



La lucha anticorrupción desde el nuevo paradigma tecnológico

DENISSE RODRÍGUEZ-OLIVARI

La inteligencia artificial se ha convertido en una de las herramientas más novedosas en la lucha contra la corrupción. Esta nueva tecnología cuenta con innumerables bondades sin precedentes para identificar irregularidades, automatizar las comprobaciones de cumplimiento y mejorar la transparencia en las organizaciones públicas y privadas. Analizamos las oportunidades y retos de la aplicación de las tecnologías basadas en IA para detectar, prevenir y combatir la corrupción alrededor del mundo, con énfasis en América Latina.

Introducción

La lucha contra la corrupción continúa siendo una de las problemáticas más prevalentes en América Latina. De acuerdo al índice de control de corrupción elaborado por Americas Society/Council of the Americas (AS/COA) y Control Risks, un 70% de los expertos consideran que la corrupción continúa siendo un desafío enorme en sus países, solo superado por la inseguridad ciudadana y la situación económica pospandemia. Asimismo, según el índice de percepción de la corrupción de la ONG Transparencia Internacional, la mayoría de los países de la región empeoraron o se estancaron en materia anticorrupción. De hecho, solo Guyana y República Dominicana registran avances significativos y Venezuela cae a un mínimo histórico en el *ranking* global.

En medio de este escenario desolador, el uso de la inteligencia artificial (IA) ofrece soluciones novedosas a este problema tan complejo. Por un lado, están el análisis de datos y la detección de anomalías, la predicción de riesgos de corrupción y la automatización de procesos. Entendida como «una serie de sistemas que exhiben un comportamiento que analiza su entorno y toma acciones, con cierto grado de autonomía, para lograr ob-

jetivos específicos» (Grupo de Expertos de Alto Nivel sobre IA de la Comisión Europea, 2019), también es imperativo mencionar los riesgos de su uso poco ético. Por ejemplo, se reportan la erosión de los datos personales y vigilancia indiscriminada, la discriminación algorítmica y una implementación indebida en campañas electorales.

Sin embargo, las oportunidades parecen superar ampliamente a los riesgos. La proliferación de la IA como una tecnología anticorrupción —también conocida como AI-ACT por sus siglas en inglés— ha despertado el interés de los funcionarios públicos, los activistas y periodistas de investigación, así como los académicos expertos en la materia. La AI-ACT constituye una serie de ensamblajes sociotécnicos que permiten analizar grandes volúmenes de información, reducir la discrecionalidad de los funcionarios públicos y mediar entre los ciudadanos y los gobiernos (Mattoni, 2024).

Su potencial predictivo y preventivo aporta agilidad y eficiencia a la lucha contra la corrupción en América Latina, especialmente en Brasil, país líder en materia de IA para anticorrupción. Odilla (2023) sistematiza más de treinta iniciativas impulsadas por funcionarios públicos (*top down*) y organizaciones civiles (*bottom up*) que

promueven el monitoreo, identificación, reporte y predicción de irregularidades y riesgos de corrupción. Rosie, Alice y Monica son solo algunas de las iniciativas a la vanguardia de la IA-ACT en América Latina. Por ejemplo, Alice (Análisis de Licitaciones, Contratos y Convocatorias Públicas) y Monica (Monitoreo Integrado para el Control de Adquisiciones) escanean los procesos de adquisición para identificar irregularidades, y el Servicio de Impuestos Internos de Brasil utiliza la IA para detectar fraudes aduaneros, mientras que algunas agencias estatales están implementando la IA para esfuerzos anticorrupción más amplios. Sin embargo, hay una lenta adaptabilidad a nuevos tipos de irregularidades con una auditoría limitada a cargo de expertos. Aún queda por afinar la generación de datos sesgados, una implementación responsable y el perfeccionamiento de algoritmos fallidos.

Oportunidades y beneficios de la IA en la lucha contra la corrupción

La inteligencia artificial generativa y los grandes modelos de lenguaje ofrecen en el ámbito gubernamental un sinfín de oportunidades para innovar en la lucha contra la corrupción. A continuación, se mencionan algunas de sus aplicaciones.

Análisis de datos y reconocimiento de patrones

La IA permite procesar grandes volúmenes de información para detectar tempranamente posibles escenarios de actividad corrupta a través de inconsistencias o duplicidad de información en transacciones financieras, licitaciones, contrataciones o subvenciones. La IA-ACT puede ayudar a predecir áreas o sectores con mayor riesgo de fraude en el futuro basándose en datos

« La mayoría de los países de la región empeoraron o se estancaron en materia anticorrupción. Solo Guyana y República Dominicana registran avances significativos y Venezuela cae a un mínimo histórico en el ranking global. »

históricos y tendencias actuales. Esto es particularmente útil para identificar conflictos de interés o evaluar riesgos de corrupción, a fin de detectar anomalías e indicios de corrupción.

Un caso particular es el de la gobernanza proactiva en España a través del sistema Saler (Sistema de Alerta Rápida) de la Inspección General de Servicios de la Generalitat Valenciana. Este tiene como objetivo principal anticipar riesgos o debilidades que puedan perjudicar a la administración pública por inercia o malas prácticas. Saler se vale de la enorme cantidad de información digitalizada que maneja la Generalitat Valenciana, además de bases de datos de registradores, notarios, entidades de propiedad intelectual, entre otras, para analizar cualquier procedimiento administrativo de interés para oficiales de *compliance*. Estos riesgos se asocian a seguridad de información, licitaciones, comités de selección, colusión, verificaciones, gobernanza, ética, cumplimiento de la ley, recursos humanos, entre otros.

Mediante este sistema, por ejemplo, la seguridad social se apoya en algoritmos para monitorear individuos en situación de paro y, con ello, detectar incidencias de

fraude entre los beneficiarios de subvenciones. Esta herramienta predictiva se evalúa el estado de salud de las personas y predice la probabilidad de que estén en condiciones de volver al trabajo. Cabe señalar que debe apoyarse de un análisis más minucioso para evitar el desbordamiento de falsos positivos en desmedro de ciudadanos que realmente necesitan la ayuda estatal.

Del mismo modo, es posible analizar gastos de gobiernos locales o ministerios e identificar posibles sobrecostos, deficiencias o malas prácticas. Entre los países miembros de la OCDE, las compras públicas representan el 13% de su producto interno bruto, mientras que para América Latina dicho porcentaje alcanza el 8% (Pérez, 2021). Pese a que es una de las áreas más vulnerables a la corrupción, los recursos para el control y el monitoreo del gasto público suelen ser escasos. Se presentan a continuación dos casos de estudio al respecto.

VigIA

Desarrollado por el *Tic Tank* de la Universidad del Rosario —un *think tank* con enfoque en tecnologías de la información— junto a la Corporación Andina de Fomento (CAF) para la Veeduría Distrital de Bogotá, este ejemplo de uso de IA contribuye a la supervisión de contratos de Alcaldía de Bogotá con alto riesgo de corrupción e ineficiencias, aprovechando los datos proporcionados por el Sistema Electrónico para la Contratación Pública de Colombia (Secop) a través de la plataforma de la Agencia Nacional de Contratación Pública (Colombia Compra Eficiente). A través de modelos de aprendizaje de máquinas (*machine learning*) se predice el riesgo de incurrir en corrupción en cada contrato. Mediante esta tecnología

» La IA facilita la automatización de tareas rutinarias, lo que permite reducir el error humano, el tiempo requerido para identificar riesgos de corrupción [...] [y] mejorar la eficiencia de los procesos. «

se agiliza el trabajo de auditoría en la detección de ineficiencias e irregularidades que alimenta puntajes de riesgo con que las veedurías distritales determinan qué contratos tienen la mayor probabilidad de ser irregulares o ineficientes.

Serenata de amor: IA para el control social de la administración pública

Este proyecto, concebido en Brasil en 2016 por el científico de datos Irio Musskopf, el sociólogo Eduardo Cuducos y el empresario Felipe Cabral a raíz del estallido de uno de los escándalos más sonados de corrupción en el país, conocido como *Mensalao* —*gran mensualidad*, en castellano—, debido a los pagos indebidos al interior de la Cámara baja del Parlamento brasileño. Mediante el uso de *machine learning*, con datos del gobierno, se detectan señales de alerta en el gasto público. Estas incidencias son publicadas en X a través de un bot llamado Rosie, al que se suman La Denunciante (*whistleblower*, en inglés), Jarbas (que permite la visualización de datos) y Toolbox. La etapa inicial registró 629 denuncias que involucraban gastos de 216 diputados federales de un total de 513.



Optimización de procedimientos

La IA facilita la automatización de tareas rutinarias, lo cual permite reducir el error humano y el tiempo requerido para identificar riesgos de corrupción. Sirve principalmente para mejorar la eficiencia de los procesos y, por consecuencia, los esfuerzos anticorrupción. Por ejemplo, Aarvik (2019) cita el caso del gobierno de Kenya en colaboración con el grupo de investigación de IBM a fin de reducir los incentivos de recurrir a sobornos para realizar trámites. Recordemos que buena parte de las transacciones corruptas tratan de engrasar las ruedas, es decir, agilizar trámites que no deberían tomar tanto tiempo o recursos en primer lugar. Al hacer los procedimientos más eficientes, el país mejoró su posición en el *ranking* Doing Business del Banco Mundial que evalúa el ambiente regulatorio para hacer negocios en 189 países. Kenya pasó del

puesto 136 al 56¹. Es imperativo contar con un alto grado de digitalización en los gobiernos como paso previo a esta transformación.

También existen oportunidades para acelerar canales de denuncia, otro de los pilares de la anticorrupción. Utilizar la IA para diseñar e implementar un algoritmo de *priorización* y recepción de denuncias tiene como objetivo jerarquizarlas reduciendo los costos asociados a atender cada una de ellas por los funcionarios. Un estudio realizado por Pierri y Lafuente (2022), del Banco Interamericano de Desarrollo, aporta evidencia sobre el procesamiento de denuncias ciudadanas en el programa Nuevos Talentos en Control Gubernamental, de la Contraloría General de la República (CGR), en Perú.

¹ Después de irregularidades en los datos de los informes Doing Business de 2018 y 2020, la administración del Banco Mundial suspendió la elaboración de la edición siguiente e inició una serie de revisiones y auditorías del informe y su metodología.



Con una muestra de cinco mil incidentes, donde un 40% no requieren la atención de la CGR, mediante el uso de dos algoritmos de *priorización y admisión* se aumentó la tasa de éxito en el manejo de denuncias en un 36%, mientras que la tasa de éxito de las advertencias mejoró en un 27%. De acuerdo con estos resultados preliminares, el programa parece ser una iniciativa efectiva para mejorar los procesos internos de la CGR y contribuir a la lucha contra la corrupción en Perú. Mejorar el proceso de denuncia permite que la IA recomiende una serie de pasos o acciones basándose en casos anteriores, optimizando así los recursos y los tiempos de investigación.

Riesgos y desafíos del uso de la IA en la lucha contra la corrupción

Pese al creciente interés de la sociedad en las inmensas oportunidades del uso de la IA

y el consenso generalizado sobre el impacto positivo de esta en materia anticorrupción (Colonelli et al., 2020), existe también una serie de peligros directos e indirectos que deben considerarse. Figuras públicas del mundo de la tecnología, academia, funcionarios y periodistas firmaron una carta sobre los riesgos y estrategias de mitigación como una prioridad global, al mismo nivel que el manejo pospandemia o la guerra nuclear. Algunos de estos se mencionan brevemente a continuación.

Manipulación de los sistemas por actores corruptos

Podría existir una corrupción de IA donde el uso de sistemas de IA por funcionarios se realiza para obtener beneficios privados (Köbis et al., 2022). Siguiendo la lógica de la definición más popular de corrupción, los servidores públicos potencialmente tendrían acceso a una serie de ensambla-

jes tecnológicos que les permitiría cometer actos ilícitos y abusar de su discrecionalidad. Al tratarse de una nueva tecnología, la opacidad en el diseño, manipulación e implementación de esta puede obstaculizar la comprensión del proceso de toma de decisiones y, por consecuencia, generar desconfianza entre los usuarios. Y no estamos hablando de uso conscientemente corrupto de la IA, sino también aprovechamiento de las vulnerabilidades de los sistemas.

Riesgos de vigilancia masiva y violación de derechos civiles

Aunque la corrupción sigue siendo una preocupación primordial para los latinoamericanos, el principal lastre es la inseguridad. Aunque América Latina concentra el 9% de la población mundial, también registra la tercera parte de la tasa de homicidios a nivel global. Dentro de la región, México destaca con más de treinta mil asesinatos anuales en medio de una pelea por el control del territorio por una docena de carteles.

No es sorpresa que durante las últimas elecciones el ex candidato presidencial Marcelo Ebrard presentase un plan de seguridad llamado Angel (Avanzadas Normas de Geolocalización y Seguridad) que incluía cámaras con dispositivos de reconocimiento facial a fin de crear un ecosistema basado en IA con todas las bases de datos de México. Suponía la implementación de tecnologías de vigilancia masiva y biométrica en el espacio público para generar sistemas de vigilancia predictiva, iniciativas de ley para instalar cámaras de vigilancia con tecnología de reconocimiento, geolocalización de vehículos, identificación morfológica de delincuentes por la forma de caminar, uso de drones

❖ **Si bien la IA tiene el potencial de ser una herramienta poderosa en la lucha contra la corrupción, es esencial abordar sus implicaciones éticas a fin de garantizar un uso responsable y transparente.** ❖

y cámaras inteligentes corporales para elementos de la Guardia Nacional mexicana.

Sin embargo, numerosas investigaciones demuestran que las tecnologías de vigilancia masiva con reconocimiento facial son altamente susceptibles de identificar erróneamente a las personas, lo que ha provocado múltiples casos de detenciones arbitrarias de personas inocentes identificadas por equivocación como perpetradoras de delitos, especialmente si no son blancas.

Sobredependencia de la tecnología

Por otro lado, una dependencia excesiva de la tecnología puede hacer de una institución o un gobierno un blanco fácil de ciberataques y fallas técnicas. Es necesario tener en cuenta experiencias como Albania, que se convertiría en el primer país en desplegar el uso de la IA en su proceso de adhesión a la Unión Europea. El gobierno albanés utilizará ChatGPT, el modelo de LLM más popular del mundo con un millón de usuarios en su primera semana, para traducir al shqip miles de páginas de medidas y disposiciones legales de la UE, a fin de integrarlas en la legislación albanesa vigente. Esto ocurre luego de un acuerdo con OpenAI, cuya directora tecnológica eje-

cutiva Mira Murati es de origen albanés. Sin duda, se trata de una manera novedosa que ahorrará dinero y tiempo al aparato estatal. Aunque no hay que olvidar las implicaciones éticas sobre el vacío legal existente en materia de privacidad, transparencia y dependencia excesiva de la tecnología en dicho país.

Sesgos algorítmicos en la identificación

Ya que esta tecnología se alimenta de información preexistente, no es más que un reflejo fidedigno de lo que ocurre en la realidad (que también es susceptible de sesgos conscientes e inconscientes). A esto se le llama *sesgo algorítmico*, cuya repercusión en el uso de IA anticorrupción es generar falsos positivos mediante el refuerzo de desigualdades y discriminaciones. Por ejemplo, si al analizar la incidencia de la corrupción en el pasado existió una concentración de personas con características particulares de grupo étnico, edad, lugar de origen u ocupación, un algoritmo destinado a detectar futuros casos de corrupción podría correlacionar erróneamente a personas con dichas características pero que no han cometido actos ilícitos.

Estudios en Estados Unidos muestran que mientras más oscuro sea el color de piel, menos acertado será el resultado. Esto se debe a que los repositorios existentes cuentan, en su mayoría, con una sobrerrepresentación de hombres blancos. Esto es particularmente problemático en el uso policial. El uso de datos de entrenamiento del algoritmo con información sesgada no hace más que generar fallos en la identificación y, finalmente, decisiones de tratamiento incorrectas. Por ello, es vital utilizar la tecnología a favor de la eficiencia y la cobertura, pero sin prescindir de la pericia y experiencia de agentes encargados de filtrar y analizar las bases de datos que alimentan los sistemas de IA.

Reflexiones finales en torno al potencial de la IA en la lucha contra la corrupción y el futuro de la gobernanza pública en la era digital

Si bien la IA tiene el potencial de ser una herramienta poderosa en la lucha contra la corrupción, es esencial abordar sus implicaciones éticas a fin de garantizar un uso responsable y transparente. Saber aprovechar las bondades de la IA para analizar, predecir y automatizar datos, ya sea desde las agencias anticorrupción o desde la sociedad civil, debe ser acompañado de mecanismos que promuevan la transparencia, la rendición de cuentas y la mitigación de sesgos que aseguran una buena gobernanza de IA.

Cabe señalar los diferentes retos y oportunidades para las iniciativas en materia de AI-ACT que vengan desde las agencias anticorrupción (desde arriba) o desde la sociedad civil (desde abajo). Las primeras podrían perpetuar las existentes asimetrías de poder de las entidades estatales y generar consecuencias no anticipadas en la lucha contra la corrupción, mientras que las segundas se enfrentan a barreras de acceso a datos abiertos que dependen en gran medida del nivel de digitalización de los gobiernos. Sin embargo, apoyadas de las redes sociales y la vigilancia ciudadana, ofrecen ventajas para la difusión y actualización en tiempo real de incidencias y riesgos de corrupción.

Por otro lado, si bien las iniciativas IA anticorrupción agilizan procesos, estos no pueden prescindir de la acción humana. La opacidad en el diseño e implementación de algoritmo sigue siendo un desafío para generar confianza en los sistemas, sobre todo en América Latina, donde la mayoría de la gente tiene bajos niveles de confianza interpersonal y en las instituciones. De acuerdo con un estudio del Banco Interamericano de Desarrollo,

nueve de cada diez latinoamericanos desconfían de su prójimo. Esto se suma a la falta de independencia y transparencia del Poder Judicial en la mayoría de los países de la región, así como a vacíos y limitaciones de la legislación vigente y el grado de discrecionalidad de las élites políticas y económicas. En un contexto de este tipo, es complejo implementar mecanismos anticorrupción que se valgan o no de la IA, que sean eficaces y cuenten con el respaldo ciudadano necesario.

Más allá de innovaciones, los organismos sancionadores también deben operar con sumo cuidado nuevos sistemas, a fin de evitar agravar la desigualdad y generar una persecución selectiva basada en sesgos algorítmicos. Por ejemplo, los funcionarios públicos que provienen de comunidades vulnerables o de minorías podrían ser desproporcionadamente investigados o sancionados, aunque sus acciones no sean más corruptas que las de otros funcionarios. Esto no solo crea una injusticia individual, sino que también refuerza los estereotipos sociales y agrava la percepción de parcialidad en la lucha contra la corrupción.

Si las personas perciben que el sistema solo persigue a ciertos grupos, en lugar de tratar a todos los funcionarios por igual, puede generarse una desconfianza hacia las instituciones anticorrupción. La falta de transparencia sobre cómo se toma la decisión de investigar a alguien también puede contribuir a esta desconfianza. Se registran casos donde la IA es utilizada por regímenes autoritarios y de manera discrecional como la persecución de activistas antirracismo en Miami y Nueva York, grupos feministas en Estados Unidos, grupos feministas en la Ciudad de México, activistas prodemocracia en Hong Kong, periodistas y opositores políticos en Egipto,

« Si las personas perciben que el sistema solo persigue a ciertos grupos, puede generarse una desconfianza hacia las instituciones anticorrupción. »

to, hasta el monitoreo sistemático, perfilamiento y persecución de minorías étnicas como los uigures en Xinjiang.

Una de las estrategias de mitigación de riesgo es la transparencia algorítmica para explicar cómo funcionan los algoritmos y qué tipo de decisión toman, de forma que puedan ser auditables y monitoreables y así eliminar la perpetuación de sesgos. Del mismo modo opera el aumento en número y variedad de las fuentes de datos, para entrenar los algoritmos mientras se protege la privacidad de la información personal de los usuarios.

El camino a seguir es generar más confiabilidad y precisión en las predicciones de riesgos, sin reemplazar la pericia y experiencia de auditores. Esto representa una gran tarea en América Latina, región con una gran brecha de infraestructura digital, donde solo el 57% de los ciudadanos tienen acceso a un servicio activo de internet móvil. La diferencia entre América del Sur y Centroamérica es casi del doble (77 % en la primera, y 37% en la segunda), destacando Brasil (77%) y Haití tan solo 6%. Cerrar las brechas entre y dentro de cada país, considerando las desigualdades entre las zonas rurales y urbanas, es vital para asegurar una implementación y despliegue justo de la arquitectura digital de sistema de IA para la lucha contra la co-

rrupción, así como sistemas neutrales que reduzcan los sesgos y las desigualdades producto de estos.

Los gobiernos, las empresas y la sociedad civil deben comprometerse en aprovechar el poder transformativo de la IA mediante una vigilancia constante, nuevo marco regulatorio y compromiso ético. Recordemos que corromper a un individuo puede tener un impacto en un número limitado de personas. En cambio, corromper un algoritmo podría afectar a miles de personas en tiempo récord. ♦

Bibliografía

- AARVIK, P. (2019). *Artificial Intelligence – a promising anti-corruption tool in development settings?* U4 Anti-Corruption Resource Centre. <https://www.u4.no/publications/artificial-intelligence-a-promising-anti-corruption-tool-in-development-settings>
- ADAM, I., Y FAZEKAS, M. (2021). Are emerging technologies helping win the fight against corruption? A review of the state of evidence. *Information Economics and Policy*, 57, p. 100950. DOI: 10.1016/j.infoecopol.2021.100950.
- COLONNELLI, E., GALLEGO, J. A., Y PREM, M. (2020, 26 de diciembre). *What Predicts Corruption?* https://www.researchgate.net/publication/347995419_What_Predicts_Corruption
- DÁVILA PÉREZ, J. (2021). Impacto y beneficios de las reformas en los sistemas de contratación pública en América Latina y el Caribe. *Red Interamericana de Compras Gubernamentales*. <https://ricg.org/es/publicaciones/impacto-y-beneficios-de-las-reformas-en-los-sistemas-de-contratacion-publica-en-america-latina-y-el-caribe/>
- KÖBIS, N. (2023). Bribes for Bias: Can AI be corrupted? *Transparency International Blog*. <https://www.transparency.org/en/blog/bribes-for-bias-can-ai-be-corrupted>
- KÖBIS, N., STARKE, CH., Y EDWARD-GILL, J. (2022). *The corruption risks of artificial intelligence*. Transparency International Working Paper. <https://knowledgehub.transparency.org/assets/uploads/kproducts/The-Corruption-Risks-of-Artificial-Intelligence.pdf>
- ODILLA, F. (2023). Bots against corruption: Exploring the benefits and limitations of ai-based anti-corruption technology. *Crime Law Soc Change*, 80(4), 1-44. DOI: 10.1007/s10611-023-10091-0.
- PIERRI, G., Y LAFUENTE, M. (2022). *Human Talent Management and Corruption Control: The Effect of the New Talents in Government Control Program on the Detection of Corruption in Peru*. IADB Discussion Paper, IDB-DP-952. <https://publications.iadb.org/en/human-talent-management-and-corruption-control-effect-new-talents-government-control-program>



Denisse Rodríguez-Olivari

Doctora en Ciencia Política (Humboldt-Universität, Berlín). Máster en Desarrollo Internacional (Universidad de Manchester). Licenciada en Ciencia Política y Gobierno (Pontificia Universidad Católica del Perú). Research Associate de la University of Glasgow, Adam Smith Business School. Experta en anticorrupción e integridad.

X: @DenisseROlivari

IG: @denisser

LI: denisserodriguezolivari