

LA IMPLEMENTACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LOS DEBERES DEL OFICIAL DE CUMPLIMIENTO

Xenia Carolina Madariaga¹

En un mundo corporativo, cada vez más complejo y dinámico, el oficial de cumplimiento desempeña un papel muy importante dentro de las líneas de defensa contra los riesgos empresariales que allí se presentan. Es así como, con el auge del estudio por la cultura empresarial y la evolución de las regulaciones, surge la necesidad de crear herramientas más avanzadas para detectar riesgos de manera oportuna y efectiva, y apalancar los deberes esenciales del oficial de cumplimiento. A lo largo de este artículo, se aborda cómo esta innovación revoluciona la detección temprana de riesgos en entornos empresariales cada vez más complejos y regulados.

Sumario

I. Introducción; II. *Compliance* y la importancia del rol del oficial de cumplimiento; III. Rol de la IA en la detección oportuna de riesgos a cargo del oficial de cumplimiento; IV. Toma de postura; V. Conclusiones; VI. Bibliografía.

I. Introducción

¹ Abogada, con énfasis en Derecho Privado de la Universidad del Rosario. Especialista en Derecho Penal y Ciencias Criminológicas de la Universidad Externado de Colombia.

En los últimos años ha habido un notable aumento en la implementación de tecnologías avanzadas, como la robótica y la inteligencia artificial (en adelante, IA), especialmente en el entorno empresarial² y en el sector comercial. Así las cosas, se puede decir que la adopción de la IA³ es una estrategia fundamental para elevar la productividad, desarrollar innovadores modelos de negocio y fortalecer la capacidad de tomar decisiones en un escenario digital en constante evolución.

En un estudio conducido por la Universidad EAFIT⁴ sobre el análisis del comportamiento de la adopción de IA en las organizaciones colombianas se reveló que más de 8500 empresas en el país han implementado la inteligencia artificial. El sector de la construcción lidera con el 63 %, seguido por el comercio (48 %), los servicios (42 %) y la industria manufacturera (38 %). Dentro de este estudio también se observó que el empleo de tecnologías de inteligencia artificial es más prominente en áreas como el *marketing* y las ventas. Este patrón bien podría estar vinculado a la coyuntura económica y social provocada por la pandemia. El estudio evidenció que hay un incremento en la utilización de *chatbots* basados en procesamiento de lenguaje natural para la atención al cliente. Estas herramientas permiten perfilar a los potenciales compradores a través de redes sociales, optimizar los precios y ofrecer propuestas de mercado personalizadas. En otras palabras, se están aplicando técnicas de aprendizaje automático para efectuar análisis de mercado, entre otras estrategias⁵.

En el contexto actual, aún se debate si el legislador en realidad debe crear marcos regulatorios que posibiliten la implementación de esta nueva tecnología⁶ en diversas áreas y sectores. Quizás una

2 Por ejemplo, en el sector legal, la firma PPU (Philippi Prietocarrizosa Ferrero DU & Uría) presentó hace pocos meses una nueva plataforma creada con inteligencia artificial llamada Quintus que apalanca el área de *Compliance* y facilita el proceso de auditoría a sus clientes. Otro ejemplo también es Amazon, que utiliza la IA en sus asistentes de voz a través del procesamiento de lenguaje natural (NPL) para comprender y responder preguntas de manera ágil y sencilla. Otro caso de éxito de implementación de la IA en el ámbito legal es la plataforma Ariel, que nace como un asistente legal virtual para buscar leyes actuales, jurisprudencia, entre otros. Esta plataforma fue creada en Colombia por las firmas MPA y PDA Abogados.

3 En este escrito se adoptará la definición de IA establecida por la OCDE (Organización para la Cooperación y el Desarrollo Económico): «Un campo de la informática dedicado a resolver problemas cognitivos comúnmente asociados con la inteligencia humana o seres inteligentes, entendidos como aquellos que pueden adaptarse a situaciones cambiantes. Su base es el desarrollo de sistemas informáticos, la disponibilidad de datos y algoritmos».

4 Lina María Vera Otálvaro, «Adopción de Tecnologías de Inteligencia Artificial: un estudio para las empresas en Colombia» (tesis de maestría, Universidad EAFIT, 2023), 4-12.

5 *Ibidem*.

6 Luis Alberto Peralta, «¿Es realmente necesaria una regulación de la inteligencia artificial?». *Revista Cinco Días*, 10 de abril del 2023, <https://cincodias.elpais.com/economia/2023-04-11/es-realmente-necesaria-una-regulacion-de-la-inteligencia-artificial.html>

de las áreas en la que es fundamental la adaptación, implementación y regulación de la inteligencia artificial es en el denominado *compliance* dentro del sector privado. La IA puede ayudar a las empresas a identificar y mitigar riesgos en áreas como seguridad cibernética, fraude financiero y gestión de riesgos empresariales de la mano con los oficiales de cumplimiento⁷. Esto es relevante sobre todo en un entorno empresarial cada vez más digitalizado y conectado.

Dicho lo anterior, es claro que la implementación de la IA en otros espacios también es trascendental. Sin embargo, para los fines de este escrito, se hará énfasis en los desafíos y ventajas de la adopción de la IA en el ámbito corporativo. Asimismo, se planteará si es procedente determinar hasta qué punto la responsabilidad penal del oficial de cumplimiento se ve modificada por la integración de la IA en sus funciones y cuáles son los límites de su deber de supervisión sobre el sistema de la IA.

II. Compliance y la importancia del rol del oficial de cumplimiento

Compliance se refiere «al conjunto de procesos y medidas que una organización implementa para asegurarse de que cumple con las leyes, regulaciones [internas y externas], estándares éticos»⁸ y códigos de conducta aplicables a su actividad. Esto implica monitorear y garantizar que las operaciones de la organización se ajusten a todas las normativas relevantes para evitar así posibles riesgos legales, financieros o reputacionales⁹.

Ahora bien, en palabras de Bacigalupo¹⁰, aunque el *compliance* es el término general para referirnos a la implementación de «cultura, principios o valores» dentro del entorno empresarial, se deben extraer al menos dos consecuencias de estos términos:

7 Silvana Bacigalupo, «Compliance». *Eunomía, Revista en Cultura de la Legalidad*, n.º 21 (2021): 260-276. <https://doi.org/10.20318/eunomia.2021.6348>.

⁸ «Beneficios del *compliance* para tu empresa», *Aicad Business School*, 21 de marzo de 2024, <https://www.aicad.es/beneficios-del-compliance-para-tu-empresa>

⁹ Juan Francisco Pozo Torres, «Compliance y posición de garante: Imputación de hechos delictivos al compliance officer». *FORO. Revista de Ciencias Jurídicas y Sociales Nueva Época* 23, n.º 1 (2020): 140, <https://go.gale.com/ps/i.do?id=GALE%7CA667619781&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=16985583&p=IFME&sw=w&userGroupName=anon%7E9c8e9bb0&aty=open-web-entry>

¹⁰ Bacigalupo. «Compliance», 260- 276.

- a) La adopción del *compliance* trae como exigencia la revisión y el cumplimiento de diversas regulaciones normativas que rigen la actividad empresarial.
- b) La empresa podrá adoptar cualquier norma de *soft law*¹¹ que considere pertinente para determinar su valor de actuación.

Es así como nace, del *soft law*, el término *compliance officer* u **oficial de cumplimiento** (en adelante, OC). Este concepto se incorporó por primera vez a la doctrina en la redacción de la sección 8B2.1 de las *United States Sentencing Guidelines* en 1991⁽¹²⁾, junto con la definición de «High-level personnel of the organization», que abarca los deberes y funciones de los directores y ejecutivos.

Cabe preguntarnos entonces por qué es relevante el rol del oficial de cumplimiento dentro de las actividades empresariales. Pues bien, con la aprobación y adopción de la *Sarbanes-Oxley Act* en Estados Unidos, en el 2002, se propuso la designación de un alto miembro ejecutivo para la supervisión de la aplicación de los programas de cumplimiento. Como consecuencia, los términos *compliance officer* y *corporate compliance* se volvieron comúnmente utilizados en materia penal para hablar sobre las limitaciones tanto de la responsabilidad penal de las personas jurídicas¹³ como de la responsabilidad de estos altos funcionarios.

Un ejemplo claro de la importancia del rol de un *compliance officer* es el caso de una empresa de tecnología que establece una serie de políticas de cumplimiento para proteger la privacidad de los datos de sus usuarios. El oficial de cumplimiento es quien se encarga de garantizar que la empresa cumpla con las leyes de protección de datos, como el *Reglamento General de Protección de Datos* (GDPR) en Europa. Esto conlleva implementar medidas de seguridad de la información, obtener el consentimiento adecuado de los usuarios para el manejo de sus datos y responder de manera oportuna a las solicitudes de acceso o eliminación de datos. Aquí, el OC juega un papel fundamental

11 Son normas o principios que no tienen fuerza legal vinculante, pero que aun así influyen en la conducta de los actores en un determinado ámbito. Estas normas pueden incluir declaraciones de principios, códigos de conducta, directrices, recomendaciones u otros instrumentos similares.

12 Norberto J. De la Mata Barrera, «El órgano de control permanente de la persona jurídica (oficial de cumplimiento) en el marco de la responsabilidad penal corporativa». *Revista Penal México* 11, n.º 21 (2022): 3-14.

13 *Ibidem*.

en la protección de la reputación y la integridad de la empresa, así como en la construcción de la confianza del público en su compromiso con la privacidad de los datos.

Por otro lado, en Colombia, actualmente la figura del OC no se menciona en el Código Penal. Sí lo hace, por ejemplo, el Código Penal de España bajo la tesis de la omisión. De igual forma, en Alemania tienen una figura estandarizada sobre el OC a través del estándar IDW AssS 980 del Instituto Alemán de Auditores, en conjunto con normas internacionales como la ISO 19600 y 37001. Lo anterior implica que el papel del oficial de cumplimiento puede tener distintas funciones según las políticas públicas de los diferentes ordenamientos jurídicos donde se encuentre una empresa y sus necesidades respecto a la estrategia de prevención de riesgos.

En Alemania, la responsabilidad penal del OC se determinó por primera vez en 2009 con una sentencia del Tribunal Supremo Federal¹⁴ en un *obiter dictum*¹⁵ que definió el deber jurídico personal de un *compliance officer* como el acto de **prevenir activamente** la comisión de delitos por parte de los empleados de la empresa. Con lo anterior, la empresa traslada sus tareas de gestión y control, y, por lo tanto, parte de su autoridad al responsable, poniendo de manera prevalente sobre la mesa el estudio de los delitos por omisión.

Si tomamos como punto de partida los precedentes alemanes respecto a las funciones del *compliance officer* tendríamos que algunas de sus actividades esenciales son, entre otras:

- a) Establecer una organización interna que asegure el cumplimiento de las normativas legales;
- b) integrar de forma sistemática esta estructura organizativa en los procedimientos operativos de la empresa;
- c) implementar un sistema de control que supervise el cumplimiento de las normas y castigue las violaciones según sea necesario;

14 Lutz Carlos Moratinos Meissner, «La responsabilidad penal y civil del Compliance Officer en Alemania». *Revista Asociación Española de Abogados Especializados en Responsabilidad Civil y Seguros*, n.º 82 (2022): 149-159.

15 «*Obiter dictum* es una expresión en latín que literalmente en español significa 'dicho de paso'. Hace referencia a aquellos argumentos expuestos en la parte considerativa de una sentencia o resolución judicial que corroboran la decisión principal, pero que carecen de poder vinculante, pues su naturaleza es meramente complementaria». Definición tomada de: [https://dbpedia.org/page/Obiter dictum](https://dbpedia.org/page/Obiter_dictum).

d) proporcionar un sistema de denuncias anónimas¹⁶.

Lo anterior demuestra que el OC ejerce un rol de análisis privado, en una entidad privada, y que este rol se basa en cumplir con las normas y políticas de la empresa, no en dictar o juzgar cuestiones morales absolutas. Más bien, hay que entender este cargo como el de un experto que está al servicio de los intereses y los objetivos de una empresa.

Sobre el debate de la regulación de la IA

El debate sobre la regulación de la inteligencia artificial en el mundo es complejo y abarca varios conceptos y aspectos. Por ejemplo, para Kurzweil, la IA es «El arte de desarrollar máquinas con capacidad para realizar funciones que cuando son realizadas por personas requieren de inteligencia¹⁷». En cambio, Bellman se refiere a la IA como «La automatización de actividades que vinculamos con procesos de pensamiento humano, actividades como la toma de decisión, resolución de problemas, aprendizaje...»¹⁸.

Sea cual sea la posición que asuma una persona que estudie la IA desde una perspectiva legal debe tener en cuenta que al final del día esta tecnología se traduce también como un conjunto de atributos que aportan tanto económica como socialmente al mundo en el que vivimos hoy. En la actualidad, al menos treinta y un países han adoptado leyes que regulan la inteligencia artificial. Estados Unidos encabeza la lista con veintidós leyes dirigidas al asunto¹⁹.

Un estudio de la Universidad de Stanford²⁰ demuestra que la tendencia mundial hacia la legislación sobre la IA es innegable. Expone, igualmente, que la mayoría de los países de occidente optan por una regulación de carácter convencional enfocada a la protección de los datos de identidad de las

16 UIAF. «Preguntas frecuentes para los grupos de valor UIAF». *Unidad de Información y Análisis Financiero*. 2022. 34-39. https://www.uiaf.gov.co/sites/default/files/2022-07/documentos/archivos-anexos/Documento_Preguntas_frecuentes.pdf

17 «Artificial Intelligence Index Report 2024». *Stanford University for Human-Centered Artificial Intelligence*, p.2.

https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf

18 *Ibidem*, 2.

19 Peralta, «¿Es realmente necesaria una...».

20 «Artificial Intelligence Index Report 2024». *Stanford University for Human-Centered Artificial Intelligence*. https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf

personas (biometría y reconocimiento de voz). También se toma como prioridad el impacto de la IA en el medio ambiente. En Europa existe una tendencia hacia la regulación de la inteligencia artificial de forma flexible²¹ y complementaria, donde se hace un análisis basado en cuatro niveles de riesgos: riesgo inaceptable, riesgo limitado, riesgo alto y riesgo mínimo.

En este sentido, y con el fin de tener concesiones que abarquen diversos sistemas legales, el 21 de marzo del 2024 la Asamblea General de la ONU adoptó una resolución histórica²² sobre la IA, decisión que fue liderada por Estados Unidos. Este pronunciamiento se dividió en cuatro ejes de interés. Lo más destacado allí fue la exhortación de la Asamblea a todos los Estados, al sector privado y a la sociedad civil en general a garantizar que «Los mismos derechos que tienen las personas fuera de línea deben protegerse también en línea, incluso durante todo el ciclo de vida de los sistemas de inteligencia artificial». Esto implica un margen amplio de protección hacia los datos personales, casi con un tratamiento que contempla tanto el análisis previo como el posterior de la información de cada individuo.

Actualmente, Colombia cuenta con siete proyectos de ley que nos pueden dar línea de cómo sería el futuro de la implementación y utilización de la IA en el país. Cabe resaltar que lo difícil no es implementar o sancionar una ley *per se* en esta materia. El problema en realidad es que los legisladores se enfrentan a la tarea compleja de definir el concepto de la IA que se va a incorporar al ordenamiento jurídico para así determinar el ámbito de aplicación y quiénes estarán obligados al cumplimiento de la regulación que se expida. En el camino, definir la IA cada día se vuelve más complicado, porque existe una rápida evolución de esta tecnología y su carácter técnico.

Desafíos actuales en la detección de riesgos

El oficial de cumplimiento no solo enfrenta riesgos respecto a la prevención de lavado de activos y corrupción. La globalización y la digitalización de casi todas las actividades diarias que realizamos exponen a las empresas a múltiples desafíos que las obligan a estar a la vanguardia ante las nuevas

²¹ *Ibidem*.

²² «La Asamblea General adopta una resolución histórica sobre la IA». Noticias ONU, 21 de marzo de 2024, <https://news.un.org/es/story/2024/03/1528511>

tendencias y técnicas de los delincuentes para cometer todo tipo de delitos. Un reciente artículo de la BBC²³ indicó que el uso de la IA para cometer delitos está teniendo un crecimiento exponencial, desde clonaciones de voces²⁴ hasta videollamadas en tiempo real donde se suplanta la imagen, movimiento y gestos de una persona. Todos estos son escenarios aterradores para cualquiera que se lo pueda imaginar.

Un ejemplo relevante de la clonación de voces (*deepfake*) es el programa de Microsoft llamado *Valle-E*, cuya «red neuronal ha sido entrenada con más de 60 000 horas de audio en inglés de 7000 personas diferentes»²⁵. Esto le permite clonar la voz de cualquier persona con solo tres segundos de exposición del habla. Sin embargo, en general estos programas no nacen con un fin delictivo, sino con fines sociales y productivos, como en el caso de las productoras de video y animación.

Otro gran reto para quienes presiden estas actividades de prevención y control es el volumen o magnitud de datos, procesos o información dentro de las organizaciones, lo que muchas veces dificulta la identificación de patrones y de señales de alerta que podrían indicar riesgos potenciales. A lo anterior, se le suma que, en temas de cumplimiento normativo, las regulaciones cambian constantemente. Esto implica un esfuerzo financiero e intelectual para que el oficial de cumplimiento adapte los procedimientos de detección de riesgos y fraudes que sean pertinentes. Así mismo, hay que mencionar que los costos de prevención e implementación de programas de cumplimiento o la contratación de un oficial de cumplimiento, no suelen ser económicos²⁶. Ahora bien, es claro que las empresas que han invertido en digitalización y automatización de sistemas de gestión afrontan con mayor éxito las nuevas exigencias de un mundo cada vez más expuesto a la delincuencia.

IA y determinación de la responsabilidad penal del oficial de cumplimiento

23 Oliver Buckley, «Inteligencia Artificial: el cada vez más frecuente uso de voces familiares clonadas para estafas telefónicas (y como protegerse)». *BBC News*, 14 de julio de 2023, <https://www.bbc.com/mundo/articles/cz9q41r80n4o>

24 Como en el conocido caso de Bad Bunny contra Tik Tok por «potenciar» su canción *FlowGPT*.

25 Juan Ignacio Rouyet, «El peligro real de los deepfakes de clonación de voz y como detectarlos». *The Conversation*, 27 de noviembre de 2023, <https://theconversation.com/el-peligro-real-de-los-deepfakes-de-clonacion-de-voz-y-como-detectarlos-215012>

26 Diego Hernán Goldman, «Bases para el análisis económico de los sistemas de compliance penal». *Ius et Veritas*, n.º 57 (2018): 14-28. <https://doi.org/10.18800/iusetveritas.201802.001>

Quizás el desafío más grande que se evidencia ante la implementación de la IA en los deberes del oficial de cumplimiento es la identificación legal de su responsabilidad penal sobre las funciones de detección oportuna de riesgos. A medida que la IA se integra en las tareas de supervisión y cumplimiento normativo surge el interrogante sobre si el oficial sigue siendo por completo responsable de las decisiones tomadas por el sistema automatizado que se implemente en una empresa. Esto plantea un dilema en términos de supervisión y control, ya que la capacidad de comprensión y supervisión del oficial sobre el funcionamiento interno del algoritmo puede ser limitada. Si partimos de la base de que los principios rectores que guían la labor del *compliance officer* son los de independencia, neutralidad, autonomía e integridad²⁷, deberíamos entonces hablar sobre la delegación de competencias en los programas de cumplimiento, inclusive cuando sus actividades también dependan de lenguajes de programación, como es el caso de la inteligencia artificial.

El debate actual gira en torno a que, hoy en día, se habla de responsabilidad penal del oficial de cumplimiento cuando deja de realizar alguna de sus actividades esenciales en razón de su rol (comisión por omisión). Sin embargo, otro escenario podría surgir si, por ejemplo, al implementar un *prompt*²⁸ para ejecutar una orden que evalúe con precisión el perfil crediticio de una persona para conceder un crédito, este no se ejecuta correctamente. Esto podría llevar a una identificación errónea en la que la persona sea confundida con un delincuente buscado por financiamiento al terrorismo. Tal situación abre un espacio donde se trae a colación el análisis sobre la imputabilidad, la atribución de responsabilidad en caso de errores o decisiones incorrectas y hasta la evaluación del riesgo permitido.

III. Rol de la IA en la detección oportuna de riesgos a cargo del oficial de cumplimiento

27 Alejandro Turienzo Fernández, «La responsabilidad penal del *compliance officer*» (tesis de doctorado, Universitat de Barcelona, 2020), https://diposit.ub.edu/dspace/bitstream/2445/173983/1/ATF_TESIS.pdf.

28 Un *prompt* es una instrucción o estímulo utilizado en el contexto de la programación, la inteligencia artificial y el aprendizaje automático. Es una breve frase, pregunta o descripción que se utiliza para indicarle a un sistema qué tipo de salida se espera o qué acción debe realizar.

Como se mencionó anteriormente, algunas de las funciones del oficial de cumplimiento son la identificación de las situaciones que generen un riesgo para la empresa y el velar por el efectivo, eficiente y oportuno funcionamiento del sistema. En ese sentido, la IA debe ser aprovechada para optimizar estos procesos de detección de riesgo oportuno.

Dicho esto, un subcampo de la inteligencia artificial que crece de forma exponencial es el aprendizaje automático, que involucra algoritmos de autoaprendizaje que derivan el conocimiento a partir de datos para crear predicciones. Es lo que se conoce como *machine learning*²⁹. Por ejemplo, en el 2020 se publicó³⁰ un estudio sobre un modelo de *machine learning* aplicado para la predicción del hurto en Colombia. Este estudio propuso un modelo basado en un algoritmo³¹ de aprendizaje utilizado para hacer tareas de clasificación y regresión de datos. Así, se emplearon datos de la Fiscalía General de la Nación para el análisis de 2.662.402 denuncias y así determinar cuáles fueron los delitos más cometidos en Colombia desde el año 1960 hasta el 2019. El resultado arrojó el hurto como delito preponderante.

Todo lo expuesto nos permite ver cómo la IA puede optimizar la toma de decisiones de un OC respecto a la implementación de un programa normativo en particular, según las necesidades de la empresa o la ubicación territorial de esta. Un caso ilustrativo es el de un banco, donde a través del *machine learning* se pueden mejorar los estándares de seguridad aplicados por el OC tanto dentro como fuera de la organización. Esto se logra con un análisis de datos conductual de los colaboradores o de las tendencias del mercado sobre un producto financiero en particular.

29 «El *machine learning*, o aprendizaje automático, es un campo científico y, más particularmente, una subcategoría de inteligencia artificial. Consiste en dejar que los algoritmos descubran *patterns*, es decir, patrones recurrentes, en conjuntos de datos. Esos datos pueden ser números, palabras, imágenes, estadísticas, etc. Todo lo que se pueda almacenar digitalmente puede servir como dato para el *machine learning*. Al detectar patrones en esos datos, los algoritmos aprenden y mejoran su rendimiento en la ejecución de una tarea específica». Tomado de: «Machine Learning: definición, funcionamiento, usos». Data Scientist. 13 de diciembre de 2021, <https://datascientest.com/es/machine-learning-definicion-funcionamiento-usos>.

30 Hugo Ordoñez *et al.*, «Modelo de *machine learning* para la predicción de las tendencias de hurto en Colombia». *Revista Ibérica de Sistemas e Tecnologías de Informação*, n.º E29 (2020): 494–506. <https://www.proquest.com/docview/2394537974?sourcetype=Scholarly%20Journals>

31 Los algoritmos pueden encontrarse en diversas áreas como las matemáticas, la informática, la ciencia de datos, la ingeniería y muchas otras disciplinas. Pueden ser simples o complejos, dependiendo de la naturaleza del problema que se esté abordando. En informática, los algoritmos son fundamentales para el desarrollo de programas y sistemas, ya que permiten resolver problemas de manera eficiente y sistemática. Se utilizan para realizar operaciones como ordenar datos, buscar información, calcular rutas óptimas, entre otras tareas.

Adicionalmente, lo que podemos concluir del análisis anterior es que la aplicación de la IA para la automatización, predicción y toma de decisiones de un OC en contextos específicos evita que los sesgos cognitivos de las personas afecten los procesos de las empresas. Esto se debe a que la interacción del individuo con dinámicas preestablecidas puede alterar su juicio y condicionar su actuar³², y la IA podría mitigar estos efectos. Así, con la correcta aplicación de algoritmos y el ingenio de un buen programador para crear un programa predictivo podemos detallar o acercarnos a un pronóstico certero respecto de un comportamiento que represente una posible amenaza y, a partir de ello, elaborar una matriz de riesgos³³.

Otro de los beneficios del *machine learning* para la prevención del fraude y la detección oportuna de riesgos es que desde la línea de defensa corporativa se obtiene la habilidad de parcializar y procesar considerables cantidades de información. Esto significa reducción en el tiempo de revisión manual, mejoría de predicciones de grandes conjuntos de información, soluciones económicas y efectivas, y la principal, detección más rápida y eficiente de escenarios de pérdida o daño.

Es importante aclarar que, a pesar de lo ya mencionado, las funciones del oficial de cumplimiento en las actividades de detección oportuna de riesgos no pueden remplazarse por la implantación de la IA. Aunque es claro que el racionamiento humano se debe apalancar en las nuevas tecnologías para poder hacer un mejor trabajo.

IV. Toma de postura

En primer lugar, la IA puede ser una herramienta muy eficaz para la optimización de múltiples actividades propias de un OC. Sin embargo, con la implementación de modelos de tecnología predictivos se crea una preocupación en temas de desplazamiento laboral, ya que muchas empresas propenden a economizar recursos humanos con la implantación de nuevas tecnologías.

32 Andrés Felipe Díaz Arana, «Sesgos cognitivos y dinámicas empresariales: el lado “subjetivo” de los programas de cumplimiento» *Diálogos Punitivos*, 4 de octubre de 2018, <https://dialogospunitivos.com/sesgos-cognitivos-y-dinamicas-empresariales-el-lado-subjetivo-de-los-programas-de-cumplimiento/>

33 Juan Eduardo Rosales Álvarez, «Construyendo un puente ético: inteligencia artificial y cumplimiento normativo». *Diálogos Punitivos*, febrero 21 de 2024, <https://dialogospunitivos.com/construyendo-puente-etico-inteligencia-artificial-cumplimiento-normativo/>

Así mismo, encontramos algunos dilemas éticos y legales, pues entra en debate la asignación de responsabilidad y obligaciones donde intervienen sistemas inteligentes. Por ejemplo, nos podríamos acercar a un problema respecto a la prohibición de regreso si pensamos sobre un OC que toma una decisión relevante con base en un análisis erróneo de la IA. Esta persona podría tener responsabilidad, pero también el dueño intelectual de la IA que se emplee³⁴. Por esto, se hace un llamado a los desarrolladores de sistemas inteligentes, puesto que ellos tienen la responsabilidad de cumplir con estándares internacionales que aseguren la transparencia y la confiabilidad.

Además, es esencial destacar que es adecuado que el OC solo asuma responsabilidad por aquello que en realidad pueda gestionar. Su ámbito de actuación se limita al cumplimiento normativo dentro de una empresa, como su nombre lo indica. No obstante, pueden surgir algunas excepciones cuando se detectan comportamientos fraudulentos o negligentes que amenacen indiscriminadamente los intereses de la empresa.

La cultura organizacional juega un papel crucial al establecer un ambiente de transparencia, responsabilidad y compromiso con el cumplimiento normativo. La IA puede ser utilizada para fortalecer esta cultura al proporcionar herramientas de monitoreo y evaluación que promuevan la ética y la conformidad en todos los niveles de la organización.

Así las cosas, la combinación efectiva de la inteligencia artificial y la cultura organizacional de una empresa puede ser fundamental para fortalecer los deberes de detección temprana de riesgos del oficial de cumplimiento. En primer lugar, la implementación de sistemas de IA puede potenciar la capacidad del oficial de cumplimiento para «analizar grandes volúmenes de datos de manera rápida y precisa [e identificar] patrones, anomalías y tendencias»³⁵ que podrían indicar posibles riesgos. Estos sistemas pueden adaptarse a la cultura organizacional mediante la personalización de

34 En marzo de 2024 se divulgó un informe elaborado por la UNESCO que revela inquietantes patrones en las herramientas de procesamiento del lenguaje natural utilizadas por las plataformas de inteligencia artificial generativa. Estas herramientas están propensas a generar estereotipos de género y raza, así como contenido negativo relacionado con la comunidad LGBTQ+. <https://news.un.org/es/story/2024/03/1528182>

35 Alejandro Reyes, «Estrategias de IA aplicada a la auditoría informática», *Technology Rain Journal* 2, n.o 2 (2023), <https://doi.org/10.55204/trj.v2i2.e18>.

algoritmos y procesos para reflejar los valores y las prioridades específicas de la empresa, lo que garantiza una integración armoniosa con las prácticas y políticas existentes.

Al mismo tiempo, es primordial que la empresa fomente una cultura que valore la innovación y el aprendizaje continuo. Esto permitirá al OC y al equipo adoptar de forma proactiva nuevas tecnologías y técnicas, como el mencionado *machine learning*, el análisis de datos, la minería de datos y el Python, para adaptarse a los cambios en el panorama de riesgos. En última instancia, la colaboración entre la IA y la cultura organizacional puede crear un entorno más resiliente y ágil para el OC que le facilite la detección temprana y la mitigación efectiva de riesgos para el beneficio a largo plazo de la empresa y sus partes interesadas.

V. Conclusiones

La IA se dedica a desarrollar programas y máquinas con capacidad para llevar a cabo tareas que se asemejen a las realizadas por los seres humanos, como aprender y razonar de manera lógica. Por otra parte, desempeña un papel esencial en el ámbito legal, ya que, como vimos en algunos ejemplos, utiliza el lenguaje lógico para optimizar información. Del mismo modo, en algunos sistemas judiciales se recurre a estos programas porque tienen la capacidad de procesar datos legales y prever decisiones válidas y legalmente justificadas, similares a las que tomaría un jurista³⁶ que siguiera los parámetros y reglas establecidos por la ley.

Respecto a los oficiales de cumplimiento y a los programas normativos se dejó claro que la IA facilita análisis avanzados que complementan la labor de estos funcionarios. Esto les permite aprovechar información en tiempo real sobre los riesgos detectados por los sistemas basados en IA de la empresa, dado que el objetivo es tomar decisiones más acertadas para mejorar la eficacia y transparencia. Así, se evitan posibles sanciones que puedan afectar la reputación de la empresa por acciones perjudiciales.

36 «Juez colombiano usa inteligencia artificial de ChatGPT en un caso». France 24. 2 de febrero de 2023. <https://www.france24.com/es/minuto-a-minuto/20230202-juez-colombiano-usa-inteligencia-artificial-de-chatgpt-en-un-caso>

La integración de IA representa un cambio significativo en la forma en la que se abordan los desafíos legales y de cumplimiento normativo. La capacidad de la IA para analizar grandes cantidades de datos de manera rápida y precisa permite a los oficiales de cumplimiento tomar decisiones más informadas y eficientes. Ahora, para garantizar su uso ético y responsable es sustancial contar con una regulación adecuada que fije normas claras sobre la recopilación, el procesamiento y el uso de datos por parte de los sistemas de inteligencia artificial.

En este contexto, el papel del OC cobra una importancia aún mayor, ya que se puede convertir en el garante de que las actividades de inteligencia artificial en la empresa se lleven a cabo de acuerdo con los estándares legales y éticos establecidos. Su labor es fundamental para asegurar la transparencia, la legalidad y la integridad en el uso de la inteligencia artificial dentro de la línea de defensa corporativa. Todo ello refuerza la confianza y la credibilidad en el sistema legal y en las instituciones que respaldan al sector empresarial.

VI. Bibliografía

«Artificial Intelligence Index Report 2024». *Stanford University for Human–Centered Artificial Intelligence*. https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf, 501 pp.

Bacigalupo, Silvana. «Compliance». *Eunomía, Revista en Cultura de la Legalidad*, n.º 21 (2021): 260-276. <https://doi.org/10.20318/eunomia.2021.6348>.

«Beneficios del compliance para tu empresa». Aicad Business School, 21 de marzo de 2024, <https://www.aicad.es/beneficios-del-compliance-para-tu-empresa>.

Buckley, Oliver. «Inteligencia Artificial: el cada vez más frecuente uso de voces familiares clonadas para estafas telefónicas (y como protegerse)». *BBC News*, 14 de julio de 2023, <https://www.bbc.com/mundo/articles/cz9q41r80n4o>

«Cómo mitigar el riesgo reputacional corporativo frente a la IA maliciosa». *IT Digital Security*, 16 de octubre de 2023, <https://www.itdigitalsecurity.es/actualidad/2023/10/como-mitigar-el-riesgo-reputacional-corporativo-frente-a-la-ia-maliciosa>.

- De la Mata Barranco, Norberto J. «El órgano de control permanente de la persona jurídica (oficial de cumplimiento) en el marco de la responsabilidad penal corporativa». *Revista Penal México* 11, n.º 21 (2022): 3-14.
- Díaz Arana, Andrés Felipe. «Sesgos cognitivos y dinámicas empresariales: el lado “subjetivo” de los programas de cumplimiento» *Diálogos Punitivos*, 4 de octubre de 2018, <https://dialogospunitivos.com/sesgos-cognitivos-y-dinamicas-empresariales-el-lado-subjetivo-de-los-programas-de-cumplimiento/>
- Goldman, Diego Hernán. «Bases para el análisis económico de los sistemas de *compliance* penal». *Ius et Veritas*, n.º 57 (2018): 14-28. <https://doi.org/10.18800/iusetveritas.201802.001>
- «Juez colombiano usa inteligencia artificial de ChatGPT en un caso». *France 24*. 2 de febrero de 2023. <https://www.france24.com/es/minuto-a-minuto/20230202-juez-colombiano-usa-inteligencia-artificial-de-chatgpt-en-un-caso>
- «La Asamblea General adopta una resolución histórica sobre la IA». Noticias ONU, 21 de marzo de 2024, <https://news.un.org/es/story/2024/03/1528511>
- Moratinos Meissner, Lutz Carlos. «La responsabilidad penal y civil del Compliance Officer en Alemania». *Revista Asociación Española de Abogados Especializados en Responsabilidad Civil y Seguros*, n.º 82 (2022): 149-159.
- Mirjalili, Vahid y Sebastian Raschka. *Python Machine Learning*. España: Marcombo, 2019.
- Ordoñez, Hugo; Carlos Cobos y Víctor Bucheli. «Modelo de *machine learning* para la predicción de las tendencias de hurto en Colombia». *Revista Ibérica de Sistemas e Tecnologías de Informação*, n.º E29 (2020): 494-506. <https://www.proquest.com/docview/2394537974?sourcetype=Scholarly%20Journals>
- Peralta, Luis Alberto. «¿Es realmente necesaria una regulación de la inteligencia artificial?». *Revista Cinco Días*, 10 de abril del 2023, <https://cincodias.elpais.com/economia/2023-04-11/es-realmente-necesaria-una-regulacion-de-la-inteligencia-artificial.html>
- Pozo Torres, Juan Francisco. «Compliance y posición de garante: Imputación de hechos delictivos al compliance officer». *FORO. Revista de Ciencias Jurídicas y Sociales Nueva Época* 23, n.º 1 (2020): 4-15, <https://go.gale.com/ps/i.do?id=GALE%7CA667619781&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=16985583&p=IFME&sw=w&userGroupName=anon%7E9c8e9bb0&aty=open-web-entry>
- Reyes, Alejandro. «Estrategias de IA aplicada a la auditoria informática», *Technology Rain Journal* 2, n.º 2 (2023), <https://doi.org/10.55204/trj.v2i2.e18>.

Rosales Álvarez, Juan Eduardo. «Construyendo un puente ético: inteligencia artificial y cumplimiento normativo». *Diálogos Punitivos*, febrero 21 de 2024, <https://dialogospunitivos.com/construyendo-puente-etico-inteligencia-artificial-cumplimiento-normativo/>

Rouyet, Juan Ignacio. «El peligro real de los deepfakes de clonación de voz y como detectarlos». *The Conversation*. 27 de noviembre de 2023, <https://theconversation.com/el-peligro-real-de-los-deepfakes-de-clonacion-de-voz-y-como-detectarlos-215012>

Russell, Stuart J. y Peter Norvig. *Artificial Intelligence: A Modern Approach. Third edition, Global edition. Prentice Hall Series in Artificial Intelligence*. Boston: Prentice Hall, 2016. UIAF. «Preguntas frecuentes para los grupos de valor UIAF». *Unidad de Información y Análisis Financiero*. 2022. 34-39. https://www.uiaf.gov.co/sites/default/files/2022-07/documentos/archivos-anexos/Documento_Preguntas_frecuentes.pdf

Vera Otálvaro, Lina María. «Adopción de Tecnologías de Inteligencia Artificial: un estudio para las empresas en Colombia» (tesis de maestría, Universidad EAFIT, 2023), 4-12.