemas de IA, si bien es cierto, que, de momento, la Resolución del Parlamento Europeo, de 20 de octubre de 2020, que propone un Reglamento del Parlamento Europeo y del Consejo relativo a la responsabilidad civil por el funcionamiento de los sistemas de IA, se decanta por NO conferir personalidad jurídica a dichos sistemas[32].

La actual corriente normativa en Europa atribuye a los sistemas de IA la condición de "objeto o instrumento generador de responsabilidad" y "no" de sujeto[33].

Y esta cuestión entraña ciertos problemas si se quiere utilizar la "culpa" como criterio de imputación de responsabilidad (el subjetivo), al "operador".

De las distintas subcategorías existentes de responsabilidad subjetiva, parece que la responsabilidad por daños originados por "el hecho de las cosas", es bastante aceptada, y consistiría en atribuir dicha responsabilidad al "operador", en su *posición abstracta de persona que tiene bajo su control la cosa -la IA[34]-*.

32 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, en su considerando 6º dispone que: Cualquier cambio necesario del marco jurídico vigente debe comenzar con la aclaración de que los sistemas de IA no tienen personalidad jurídica ni conciencia humana, y que su única función es servir a la humanidad. Y en su artículo 1 dispone que: El presente Reglamento establece normas en relación con las demandas por responsabilidad civil de las personas físicas y jurídicas contra los operadores de sistemas de IA.

33 Vid. Derecho de contratos, responsabilidad extracontractual e Inteligencia Artificial. Obra colectiva. pág. 422 y ss., Capítulo VIII. Fernando Peña López (Asociación de profesoras y profesores de Derecho Civil. Editorial ARANZADI. 2024).

34 Vid. Op. Cit., Derecho de contratos, responsabilidad extracontractual e Inteligencia Artificial. Obra colectiva. pág. 424 y pág. 427 ss., Capítulo VIII. Responsabilidad objetiva y subjetiva en las propuestas legislativas europeas sobre responsabilidad civil aplicables a la Inteligencia Artificial. Fernando Peña López.

Los problemas derivados de la atribución subjetiva de responsabilidad o por culpa derivan de varias cuestiones[35]:

En dichos sistemas de responsabilidad dicha culpa se asocia a la identificación de una conducta atribuible a una persona y quien produce el daño es una "cosa".

Por otra parte, tampoco es fácil encajar la "falta de previsibilidad" de los sistemas de IA cuando adoptan decisiones de forma autónoma, aunque aceptemos que se puedan establecer límites, con la imputación de culpa a uno o varios de los operadores que la normativa considera como sujetos intervinientes: (i) sería posible que ninguno de ellos pudiera prever o explicar, ex post, la decisión de la IA generadora del daño; (ii) o, ante una actuación de un sistema inteligente generador de perjuicios, no fuera posible determinar cuál habría sido la "diligencia debida" que pudiera exigirse a cualquiera de dichos sujetos.

De la dificultad para localizar a cuál de todos los intervinientes es el "responsable" que no ha sido diligente, en sistemas en donde es comúnmente aceptada la opacidad de sus procesos de creación, y cómo probar cuál ha sido la concreta negligencia del sistema que ha ocasionado el daño.

En el RIA se establece dicha diligencia debida en la implementación de una serie de medidas de seguridad y control del sistema IA que mitiguen los eventuales daños (monitorización, introducción de mecanismos de desconexión, … etc.).

"La figura del responsable es fundamental, ya que, aunque exista una causa y un resultado (el daño), sin un responsable a quien atribuir la responsabilidad, el sistema de responsabilidad no puede alcanzar su propósito: el resarcimiento."

Al igual que también es "imprescindible" establecer el "sistema" de responsabilidad (objetivo o subjetivo), aplicable, que determinará el cuándo y por qué pueden reclamarse los daños y perjuicios derivados del uso de dichos sistemas.

Posteriormente expondremos las opciones escogidas por el legislador comunitario para regular el régimen de responsabilidad derivado del uso de los sistemas de IA, en las distintas recomendaciones o propuestas emitidas, y aquellas normas más relevantes, aprobadas o en tramitación.

35 Vid. Op. Cit., Derecho de contratos, responsabilidad extracontractual e Inteligencia Artificial. Obra colectiva. pág. 424, pág. 431 y pág. 442 y ss., Capítulo VIII. Responsabilidad objetiva y subjetiva en las propuestas legislativas europeas sobre responsabilidad civil aplicables a la Inteligencia Artificial. Fernando Peña López.

El legislador supranacional (UE), intenta en todas las fases que integran el proceso normativo (informes de expertos, propuestas, directivas y reglamentos), que regula la IA, propiciar el desarrollo de esta tecnología, claramente estratégica y con indudables beneficios para usuarios, empresas y administraciones públicas, y al mismo tiempo, preservar los derechos fundamentales como la privacidad y la no discriminación y la seguridad que pueden verse afectados por la materialización de riesgos tangibles derivados de la creación, implementación y explotación de los sistemas de IA.

Por ello, en materia de consumidores el objetivo es contar con el mismo nivel de protección con independencia de si los productos utilizan modelos os sistemas de IA, lo cual dificulta la identificación de los elementos que integran el sistema tradicional de responsabilidad (el incumplimiento o la culpa y el nexo causal entre conducta y daño o perjuicio[36].

En materia de responsabilidad civil, las propuestas y normas, vigentes o en tramitación más relevantes, son:

1) La Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de Inteligencia Artificial (2020/2014(INL), en cuyo Anexo, se exponen recomendaciones para la elaboración de un Reglamento del Parlamento Europeo y del Consejo relativo a la responsabilidad civil por el funcionamiento de los sistemas de IA, e integran "Propuesta de Reglamento sobre el régimen de responsabilidad civil" que deberá operar en los casos en que un sistema de IA cause daños a un tercero.

36 REGULACION DE LA Inteligencia Artificial EN EUROPA. Incidencia en los regímenes jurídicos de protección de datos y de responsabilidad por productos. Carmen Muñoz García. Tirant Lo Blanch, 2203, pág. 161 y ss.

2) El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de Inteligencia Artificial. Reglamento de Inteligencia Artificial.

3) La Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial (Directiva sobre responsabilidad en materia de IA), de 28.9.2022 COM (2022) 496 final 2022/0303 (COD) (PDRIA).

4) Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos, de 28.9.2022. COM (2022) 495 final 2022/0302 (COD). (PDRP).

5.3.1. Recomendaciones del Parlamento Europeo y del Consejo relativo a la responsabilidad civil por el funcionamiento de los sistemas de IA

Ámbito de aplicación: Tanto a robots como a sistemas de IA que carecen de cuerpo físico (bots), como los sistemas de IA destinados a actividades de inversión financiera.

Personalidad jurídica a efectos de ser responsables civiles. Los sistemas de IA carecen de responsabilidad jurídica, por lo que las demandas de responsabilidad deberán ejercitarse frente a personas físicas o jurídicas. Lo anticipa en el apartado 7 de su introducción[37] y lo reitera en su considerando 6º[38].

Naturaleza o tipos de daño: personales, materiales, económicos y morales (por ejemplo, en casos de daño a la reputación de una marca)[39].

Régimen de responsabilidad objetiva para los daños causados con sistemas de IA de riesgo alto.

37 Observa que todas las actividades, dispositivos o procesos físicos o virtuales gobernados por sistemas de IA pueden ser técnicamente la causa directa o indirecta de un daño o un perjuicio, pero casi siempre son el resultado de que alguien ha construido o desplegado los sistemas o interferido en ellos; observa, a este respecto, que no es necesario atribuir personalidad jurídica a los sistemas de IA; opina que la opacidad, la conectividad y la autonomía de los sistemas de IA podrían dificultar o incluso imposibilitar en la práctica la trazabilidad de acciones perjudiciales específicas de los sistemas de IA hasta una intervención humana específica o decisiones de diseño; recuerda que, de conformidad con conceptos de responsabilidad civil ampliamente aceptados, se puede eludir, no obstante, este obstáculo haciendo responsables a las diferentes personas de toda la cadena de valor que crean, mantienen o controlan el riesgo asociado al sistema de IA;

38 Propuesta de Reglamento Responsabilidad, en su Considerando (6) dispone: Cualquier cambio necesario del marco jurídico vigente debe comenzar con la aclaración de que los sistemas de IA no tienen personalidad jurídica ni conciencia humana, y que su única función es servir a la humanidad.

39 BREVES APUNTES A LA PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO SOBRE RESPONSABILIDAD CIVIL EN MATERIA DE Inteligencia Artificial. Alejandro Zornoza Somolinos. R.E.D.S. núm. 17, Julio-diciembre 2020

Y se trata de una responsabilidad OBJETIVA, que atribuye al operador de un sistema de IA de alto riesgo la responsabilidad derivada de cualquier daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por dicha sistema de IA, e impide que dichos operadores puedan "eludir" su responsabilidad alegando que actuaron con la diligencia debida o que el daño o perjuicio fue causado por una actividad, un dispositivo o un proceso autónomos gobernados por su sistema de IA.

Se les exime de dicha responsabilidad si el daño ha sido provocado por un caso de fuerza mayor.

Están obligados a garantizar que las operaciones del sistema están cubiertas por un seguro de responsabilidad civil adecuado[40] estableciendo los importes máximos de indemnización y los plazos de prescripción. Y se establece que dicha propuesta de Reglamento prevalecerá sobre los regímenes nacionales de responsabilidad civil en caso de clasificación divergente por responsabilidad objetiva de los sistemas de IA.

Responsabilidad subjetiva para los daños causados con sistemas de IA que no supongan un alto riesgo.

El "operador", que quedará eximido de responsabilidad en caso de acreditar: (i) la inexistencia de culpa o daño

40 El operador final de un sistema de IA de alto riesgo garantizará que las operaciones de dicho sistema de IA estén cubiertas por un seguro de responsabilidad civil adecuado en relación con los importes y el alcance de la indemnización previstos en los artículos 5 y 6 del presente Reglamento. El operador inicial garantizará que sus servicios estén cubiertos por un seguro de responsabilidad empresarial o de responsabilidad civil de productos adecuado en relación con los importes y el alcance de la indemnización previstos en los artículos 5 y 6 del presente Reglamento. Si se considera que los regímenes de seguro obligatorio del operador final o inicial ya vigentes con arreglo a otra legislación de la Unión o nacional o los fondos voluntarios existentes de seguros de empresas cubren el funcionamiento del sistema de IA o el servicio prestado, la obligación de suscribir un seguro en relación con el sistema de IA o el servicio prestado con arreglo al presente Reglamento se considerará cumplida siempre que el correspondiente seguro obligatorio existente o los fondos voluntarios existentes de seguros de empresas cubran los importes y el alcance de la indemnización previstos en los artículos 5 y 6 del presente Reglamento.

porque el sistema de IA se activó sin su conocimiento (siempre que se adopten las medidas necesarias para evitar una activación fuera de su control); y (ii) observa la diligencia debida.

La diligencia debida se acredita demostrando que: (i) el sistema de IA elegido era el adecuado para las tareas para las que lo necesitaba; (ii) o que al tiempo de producirse el daño puso el sistema en funcionamiento correctamente; (iii) o que estaba controlando adecuadamente las actividades del sistema cuando se produjo el daño; (iv) o que, a pesar del daño producido, el sistema se encontrase actualizado.

El operador quedará eximido de responsabilidad si concurre una de las posibilidades antes expuestas (que son alternativas y no acumulativas).

El Reglamento completa los sistemas de responsabilidad anteriormente relacionados con determinados criterios de "imputación", que podrían desembocar en una concurrencia de culpas e, incluso, ante una exención total de responsabilidad[41] del operador, cuando en su artículo 10.1 dispone que:

"Si el daño o perjuicio es causado por una actividad física o virtual, un dispositivo o un proceso gobernados por un sistema de IA o por la actuación de una persona afectada o de una persona de la que la persona afectada sea responsable, el alcance de la responsabilidad civil del operador con arreglo al presente Reglamento se reducirá en consecuencia. El operador no será responsable si la persona afectada o la persona de la que esta es responsable es la única a la que se le puede achacar el daño o perjuicio causado".

Tal y como han advertido voces autorizadas[42] es posible la confluencia de disposiciones legales nacionales y del derecho de la unión, que el Reglamento resuelve: (i) Si se trata de un sistema de alto riesgo y existen divergencias con las legislaciones nacionales, prevalecerá la Propuesta de Reglamento; (ii) Si se trata de un sistema no considerado de alto riesgo, En cuanto a plazos de prescripción, importes y alcance de indemnización, se aplicarán las normas de los estados; (iii) En cuanto a los criterios de imputación y causas eximentes, se aplicará la Propuesta de Reglamento[43].

41 La «adaptación» del derecho de daños a la Inteligencia Artificial: la propuesta de Directiva sobre responsabilidad. Manuel Ortiz Fernández

42 EL DERECHO DE DAÑOS ANTE LA Inteligencia Artificial: LA INTERVENCIÓN DE LA UNIÓN EUROPEA. Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567, pp. 1296-1325. Manuel Ortiz Fernández.

43 EL DERECHO DE DAÑOS ANTE LA Inteligencia Artificial: LA INTERVENCIÓN DE LA UNIÓN EUROPEA. Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567, pp. 1296-1325. Manuel Ortiz Fernández.

5.3.2. La Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial

Esta propuesta de norma tiene por objeto establecer unas reglas básicas para intentar aplicar un régimen lo más uniforme u homogéneo posible para indemnizar el perjuicio causado y agilizar la carga de la prueba de los perjudicados, estableciendo una serie de presunciones sin llegar a concretar el tipo de responsabilidad.

No aborda una regulación completa del derecho de daños, por lo que subsisten los sistemas de responsabilidad de los estados miembros, que deberán transponer la Directiva y adaptar su ordenamiento a la misma y al ser una norma de mínimos, no impide que los estados establezcan un régimen jurídico más protector para los perjudicados[44].

Establece un régimen de exhibición de pruebas (artículo 3), obligando a los estados miembros a garantizar que los órganos jurisdiccionales tengan potestad para ordenar a petición del demandante la exhibición por el proveedor de las pruebas pertinentes de que disponga y contempla la presunción de culpabilidad a aplicar por los tribunales al proveedor en caso de incumplimiento de dicha obligación de exhibición (presunción del incumplimiento por parte del demandado de un deber de diligencia pertinente).

Incorpora *"una presunción general del nexo causal entre la culpa y el daño cuando: se haya probado la culpa por el demandante o se haya recurrido a la presunción de la negligencia descrita anteriormente"*. Y se establecen excepciones a dicha presunción en función del tipo de sistema de IA"[45]:

44 La «adaptación» del derecho de daños a la Inteligencia Artificial: la propuesta de Directiva sobre responsabilidad. Manuel Ortiz Fernández. Revista de los Estudios de Derecho y Ciencia Política. IDP N.º 40 (marzo, 2024) I ISSN 1699-8154.

45 La «adaptación» del derecho de daños a la Inteligencia Artificial: la propuesta de Directiva sobre responsabilidad. Manuel Ortiz Fernández. Revista de los Estudios de Derecho y Ciencia Política. IDP N.º 40 (marzo, 2024) I ISSN 1699-8154.

Sistemas de alto riesgo: no se presumirá el nexo cuando el demandado demuestre que el demandante podía acceder a pruebas y conocimientos especializados suficientes para probarlo.

Sistemas que no sean de alto riesgo: solo se aplicará la presunción de la causalidad cuando el órgano jurisdiccional nacional considere excesivamente difícil para el demandante demostrarlo.

Cuando el demandado desarrolle una actividad personal (no profesional): solo se recurrirá a la presunción cuando el demandado haya interferido sustancialmente en las condiciones de funcionamiento del sistema o cuando tuviese la obligación y estuviese en condiciones de determinar sus condiciones de funcionamiento y no lo haya hecho.

En definitiva, la tarea de regular la responsabilidad civil derivada del uso de sistemas de IA, acorde con los principios de la UE y con la protección de los usuarios -consumidores finales- de estos sistemas, frente a sus propios fallos, defectos y decisiones, es ardua y compleja y los desafíos que plantea son los propios de cualquier sistema de responsabilidad civil: (i) ¿Quién es responsable?; (ii) ¿Cómo se prueba la causalidad?; (iii) ¿Cuál es el alcance de la responsabilidad?

Por otro lado, determinar quién es responsable en cada caso (proveedor, desarrollador, usuario), en el que un sistema de IA genera un daño es complejo, porque estos sistemas son intrínsecamente complejos en su concepción (opacidad de los algoritmos y redes neuronales); son autónomos en sus decisiones (toma de decisiones independientes y aprendizaje continuo), e interactúan con factores externos (datos de entrada y entorno), y múltiples intervinientes involucrados (cadena de suministro).

Estos mismos factores son los que dificultan también la determinación de la causalidad de los daños producidos por los sistemas de IA y si la responsabilidad y correlativa indemnización o resarcimiento a satisfacer debe ser individual o compartida.

La propuesta de Reglamento de responsabilidad y la propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la IA son complementarias y comparten el objetivo garantizar que las personas que sufran daños a causa de los sistemas de IA puedan ser resarcidos y obtener una indemnización adecuada.

Muy probablemente la responsabilidad civil por daños derivados del uso de sistemas de IA y su regulación requerirán un trato diferenciado, y que probablemente afecte a los elementos que integran los sistemas de responsabilidad civil tal y como los conocemos.

6. Usos prácticos y beneficios del uso de la Inteligencia Artificial en las funciones del Compliance Officer

6.1. IA aplicada a la Prevención del Blanqueo de Capitales y Fraude

Cuando hablamos de los sistemas de prevención de prevención de blanqueo de capitales, fraude y financiación del terrorismo hacemos referencia a las medidas, procesos y políticas de identificación, prevención y mitigación del riesgo interno y externo al que están expuestas las empresas.

Los modelos de prevención van a ser más o menos eficientes y eficaces según los sistemas que utilicen para el depuramiento y tratamiento de datos y en función de la cantidad de procesos automatizados. Un modelo de Compliance con procesos manuales y nutrida de una base de datos de pobre calidad estará destinado al fracaso.

Los sistemas de IA bien aplicados sirven para automatizar y optimizar los procesos de tratamiento de datos y de ejecución de los programas de Compliance. Así por ejemplo, tienen la capacidad de optimizar los sistemas de monitorización transaccional -en prevención de blanqueo de capitales, financiamiento del terrorismo y fraude-, los de identificación y validación de personas -conoce a tu cliente-, los controles de la segunda línea de defensa, los realizados por la tercera línea de defensa, como cualquier otra área o proceso que forme parte del sistema de gestión de Compliance. Es por ello por lo que una tarea que una empresa cumple haciendo cientos de clicks por día, utilizando tres aplicaciones en simultáneo y una decena de ventanas de internet abiertas al mismo tiempo, un sistema de IA podría optimizarlo y hacerlo posible en un click.

Si bien la aplicación práctica de la IA puede beneficiar todas las áreas de Compliance, los beneficios a corto plazo se reconocerán principalmente por los equipos de identificación y conocimiento del cliente ("Know Your Counterparty" o "KYC") y los de monitorización transaccional, que suelen ser las áreas más operativas de los departamentos de Compliance y las que generan mayores fricciones con los clientes. Además de mejorar y optimizar los procesos, reducir los riesgos y sus márgenes de errores, servirán para reducir costes y aminorar la fricción con los clientes.

La prevención de blanqueo de capitales y fraude puede confiar en sistemas de IA basados en algoritmos basados en *Machine Learning* and *Deep Learning* .

Machine Learning o aprendizaje automático se basa en algoritmos que aprenden automáticamente de los datos mediante la observación de grandes cantidades de datos y representación estadística de procesos reales. Esto puede servir para inferir causa de eventos y comportamientos futuros, así como recomendar decisiones.

Por su parte, el Deep Learning o aprendizaje profundo es una técnica avanzada de machine learning, que sirve para resolver problemas muy complejos, como lo haría un humano, usando algoritmos que se conocen como *deep neural networks*.

6.2. IA aplicada en los procesos de "KYC"

El atractivo de los modelos de IA está en su capacidad de procesar gigantescos volúmenes de datos de diversas fuentes, procesarlos velozmente, y en su automatización.

En el campo de KYC, la IA va a permitir una mejor identificación de los clientes, de su riesgo, y va a permitir un nivel de adaptación a las necesidades del equipo y a las características específicas de cada cliente nunca visto. Algunas de sus aplicaciones prácticas en el ámbito de la PBC y Fraude son:

1) **Automatización de datos y de procesos**: los modelos de IA pueden procesar grandes volúmenes de datos en cuestión de segundos, siendo más eficientes y reduciendo el margen del error. Los tiempos de procesamiento y costes asociados se van a ver reducidos notablemente.

2) **Evaluación del riesgo**: la utilización de matrices de riesgo es obligatoria en el KYC. Sin embargo, dicha ponderación no siempre es la adecuada durante la relación comercial. Con un sistema de IA, la categorización del riesgo podría adaptarse a las circunstancias de cada cliente, ponderando el registro histórico de datos de toda la clientela, incluyendo la probabilidad de delitos o la veracidad de la información.

3) **Verificación de identidad y reconocimiento facial**: a través de la IA se mejora la detección facial y el reconocimiento de gestos o rasgos de las personas al momento de identificarlas. Esto ayuda en la automatización de procesos y detección de anomalías en la documentación presentada por el cliente para ejecutar la transacción.

4) **Textos**: el procesamiento de lenguaje natural ("NPL") ayuda en el análisis de contenidos no estructurados y el entendimiento de los textos aportados en el proceso KYC.

5) **Revisión del historial del cliente**: la IA ayuda a que la revisión pueda hacerse sin ceñirse únicamente al riesgo del cliente, sino a las inferencias que el modelo pueda llegar a sugerir, teniendo en cuenta los datos históricos por los que el modelo ha aprendido.

6) **Propósito de negocio**: la IA puede inferir qué tipo de uso haría el cliente del producto en cuestión, por lo que el riesgo y las medidas de mitigación se personalizan.

7) **Reducción de errores**: un modelo de IA correctamente entrenado reduce el riesgo de falsos positivos o erróneas evaluaciones de riesgo.

8) **Experiencia del cliente**: menos demoras y procesos más ágiles contribuyen a una relación más fluida con los clientes, y por ende, con las áreas comerciales. Por ejemplo, el uso de chatbots facilita una mejor comunicación durante el proceso de KYC.

9) **Identificación temprana del fraude**: la capacidad de reconocimiento de patrones de la IA permite mejorar la categorización de patrones fraudulentos y no fraudulentos.

10) **Monitorización**: la actividad ejecutada por la IA es registrada y monitorizada en todo momento.

11) **Screening**: el screening de sanciones internacionales y, en particular *Adverse Media*, proceso que suele tomar mucho tiempo, puede realizarse en segundos gracias a la IA.

6.3. IA aplicada en los procesos de monitorización transaccional

Los modelos de IA sirven para mejorar los sistemas de monitorización transaccional. La categorización, agrupamiento, identificación de patrones, inferencia y predicción de resultados, anomalías o posibles eventos son claves.

Sin embargo, estos sistemas necesitan mantenimiento y adaptación de las reglas aplicadas a los clientes de forma constante con el fin de evitar un error en el propio procedimiento de monitorización. El dinamismo es fundamental.

Algunos de los grandes beneficios que podrían traer a la monitorización transaccional para la prevención del blanqueo de capitales y del fraude son:

1) **Detección**: identificación de patrones de actividades fraudulentas, sea como víctima o victimario.

2) **Anomalías**: detección de anomalías en los comportamientos de los clientes.

3) **Re-calificación** del riesgo durante la relación continua del cliente: reasignar el riesgo del cliente en base al comportamiento esperado (inferido por la IA).

4) **Detección de ataques imprevistos o no conocidos**: los modelos no supervisados podrían detectar comportamientos inusuales y no conocidos, y auto generar reglas específicas para su tratamiento.

Hemos visto los beneficios de contar con programas de Compliance basados en IA, ahora bien, ¿cuáles son los desafíos a los que estas áreas se enfrentarán?

1) **Datos**: los modelos de IA dependen de la calidad de los datos utilizados para entrenarlos. Una base de datos organizada, limpia y completa es clave para su desarrollo.

2) **Coste**: el desarrollo de modelos de Inteligencia Artificial es costoso, requiere grandes cantidades de datos, y una infraestructura adaptable. Necesita de inversión en tecnología, educación y entrenamiento.

3) **Sesgos**: otro de los puntos más críticos de los modelos de IA son los sesgos presentes en los datos o en los entrenamientos, lo que puede llevar a resultados discriminatorios o groseramente incorrectos.

4) **Gobernanza**: es importante inculcar una cultura responsable a lo largo de la organización. Establecer una hoja de ruta, una estrategia, dotar de poderes y recursos a las personas encargadas de implementar los modelos y establecer controles regulares sobre los modelos de IA y evaluaciones sobre su performance.

6.4. IA aplicada al cumplimiento de deberes de diligencia debida de terceros

La debida diligencia es el proceso mediante el cual las empresas pueden identificar, prevenir, mitigar y explicar cómo abordan sus efectos adversos reales y potenciales (Guía para empresas multinacionales de la OCDE, capítulo II - Políticas generales, párr. 10). La debida diligencia suele estar incluida en los procesos de Compliance de las organizaciones comprendiendo todos los riesgos recogidos en la guía de debida diligencia de la OCDE para prácticas comerciales responsables.

La aplicación de este proceso se está imponiendo como práctica en muchas empresas por diversos factores:

1) Normativa aplicable en grupos multinacionales[46]
2) Riesgo reputacional
3) Procesos de fusiones y adquisiciones

Para valorar los riesgos de proveedores en el proceso de diligencia debida, existen soluciones de mercado que gestionan grandes bases de datos para ofrecer las siguientes funcionalidades:

46 Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (LPBCFT) DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre diligencia debida de las empresas en materia de sostenibilidad y por la que se modifica la Directiva (UE) 2019/1937 Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (en adelante, "RDLPBCFT") Foreign Corrupt Practices Act (FCPA) OCDE: Guía de la OCDE de debida diligencia para una conducta empresarial responsable 2018

1) Politically exposed persons (PEP) screening: Este proceso implica la identificación y el análisis de individuos que ocupan o han ocupado cargos políticos prominentes o funciones gubernamentales importantes, así como socios cercanos y familiares, con el fin de evaluar el riesgo de realizar negocios con ellos debido a posibles conexiones con corrupción, blanqueo de capitales u otros delitos financieros.
2) Listas de sanciones: realiza comprobaciones de datos contra las listas de individuos y entidades sancionados.
3) Diferentes tipos de alertas, entre las que se encuentra: blanqueo de capital y financiación del terrorismo; involucración en procesos de soborno y corrupción; involucración en procesos de delitos financieros.
4) Negative media: localizar noticias que puedan suponer indicios de implicación en delitos financieros.

Estas funcionalidades se pueden aplicar a diferentes individuos relacionados con la organización, entre los que se destacan: clientes, proveedores, socios empresariales, empleados, puestos directivos o consejeros.

Las anteriores funcionalidades para llevar a cabo el proceso de diligencia debida se basan en alertas automáticas que analizan las bases de datos que gestionan. La utilidad de la AI, especialmente los algoritmos de Machine Learning o Deep Learning, está en la gestión de grandes bases de datos para determinar las alertas automáticas sobre PEPs, riesgo de blanqueo, riesgo de soborno u otros delitos financieros. También pueden usarse en combinación con los modelos de propósito general o GeNAI para análisis de textos para determinación de negative media o detección de “fake” news.

Las alertas positivas deben gestionarse según la normativa aplicable y producirán efectos en el proceso afectado, ya sea la contratación de un cliente, un proveedor o una transacción. Por esta razón, es conveniente considerar no solo las normativas referentes a ALM y diligencia debida, sino también las de privacidad, así como los posibles conflictos entre ellas.

Las políticas de selección de proveedores establecen distintos niveles de riesgo en función de factores como, por ejemplo:

- Tipo proveedor.
- Tipo de servicio.
- Importe del servicio.

- Existencia de intermediarios o comisionistas.
- Vinculación entre el proveedor o sus directivos y la empresa.
- Pagos en divisas.

El nivel de riesgo determinará la aplicación de diligencia normal o reforzada, pero en ambos casos se utilizarán los sistemas de ALM para detección de alarmas de fraude y corrupción que deberán comprobarse con la documentación aportada por el proveedor en el proceso de selección, pero en el caso de la diligencia reforzada se ampliará el screening de personas a los directivos, consejo de administración.

Los *screenings* de las personas jurídicas requieren screening de las personas físicas al ser necesario identificar los titulares reales de las empresas y verificar los antecedentes de corrupción que puedan tener[47]. Para ello, se usan distintas fuentes que pueden ofrecer mayor o menor cobertura en cuanto a riesgos de privacidad se refiere.

En general, estas herramientas han surgido en países anglosajones, USA, donde las leyes anticorrupción y antisoborno son muy fuertes, pero no son tan exigentes en cuanto a privacidad. Esto supone un riesgo en el proceso de diligencia debida en Europa, donde podría afectar sobre los derechos y libertades de los individuos (RGPD). A todo esto, se suma el uso de IA donde se deben salvar los riesgos en los sesgos, veracidad de las fuentes de la información y uso ético de los datos.

Por ello es crucial revisar las políticas de privacidad de estas herramientas, para detectar si utilizan fuentes

47 Artículo 3 de la LPBCFT "1. Los sujetos obligados identificarán a cuantas personas físicas o jurídicas pretendan establecer relaciones de negocio o intervenir en cualesquiera operaciones." Artículo 4 LPBCFT "1. Los sujetos obligados identificarán al titular real y adoptarán medidas adecuadas a fin de comprobar su identidad con carácter previo al establecimiento de relaciones de negocio o a la ejecución de cualesquiera operaciones."

fiables como sanciones firmes de condenas en distintas jurisdicciones, o si también utilizan fuentes "públicas", normalmente vinculadas a negative media.

Las fuentes públicas como internet, tiene tres riesgos fundamentales:

- Validación de la fuente en sí misma y la noticia asociada, puede recoger información no suficientemente verificada.
- Principio de finalidad, aunque la fuente sea válida, la información no se generó para una finalidad posterior de lucha contra fraude, corrupción, soborno o blanqueo de capital.
- Gestión del derecho al olvido, si este derecho no es gestionado correctamente por la fuente, puede utilizarse información que debería haber sido eliminada o corregida.

El otro riesgo detectado en las herramientas AML con grandes bases de datos son las bases legitimadoras que utilizan para la gestión de los datos:

1) Obligación legal.
2) Interés público.
3) Interés legítimo.

En cuanto al tratamiento de datos personales por obligación legal que conlleven el cumplimiento de la diligencia debida, el artículo 32 bis de la LPBCFT remite al art. 8.1 de la LOPDGDD en el que se establece que:

Artículo 8. LOPDGDD Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.

"1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679."

Puede considerar que la legitimación del screening de proveedores en el cumplimiento de una obligación legal (Art. 6.1.c RGPD) siguiendo las indicaciones del artículo 32 bis de la LPBCFT y su referencia al artículo 8.1 de la LOPDGDD,

en la medida en que los tratamientos que se prevean realizar sean exclusivamente aquellos previstos en la LPBCFT respecto de los "clientes", aplicando el concepto de "relaciones de negocio". Por tanto, no se observa contradicción con el espíritu de la LPBCFT en tanto que esta interpretación se basa en el concepto de "relaciones de negocio" contemplado en la misma, justificándose un screening de proveedores exclusivamente legitimado en la base del cumplimiento de una obligación legal en relación con los tratamientos permitidos respecto de clientes.

En el resto de los tratamientos orientados al cumplimiento de obligaciones legales de normas extranjeras que no se prevean respecto de clientes en la LPBCFT, se deberá analizar mediante un juicio de ponderación la aplicabilidad del interés legítimo, ya que no existe una ley española o de EU que tenga ese ámbito no siendo directamente aplicables leyes como SAPIN II os la FCPA.

En cualquier caso, es preciso realizar un juicio de ponderación como el señalado en el considerando 47 RGPD para aquellos tratamientos legitimados según el interés legítimo.

En cuanto al uso del interés público, GDPR establece en el considerando 45 que una misión realizada en interés público debe basarse en el derecho de la unión o en el de los estados miembros. Por lo tanto, debemos encontrar una legislación europea o española con rango de ley para basar este tratamiento legitimado en interés público, sin embargo, ninguna normativa establece esta base legitimadora.

Por último, en cuanto al interés legítimo, es posible su uso en una relación empresarial, en el proceso precontractual, si se realiza un juicio de proporcionalidad, necesidad e idoneidad para determinar si los intereses del responsable permanecen sobre los de los titulares de la empresa que se pretende investigar.

6.5. IA aplicada en los procesos de creación de Sistemas de Gestión de Compliance

Los LLM (Large Language Modeles o Modelos de Lenguaje de Gran Escala) son sistemas de IA que analizan millones de textos para entender y aplicar patrones de lenguaje, gramática y contexto.

Un tipo de LLM es el ChatGPT, se trata de un asistente virtual, creado mediante aprendizaje automático con toda la información disponible en internet y que ha sido entrenado con reaprendizaje de refuerzo, para que mediante tecnología de procesamiento de lenguaje natural pueda comprender y responder a las preguntas y solicitudes de los usuarios en tiempo real.

A continuación, vamos a analizar un caso de clasificación de correos de entrada en buzón del Delegado de Protección de Datos.

Descripción del caso: el buzón DPO es el buzón de contacto para ejercicios de derechos de privacidad, así como para cuestiones relacionadas con la privacidad (políticas de privacidad, tratamientos, transferencias de datos, etc.).

Este buzón gestiona gran volumen de emails entrantes que hay que clasificar y tratar. Es importante:

1) Asignar urgencia y fecha límite de respuesta.
2) Clasificar las tipologías más frecuentes.
3) Limpiar el spam.
4) Resolver otros temas no frecuentes.

El caso de uso consiste en clasificar los mensajes entrantes y asignar una prioridad.

Para el desarrollo de este caso de uso se va a utilizar el ChatGPT de Open AI pero en una instancia privada para evitar problemas de fuga de información y confidencialidad de datos. El uso de este sistema se realizará en modo API.

Para asegurar el éxito del proyecto es fundamental aportar la información suficiente para la correcta identificación de la tipología. La asignación correcta de la tipología y la prioridad en función de la fecha de entrada en la compañía permitirá ganar eficiencia en las respuestas y cumplir con los plazos de respuesta al interesado.

La fase de entrenamiento es fundamental para que la clasificación sea correcta y el sistema puede reportar la productividad esperada. Para ello, se realizan pruebas con distintos emails para ver resultados e ir depurando errores.

Es fundamental el uso del *Promt* o input correcto para que la clasificación sea la adecuada. La arquitectura tecnológica consistirá en:

1) Conectar el buzón Outlook con la base de datos para realizar una copia del buzón de entrada de DPO.

2) Realizar una consulta síncrona de la base de datos a nuestro GPT cada vez que se reciba un nuevo email.

3) La salida del Promt de nuestro GPT será la tipología del email y prioridad.

Una vez clasificados las solicitudes deben atenderse gestionando los distintos aplicativos de negocio donde debe gestionarse la oposición, bloqueo, acceso, rectificación, etc.

Un paso posterior en esta automatización puede consistir en elaborar los modelos de respuesta según corresponda, pero esto supone tener conexión con los aplicativos de negocio para la gestión de datos de los interesados.

Riesgos apreciados en este caso de uso:

1) **Regulatorio**: la clasificación no sea la adecuada y no atendamos los derechos en plazo. Este riesgo se mitiga con la revisión por parte de los usuarios que gestionan el buzón de las clasificaciones realizadas por el LLM y corrigiendo los casos mal clasificados para que se vaya retroalimentando el sistema.

2) **Confidencialidad**: acceso a datos de clientes, a veces sensibles que pueden tener acceso externo si el ChatGPT es el modelo abierto.

Anexo - Relación de asociados de ASCOM que han participado en la elaboración del presente documento

Coordinador del grupo:

- Hurtado, Alonso

Coordinadores del documento:

- Castilla, Yolanda
- Hurtado, Alonso

Participantes (por orden alfabético):

- Carabias, Victoria
- Castilla, Yolanda
- García, Pilar
- Garzón, Fuencisla
- Hurtado, Alonso
- Langevin, Julián
- Llatas, Juan
- Silva, María
- Vidal, María

Asociación
Española
de Compliance