

II

2023

N.º 140

cuadernos de política criminal segunda época



Dykinson, S.L.

II

2023

N.º 140

**cuadernos
de política criminal
segunda época**

Edita

Dykinson, S.L.

AVISO IMPORTANTE A NUESTROS SUSCRIPTORES

Si desea suscribirse a **Cuadernos de Política Criminal**, llame por teléfono o envíe un e-mail a info@dykinson.com, indicando la forma de pago y el número o números a los que quiere suscribirse, e inmediatamente recibirá su pedido.

CPC se adhiere a las Core Practices del Committee on Publication Ethics (COPE) disponibles en: <https://publicationethics.org/core-practices>; y especialmente a los Principios de Buenas Prácticas y Transparencia en las Publicaciones Académicas desarrollados por el Committee on Publication Ethics (COPE), Open Access Scholarly Publishers Association (OASPA), Directory of Open Access Journals (DOAJ) y World Association of Medical Editors (WAME) disponibles en: <https://publicationethics.org/resources/guidelines-new/principles-transparency-and-best-practice-scholarly-publishing>. La Declaración de ética y malas prácticas completa de CPC puede ser consultada en sus versiones en español e inglés: <https://www.dykinson.com/revistas/cuadernos-de-politica-criminal/>

La Revista no se responsabiliza de las opiniones contenidas en los artículos

Edita: Dykinson, S.L.
C/ Meléndez Valdés, 61 — 28015 Madrid
Tels. 91 544 28 46 / 91 544 28 69
Fax 91 544 60 40
info@dykinson.com / www.dykinson.com

Imprime: Safekat, S. L.
Laguna del Marquesado, 32 - 28021 Madrid
www.safekat.com

ISSN: 0210-4059

Depósito Legal: M. 7533-1977

DOI: 10.14679/2247

La Editorial Dykinson, a los efectos previstos en el artículo 32.1 párrafo segundo del vigente TRLPI, se opone expresamente a que cualquiera de las páginas de esta obra o partes de ella sean utilizadas para la realización de resúmenes de prensa.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la ley. Diríjase a CEDRO (Centro Español de Derechos Reprográficos) si necesita fotocopiar o escanear algún fragmento de esta obra (www.conlicencia.com; 91 702 19 70 / 93 272 04 47).119.

CONTENIDO

SECCIÓN DE ESTUDIOS PENALES

LA SUPRESIÓN DE LA SEDICIÓN Y LA MODIFICACIÓN DEL DELITO DE DESÓRDENES: SOBRE EL ARTE DEL TRAMPANTOJO. <i>Por M^a del Carmen Gómez Rivero</i>	5
POLÍTICA CRIMINAL Y DELITOS SEXUALES: HACIA UN ENFOQUE QUE SUPERE EL FEMINISMO PUNITIVO. <i>Por Ana I. Pérez Machío</i>	39
LA REPARACIÓN DEL DAÑO A LA VÍCTIMA COMO ELEMENTO DE INDIVIDUALIZACIÓN DE LA PENA: LA ATENUANTE DEL ART. 21.5 CP DESDE UNA PERSPECTIVA RESTAURATIVA. <i>Por Eva M.^a Domínguez Izquierdo</i>	63
APROXIMACIÓN A LA APLICACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA PREVENIR LA CORRUPCIÓN EN LA ADMINISTRACIÓN PÚBLICA. <i>Por Cristina Domingo Jaramillo</i>	105

SECCIÓN ESTUDIOS CRIMINOLÓGICOS

NUEVAS FORMAS DE FINANCIACIÓN DEL TERRORISMO. RETOS Y SOLUCIONES PARA COMBATIRLA UTILIZANDO SISTEMAS INTELIGENTES. <i>Por Javier Valls Prieto</i>	135
---	-----

SECCIÓN JURISPRUDENCIAL

PANORAMA JURISPRUDENCIAL: TRIBUNAL CONSTITUCIONAL Y TRIBUNAL SUPREMO. <i>Por Manuel Jaén Vallejo</i>	163
--	-----

SECCIÓN BIBLIOGRÁFICA

RECENSIÓN A THOMAS DUVE/STEFAN RUPPERT (COORDS.), <i>RECHTSWISSENSCHAFT IN DER BERLINER REPUBLIK</i> , SUHRKAMP, BERLÍN, 2018, 767 PÁGINAS. <i>Por José Destéfanis/Pablo Sánchez-Ostíz</i>	183
--	-----

RECENSIÓN A ROMERO ABOLAFIO, J.J. <i>INTERROGANTES ACTUALES SOBRE EL CAMBIO CLIMÁTICO. ANÁLISIS CONSTITUCIONAL, PENAL Y CRIMINOLÓGICO</i> , DYKINSON, MADRID, 2023, 439 PÁGINAS <i>Por Cristina Domingo Jaramillo ..</i>	193
RECENSIÓN A LAISE, LUCIANO D., <i>CÓMO ARGUMENTAR UN CASO PENAL: TÉCNICAS PARA LA DEFENSA EN EL PROCESO ADVERSARIAL</i> , EDT. HAMMURABI, BUENOS AIRES, 2023, 176 PÁGINAS. <i>Por Roberto Cruz Palmera.....</i>	213
NOTICIARIO	217
POLÍTICA EDITORIAL, CRITERIOS Y RÉGIMEN PARA LA PUBLICACIÓN DE TRABAJOS ORIGINALES EN CPC	229

APROXIMACIÓN A LA APLICACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA PREVENIR LA CORRUPCIÓN EN LA ADMINISTRACIÓN PÚBLICA

Approach to the application of artificial intelligence systems to prevent corruption in the public administration

CRISTINA DOMINGO JARAMILLO*

Fecha de aceptación: 22/07/2023

Fecha de aprobación: 06/09/2023

DOI: 10.14679/2251

RESUMEN: Los efectos que la corrupción pública tiene en el entramado social, político y económico de un país son devastadores. La Administración es un ámbito caracterizado por la opacidad y el secretismo, por lo que los delitos cometidos en el seno de la misma suelen quedar ocultos. Por ese motivo, es necesario establecer sistemas de detección precoz de tales ilícitos, con el fin de poder prevenirlos. En dicho sentido, la Inteligencia Artificial aparece como una herramienta que puede contribuir a este objetivo. De modo que, en la presente investigación se analiza el potencial que los sistemas inteligentes tienen en la lucha contra la corrupción pública, a través de una revisión bibliográfica del análisis de aquellos estudios que han puesto en marcha dichos sistemas para combatir la corrupción.

PALABRAS CLAVE: Sistemas inteligentes, corrupción, prevención, detección temprana, transparencia.

* Investigadora postdoctoral Margarita Salas Departamento de Derecho Penal Universidad de Granada.

ABSTRACT: *The effects of public corruption on the social, political and economic framework of a country are devastating. The Administration is characterized by its opacity and secrecy, so crimes committed within it are often able to remain hidden. For this reason, it is necessary to set up protocols for the early detection of such offenses in order to prevent them. In this sense, Artificial Intelligence appears as an useful tool that can contribute to this objective. Thus, this research analyzes the potential that intelligent systems have in the fight against public corruption, through a bibliographic review of the analysis of those studies that have implemented such systems to fight corruption.*

KEYWORDS: *Intelligent systems, corruption, prevention, early detection, transparency.*

SUMARIO: I. La corrupción como grave problema social. II. El valor de la inteligencia artificial para prevenir la delincuencia. 1. Aproximación al término Inteligencia Artificial. 2. Sistemas inteligentes en materia de prevención y detección del delito. III. Inteligencia artificial en la lucha contra la corrupción. 1. Cuestiones previas. 2. Iniciativas anticorrupción según el agente que las lleva a cabo. 2.1. Top-down. 2.2. Bottom-up. 2.2.1. Sistema DOZORRO en Ucrania. 2.2.2. Botivist. 2.2.3. Experiencia en España con mapas auto-organizados. IV. Elementos fundamentales para la utilización de los sistemas de inteligencia artificial y problemas asociados. 1. Digitalización, transparencia y acceso a datos abiertos. 2. Algunas controversias sobre el uso de sistemas inteligentes. V. Conclusiones.

I. LA CORRUPCIÓN COMO GRAVE PROBLEMA SOCIAL

La corrupción es un fenómeno delictivo constante y ubicuo de todas las sociedades¹, por lo que las características que presente en cada una serán distintas y dependerán, a su vez, de las del momento y lugar concretos. Además, es un término ambiguo y de difícil definición, al no contar con unos contornos precisos, en tanto puede materializarse de múltiples formas: corrupción pública, privada, administrativa, urbanística, en los negocios, etc. Si bien es cierto que todas ellas tienen en común el hecho de suponer la alteración, tergiversación o perversión de algo². En

¹ MELO LIMA, M.S., y DELEN, D. (2020). "Predicting and explaining corruption across countries: A machine learning approach", *Government Information Quarterly*, n.º. 37, pág. 3.

² BENÍTEZ YÉBENES, J.R. (2021). "Algunos aspectos procesales de la corrupción política", en Morillas Cueva, L. (Dir.), *Respuestas jurídicas frente a la corrupción política*, Dykinson, Madrid, pág. 479. Véase, igualmente, PÉREZ FERRER, F. (2013). "Algunas reflexiones sobre el fenómeno de la corrupción y su extensión en el ámbito punitivo", en Morillas

este caso concreto, centraremos nuestro estudio en la corrupción pública, es decir, aquella que es ejecutada por una autoridad o funcionario público en el ejercicio de sus funciones, de las que hace un mal uso para obtener algún tipo de provecho ilegítimo. En dicho sentido, se considera como tal las prácticas de pagos ilegales a agentes públicos para obtener beneficios o el abuso del cargo para conseguir ganancias privadas³. Así las cosas, ha llegado a calificarse como “la contaminación de lo público por lo privado”⁴, ya sea en favor propio o en el de terceros⁵.

A día de hoy, esta modalidad delictiva es una constante y repercute negativamente en el conjunto de la sociedad, no solo por su alcance financiero y económico, pues ya en el año 2014 la Comisión Europea estimó que el coste que tenía en la economía de la UE era de 120.000 millones de euros⁶; sino también porque erosiona el contrato social que sustenta las democracias y, por ende, la credibilidad y legitimidad del sistema democrático, fomentando la desconfianza de la población y las narrativas populistas⁷. En sus manifestaciones más intensas, la corrup-

Cueva, L. (Dir.) y Suárez López, J.M. (Coord.), *Urbanismo y corrupción política (una visión penal, civil y administrativa)*, Dykinson, Madrid, págs. 139-140, quien establece una serie de características comunes de todas las modalidades corruptas: a) suponen la transgresión de un deber posicional, porque quien corrompe atenta contra las reglas del cargo o funciones que tiene asignadas; b) son parasitarios de un marco normativo de referencia donde se realiza la acción corrupta; y c) esta última debe estar unida a la expectativa de obtener un beneficio.

³ MELO LIMA, M.S., y DELEN, D. “Predicting and explaining corruption across countries...”, cit., pág. 3.

⁴ THOMPSON, D.F. (2005). “Two concepts of corruption”, *George Washington Law Review*, nº. 73, pág. 1040. En dicha línea, hemos de tener en cuenta además que la corrupción pública se encuentra ligada a la privada o cometida por particulares ajenos al ámbito público. Véase, en este sentido, más ampliamente, MORILLAS CUEVA, L. (2022). “Corrupción, derechos humanos e internacionalización de las respuestas jurídico-penales”, en Olmedo Cardenete, M., y otros. (Coords.), *Estudios en homenaje al Prof. Dr. D. Jesús Martínez Ruiz*, Dykinson, Madrid, págs. 376-382.

⁵ THOMPSON, D.F. (2018). “Theories of Institutional Corruption”, *Annual Review of Political Science*, vol. 21, nº. 26, págs. 9 y 10. El autor distingue la ganancia personal de la institucional. Cuando un funcionario acepta un soborno a cambio de un favor, la ganancia personal que recibe no es una parte legítima de su salario, del mismo modo que realizar dicho favor no está dentro de las funciones del puesto que desempeña. Por su parte, la ganancia institucional incluye bienes que fueron usados inicialmente a nivel institucional y cumplen una función en este ámbito. Unido a la ganancia, el autor en cita alude también a la ventaja institucional, catalogándola de servicio, al beneficiar a un ciudadano particular o a una organización distinta de aquella en la que el funcionario trabaja.

⁶ COMISIÓN EUROPEA. (2014). *Informe de la Comisión al Consejo y al Parlamento Europeo sobre la Lucha contra la Corrupción en la UE*. COM(2014) 38 final, pág. 2.

⁷ COMISIÓN EUROPEA. (2022). *New approaches for combatting corruption and other undue influences on political decision-making*. Recurso electrónico obtenido a tra-

ción es una de las principales amenazas del Estado de Derecho, pudiendo pervertir la división de poderes y el reconocimiento y garantía de los derechos, así como quebrantar los cimientos estructurales del operativo económico estatal⁸.

En vista de las graves consecuencias que tiene para la sociedad, la Oficina de las Naciones Unidas contra la Droga y el Delito en la Convención celebrada en Nueva York en el año 2004 contra esta lacra, la califica de “plaga insidiosa” a nivel mundial⁹, por lo que destina todo un Capítulo, el IV, a la “cooperación internacional”. No solo en este nivel, sino también en el nacional y autonómico se han llevado a cabo grandes esfuerzos para combatir la corrupción¹⁰. Nuestro legislador penal, preocupado por esta situación, ha pretendido abordarla a través de un proceso expansionista del ordenamiento punitivo, cuyo fin no es otro que castigar todos los comportamientos vinculados a la misma¹¹. De forma que ha dedicado el Título XIX del Código Penal, con diez capítulos, a los delitos contra la Administración Pública¹². Este orden jurisdiccional, regido por el principio de intervención mínima, ha de actuar en última instancia, una vez que se han sobrepasado todas las barreras de protección y se ha cometido un ilícito que reviste cierta entidad. Así, debe ponerse el foco de atención en las medidas preventivas, puesto que los recursos públicos son

vés de la Web: https://cordis.europa.eu/programme/id/HORIZON_HORIZON-CL2-2023-DEMOCRACY-01-03, [consultado el día 3 de diciembre de 2022].

⁸ MORILLAS CUEVA, L. (2021). “Doble dimensión penal de la contabilidad irregular en procesos electorales como forma de corrupción”, en Morillas Cueva, L. (Dir.), *Respuestas jurídicas a la corrupción política*, Dykinson, Madrid, págs. 123-124; y, en el mismo sentido pero unos años antes, MONTESINOS PADILLA, C. (2017). “Corrupción y transparencia en España: diagnóstico a la luz de las directrices del Consejo de Europa y la Unión Europea”, en Queralt Jiménez, J., y Santana Vega, D.M. (Dirs.), *Corrupción pública y privada en el Estado de Derecho*, Tirant lo Blanch, Valencia, pág. 79.

⁹ Sobre el estado de la corrupción a nivel internacional para el año 2021, véase TRANSPARENCIA INTERNACIONAL. (2022). *Índice Percepción de la Corrupción 2021*. ISBN: 978-3-96076-202-7, págs. 11 y ss. En el documento que la organización elabora anualmente, puede observarse que todos los países presentan registros de corrupción.

¹⁰ Vid., FERNÁNDEZ AJENJO, J.A. (2023). *Código de Lucha contra el Fraude y la Corrupción. Edición actualizada a 3 de marzo de 2023*, Boletín Oficial del Estado, Madrid.

¹¹ MORALES HERNÁNDEZ, M.A. (2021). “Problemas concursales entre el delito de cohecho y otras figuras vinculadas a la corrupción pública”, *Revista Electrónica de Estudios Penales y de la Seguridad: REEPS*, n.º. Extra 7, pág. 3.

¹² MORILLAS CUEVA, L. (2021). “Capítulo 48. Delitos contra la Administración Pública (I). Prevaricación de los funcionarios públicos y otros comportamientos injustos”, en Morillas Cueva, L. (Dir.), *Sistema de Derecho Penal. Parte Especial*, Dykinson, Madrid, pág. 1230. A juicio del autor en cita, esta criminalización de la corrupción pública, tal vez suponga una preocupación excesiva, “a veces deshilvanada y temporalizada en situaciones concretas”.

limitados. No obstante, el descubrimiento de las acciones que pueden dar lugar a un delito de corrupción no es tarea sencilla, dado que el público (al igual que el privado), se caracteriza por ser un entorno reservado. En tal línea el TEDH en la Sentencia de 12 de febrero de 2008, caso de Guja contra Moldavia, plantea que “los trabajadores tienen un deber de lealtad, de reserva y de discreción hacia el empleador. Esto vale, en particular, para los funcionarios, desde el momento en que la propia naturaleza de la función pública exige de sus miembros una obligación de lealtad y de reserva”. Asimismo, siguen produciéndose delitos de corrupción en el seno de las Administraciones Públicas, por lo que los esfuerzos realizados para frenarlos han sido insuficientes.

A pesar de los múltiples avances tecnológicos producidos en las últimas décadas, que vienen con la promesa de una mejora en la prevención de la delincuencia, pueden tener el efecto contrario y fomentar la corrupción¹³. El problema parece resistente a la solución y surgen nuevas tipologías corruptas cometidas digitalmente. Como indicamos *supra*, la corrupción se adapta a las particularidades de la sociedad del momento, caracterizada hoy día por el uso generalizado de las nuevas tecnologías de la información y la comunicación (desde este momento, TIC). Por tanto, la Comisión Europea considera, desde el punto de vista práctico, que las propuestas anticorrupción deben tener en cuenta el potencial de las tecnologías para detectar, prevenir y combatir esta realidad¹⁴. De hecho, en dicho contexto, las TIC se conciben como nuevos medios efectivos para prevenir, detectar y perseguir semejante tipo delictivo, al promover la transparencia, la rendición de cuentas y la participación ciudadana. Entre los nuevos medios anticorrupción destaca la Inteligencia Artificial (a partir de ahora, IA), junto a otros como el *Big Data*, las aplicaciones móviles y las páginas web. Todos ellos permiten un mejor acceso a la información pública, así como la posibilidad de monitorizar las actividades de los funcionarios, digitalizar los servicios públicos y fomentar la denuncia ciudadana. Sin embargo, la existencia y disponibilidad de las herramientas mencionadas no se traduce automáticamente en su uso, dependiendo del contenido proporcionado y las características de los usuarios¹⁵.

¹³ 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*, vol. 57, pág. 12.

¹⁴ COMISIÓN EUROPEA. *New approaches for combatting corruption and other undue influences on political decision-making...*, cit.

¹⁵ ADAM, I., y FAZEKAS, M. “Are emerging technologies helping win the fight against corruption?...”, cit., pág. 1.

Dada la rápida expansión de la IA en la sociedad actual, por la disponibilidad de ingentes cantidades de datos digitales, los avances tecnológicos en el ámbito de la capacidad informática y de almacenamiento, así como las innovaciones científicas y en ingeniería¹⁶; y su potencial en materia de prevención y detección de la delincuencia, en este caso concreto, en lo que a corrupción se refiere (como se pondrá de manifiesto *infra*), en lo siguiente, haciendo uso de la técnica de revisión bibliográfica, se abordará el valor de los sistemas inteligentes en la materia, analizando las distintas iniciativas puestas en marcha y algunos de los sistemas más prometedores en la lucha anticorrupción, teniendo en cuenta además los elementos necesarios para que la IA sea efectiva así como algunos de los problemas que lleva aparejada su utilización. Pero antes de profundizar en estas cuestiones, es necesario acercarse, siquiera brevemente, al concepto de inteligencia artificial y su aplicación en materia de predicción delictiva.

II. EL VALOR DE LA INTELIGENCIA ARTIFICIAL PARA PREVENIR LA DELINCUENCIA

1. APROXIMACIÓN AL TÉRMINO INTELIGENCIA ARTIFICIAL

Los avances en el ámbito de la IA consisten en la introducción de máquinas con la capacidad de aprender y ejecutar tareas cognitivas que antes se limitaban a los seres humanos¹⁷. Aunque pueda parecerlo, el término no es novedoso y se introdujo ya en la década de 1950, haciendo referencia a aquellas máquinas que podían hacer otras tareas distintas a las convencionales. A medida que aumentaba la potencia informática, el concepto se fue ampliando a las máquinas que tienen la capacidad de aprender¹⁸.

A pesar de lo inmediatamente señalado, no existe una definición única de IA y es muy difícil concretarla con exactitud, suponiendo un gran reto sistematizar un campo tan extenso y que evoluciona tan rápido¹⁹.

¹⁶ GRUPO DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL. (2019). *Directrices Éticas para una IA Fiable*, Bruselas, pág. 46.

¹⁷ COMEST. (2019). *Preliminary Study on the Ethics of Artificial Intelligence*, París, pág. 3.

¹⁸ *Ibd.*, p. 3.

¹⁹ VALLS PRIETO, J. (2021). *Inteligencia Artificial, derechos humanos y bienes jurídicos*, Aranzadi, Navarra, pág. 22; EL MISMO. (2022). "Sobre la responsabilidad penal por la utilización de sistemas inteligentes", *Revista Electrónica de Ciencia Penal y Criminología*, n.º. 24, pág. 3. Considera que la ausencia de un concepto claro y definido de IA se debe a la diversidad de disciplinas que han intentado elaborarlo, así como a la amalgama de tecnologías y definiciones existentes.

Para la Asociación por el Avance de la Inteligencia Artificial, la ausencia de dicho término preciso y universalmente aceptado de IA es lo que ha contribuido a que haya avanzado de forma más veloz²⁰.

No obstante, sobre lo que sí existe amplio consenso, es en entender que los mecanismos basados en IA o en “computación cognitiva” son capaces de imitar o incluso superar las capacidades cognitivas humanas²¹. Más concretamente, la UNESCO, si bien es consciente de que una definición única no es posible, dado que puede evolucionar con el paso del tiempo por el desarrollo tecnológico, en la Recomendación sobre la Ética de la Inteligencia Artificial adoptada el 23 de noviembre de 2021, la entiende como aquellos “sistemas que tienen la capacidad de procesar datos e información de una manera que se asemeja a un comportamiento inteligente, y normalmente incluye aspectos de razonamiento, aprendizaje, percepción, predicción, planificación o control”. Esta definición no incluye el componente humano que es fundamental para entrenar y definir los objetivos de la máquina, puesto que no puede ejecutar ninguna tarea que no esté previamente determinada. Por ese motivo, aquella ha de completarse con la ofrecida por la OCDE en la Recomendación del Consejo sobre Inteligencia Artificial de 2017, que hace referencia a la concreción de objetivos por parte de personas. De modo que cada sistema tendrá un fin específico que permitirá agilizar el proceso de toma de decisiones a los individuos que hacen uso del mismo. En dicha línea, creemos que el término más adecuado, por completo, es el ofrecido por el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial, constituido por la Comisión Europea, que entiende por mecanismos de IA los “sistemas de *software* (y en algunos casos también de *hardware*) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno a través de la obtención de datos, la interpretación de los datos estructurados o no estructurados que recopilan, el razonamiento sobre el conocimiento o el procesamiento de la información derivados de esos datos, y decidiendo la acción o acciones óptimas que deben llevar a cabo para lograr el objetivo establecido. Los sistemas de IA pueden utilizar normas simbólicas o aprender un modelo numérico; también pueden adaptar su conducta mediante el análisis del modo en que el entorno se ve afectado por sus acciones anteriores”.

²⁰ ASOCIACIÓN POR EL AVANCE DE LA INTELIGENCIA ARTIFICIAL. (2016). *Artificial Intelligence and Life in 2030*. Recurso electrónico obtenido de la Web: https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/ai100report10032016fnl_singles.pdf, [consultado el día 23 de enero de 2023], pág. 3.

²¹ COMEST, *Preliminary Study on the Ethics of Artificial Intelligence...*, cit., p. 3.

El *machine learning* reside también en este ámbito, donde múltiples métodos de varios niveles de complejidad se aplican para solucionar distintos problemas. Tales técnicas necesitan una base de datos para entrenar al algoritmo sobre la forma de tratar la información²². En ese sentido, los principales elementos que integran la IA son datos y algoritmos. Estos últimos se entrenan para inferir determinados modelos a partir de un conjunto de datos, con el fin de concretar las acciones que se precisan para alcanzar el objetivo establecido²³. Aunque los sistemas inteligentes pueden actuar de forma autónoma, los fines están acotados por personas. A tal respecto, Miró Llinares cuando aborda los diversos tipos de sistemas inteligentes, alude a una posible autonomía completa de la IA, que provendría de la capacidad real de la máquina para adaptar las decisiones a un contexto distinto de aquel para el que se programó, siendo capaz de aprender por sí misma²⁴. Esto no sería posible en la actualidad puesto que aquel ve limitados sus objetivos y funciones a lo establecido por los diseñadores, de forma que la autonomía va referida al modelado y la representación del conocimiento, la explotación de datos y el cálculo de correlaciones, tal como pone de manifiesto la UNESCO en su Recomendación de 2021, ya citada. No obstante lo anterior, recientemente una aplicación de IA utilizada para mantener conversaciones de amistad o incluso de pareja (*Replika*), ha sido denunciada por posible acoso sexual a algunos usuarios, puesto que enviaba tanto mensajes como imágenes de tal carácter. Lo que sucede es que el algoritmo aprende los patrones y el modo de actuar que tienen los individuos con él, por lo que en este caso se estaría cerca de que el instrumento fuera capaz de adquirir autónomamente guías de actuación no incluidas por los programadores en el momento del diseño.

2. SISTEMAS INTELIGENTES EN MATERIA DE PREVENCIÓN Y DETECCIÓN DEL DELITO

Son múltiples los ámbitos, tanto públicos como privados, en los que se utiliza la IA: sanitario, educativo, sistemas electorales, mercado la-

²² AARVIK, P. (2019). *Artificial Intelligence-a promising anti-corruption tool in development settings?*, U4. Anti-corruption Resource Centre, Chr. Michelsen Institute, pág. 1.

²³ COMISIÓN EUROPEA. (2020). *Libro Blanco sobre Inteligencia Artificial-un enfoque europeo orientado a la excelencia y la confianza*. COM(2020) 65 final, pág. 20.

²⁴ MIRÓ LLINARES, F. (2018). "Inteligencia Artificial y justicia penal: Más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología*, 3ª Época, nº. 20, pág. 93.

boral, publicidad, etc.²⁵. El del Derecho y, especialmente el Penal, como no podía ser de otro modo, no se mantiene ajeno a esta nueva realidad. La aplicación de sistemas inteligentes en este entorno se da en distintos momentos. Así, vinculado a la temática del presente trabajo, a nivel preventivo de la delincuencia o *predictive policing*²⁶; y en el sistema judicial, incluso en el momento en el que se dicta sentencia²⁷. Sobre esto último, a modo ejemplificativo, destacamos que el pasado 30 de enero de 2023 se emitió la primera sentencia usando el ChatGPT en la Corte Constitucional colombiana. El Juez encargado del caso, Juan Manuel Padilla, introdujo en el sistema diversas preguntas que aquel respondía. La toma de decisiones judiciales utilizando IA no está exenta de debate y controversias, como se desprende de la Resolución del Parlamento Europeo de 6 de octubre de 2021, por las posibles conculcaciones a los derechos fundamentales del encausado. Aunque esta cuestión es de suma relevancia, no se profundizará más en la misma, en tanto se escapa en mucho de nuestro objeto de estudio, no obstante, sirve para contextualizar la situación de la IA en el ámbito jurídico. Volviendo nuevamente al asunto que aquí compete, en relación a la predicción de delitos, la IA aparece como una herramienta que permite mejorar la eficacia en la lucha contra el crimen y las amenazas que afectan al Estado²⁸. La implementación de sistemas de tal índole tiene distintos fines, como son la prevención, la evaluación de la peligrosidad individual y la determinación de la posibilidad de reincidencia. En vista de las características y consecuencias del fenómeno delictivo abordado a nivel social y económico (véase, *supra*, el apartado primero de la presente investigación), interesa sobre todo el primero de los mencionados.

La idea de poder predecir y prevenir el delito antes de que ocurra suscita gran interés. Con tal finalidad, se han usado muchas técnicas a lo lar-

²⁵ VALLS PRIETO, J. *Inteligencia Artificial, derechos humanos...*, cit., págs. 25 y ss.

²⁶ Véase, en este sentido, entre otros, ALONSO SALGADO, C. (2021). "Acerca de la inteligencia artificial en el ámbito penal: especial referencia a la actividad de las fuerzas y cuerpos de seguridad", *Ius et Scientia*, vol. 7, n.º. 1, págs. 25-36; y DOMINGO JARAMILLO, C. (2021). "Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana", *El Criminalista Digital. Papeles de Criminología*. 2ª Época, n.º. 9, págs. 20-37.

²⁷ *Vid.*, Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la Inteligencia Artificial en el Derecho Penal y su utilización por las autoridades policiales y judiciales en asuntos penales.

²⁸ VALLS PRIETO, J. *Inteligencia Artificial, derechos humanos...*, cit., pág. 32; y PATIÑO, C.A. (2021). "La Policía Predictiva como estrategia de inteligencia para la disuasión de eventos delictivos", en *Inteligencia Artificial y Ética en la Gestión Pública*, CLAD, Venezuela, págs. 209 y ss.

go del tiempo. Los primeros métodos incluían puramente aproximaciones estadísticas de predicción a través del perfilado individual, centradas en determinar las características personales, las conexiones sociales y otros datos sobre el comportamiento del sujeto. Un segundo conjunto de métodos se centra en la agrupación espacial de la actividad delictiva y lleva a identificar *hotspots* (o puntos calientes), es decir, zonas donde se acumula mayor número de delitos. Las nuevas técnicas, por el contrario, han permitido pasar de la vigilancia de semejantes puntos calientes a la acción predictiva, es decir, a la identificación de objetivos policiales para prevenir o resolver crímenes pasados a través de predicciones estadísticas²⁹. Estas últimas son de gran utilidad, en tanto agilizan la labor de investigación y detección de posibles ilícitos, lo cual se ha venido a denominar *predictive policing*³⁰. Existen ya múltiples herramientas en este sentido. Por poner tan solo algunos ejemplos, en EE.UU se utilizan entre otras, PredPol que analiza zonas geográficas con elevados índices de delincuencia. A través de datos policiales examina dónde hay mayor probabilidad de que se produzcan determinados delitos; *Strategic Subject List*, centrada en datos de personas y no geográficos, pretende determinar la posibilidad de que un individuo cometa un delito con armas, pero el resultado no ha sido el deseado, porque en lugar de prevenir su comisión, ha aumentado la población carcelaria. En nuestro país también se han implementado programas similares, como VinPol, Appolo, VeriPol y VioGen³¹.

El éxito de todos ellos depende en gran medida de la calidad y diversidad de los datos con los que han sido entrenados, pudiendo producirse sesgos que causen problemas de discriminación. Hay que tener en cuenta que la forma en la que se recolectan y clasifican los datos es una cuestión sociocultural, de lo cual pueden derivarse los susodichos sesgos en las decisiones adoptadas por el algoritmo. De forma que si la misma máquina se expone a distintos conjuntos de datos, aquellos pueden reducirse pero no suprimirse completamente³². Por tanto, para obtener predicciones lo más certeras posible, hay que entrenar al algoritmo con datos suficientes y adecuados a la población a la que se destina. Los riesgos de sesgo son

²⁹ DE BLASIO, G., D'IGNAZIO, A., y LETTA, M. (2020). *Predicting Corruption Crimes with Machine Learning. A Study for the Italian Municipalities*, Working Papers Series, Dipartimento di Scienze Social and Economiche, Sapienza Università di Roma, n.º. 16, págs. 4-5.

³⁰ *Ibd.*, pág. 2; y MIRÓ LLINARES, F. "Inteligencia Artificial y justicia penal...", cit., pág. 100.

³¹ DE BLASIO, G., D'IGNAZIO, A., y LETTA, M. *Predicting Corruption Crimes with Machine Learning...*, cit., pág. 33.

³² COMEST. *Preliminary Study on the Ethics of Artificial Intelligence...*, cit., pág. 7.

fundamentalmente tres: 1) que los datos hayan sido erróneamente calificados por el programador, lo cual viciaría el aprendizaje desde el inicio; 2) que el conjunto de datos provenga de un muestreo no representativo, reduciéndose así su validez y aumentando el error de la interpretación de los resultados; y 3) que los parámetros del aprendizaje se realicen sobre intervalos temporales muy acotados³³.

En vista de la utilidad que tiene la IA en cuanto a detección y prevención de la delincuencia a nivel general se refiere, en lo siguiente se analizará su aplicación en el ámbito de la corrupción, al erigirse como uno de los grandes problemas que afectan hoy día a la sociedad.

III. INTELIGENCIA ARTIFICIAL EN LA LUCHA CONTRA LA CORRUPCIÓN

1. CUESTIONES PREVIAS

Como se mencionó en el apartado primero de la presente investigación, la corrupción es un fenómeno ubicuo que aparece en todas las sociedades y, dadas las graves consecuencias que plantea, la lucha contra ella es uno de los retos más importantes a los que hacer frente actualmente, de modo que las políticas elaboradas con dicho fin se centran en la necesidad de abordar de forma efectiva la actividad anticorrupción³⁴. Entendemos que los esfuerzos en este sentido requieren la habilidad de predecir dónde es más probable que aparezca con el objetivo último de poder evitarla.

Desde hace unas décadas, la digitalización ha permitido, entre otras cuestiones, el aumento en el nivel de transparencia de la Administración Pública, el fortalecimiento del control público y la reducción de la burocratización. Por tal motivo, tanto las tecnologías digitales como los sistemas de IA se consideran herramientas útiles para combatir la corrupción a través de un mayor acceso a la información pública y el seguimiento de las actividades administrativas y gubernamentales, la digitalización de los servicios públicos y el ofrecimiento de oportunidades para denunciar los casos de corrupción³⁵. Específicamente, los sistemas inteligentes permi-

³³ MIRÓ LLINARES, F. "Inteligencia Artificial y justicia penal...", cit., págs. 122-123.

³⁴ COLONNELLI, E., GALLEGO, J., y PREM, M. (2019), "What predicts corruption?", *Serie de Documentos de Trabajo*, n.º. 228, Universidad del Rosario, pág. 1.

³⁵ SUROVICOVA, A., y otros. (2022). "Assessment of transmission effects between "corruption-digitization-economic growth", *Financial and Credit Activity: Problems of Theory and Practice*, vol. 3, n.º. 44, pág. 133.

ten identificar anomalías, establecer patrones y relaciones informales, así como minimizar el papel de las personas en la toma de decisiones³⁶, lo cual contribuye a disminuir las posibilidades de manifestaciones corruptas.

La particularidad de la IA respecto a otras nuevas tecnologías radica en su autonomía. Los algoritmos están capacitados para encontrar soluciones por sí mismos. Se espera que esto contribuya a incrementar los esfuerzos anticorrupción, lo cual cobra impulso a medida que la Administración Pública se vuelve cada vez más digital³⁷. No obstante, para ello se necesitan datos, los cuales están aumentando considerablemente por el uso creciente de los sistemas digitales³⁸. En tal línea, la ventaja que presenta la IA es que los humanos no pueden analizar la inmensidad de información existente, mientras que los algoritmos de los mecanismos inteligentes pueden hacer inferencias analizando, modelando y visualizando dinámicamente esos datos. Así las cosas, la IA puede tomar decisiones sobre los riesgos de corrupción basadas en el *Big Data*³⁹, sin necesidad de intervención humana.

Varios instrumentos de IA y *machine learning* se han puesto ya en marcha con el fin indicado⁴⁰. Incluso agencias anticorrupción han introducido este tipo de técnicas, como Transparencia Internacional de Reino Unido que las utiliza para automatizar búsquedas en registros públicos y fortalecer su capacidad analítica. En España destaca el proyecto llevado a cabo por López Iturriaga y Pastor Sanz, quienes han diseñado un sistema basado en redes neuronales para predecir la corrupción pública en las distintas provincias de nuestro país⁴¹, cuyos resultados son prometedores. Otros ejemplos reseñables se encuentran en México y Ucrania. En el primero

³⁶ *Ibd.*, p. 135.

³⁷ KOBIS, N., STARKE, C., y RAHWAN, I. (2021). "Artificial Intelligence as an Anti-Corruption Tool (AI-AC): Potentials and Pitfalls for Top-Down and Bottom-Up Approaches", *ArXiv*, 2102. 11567, pág. 5.

³⁸ VALLS PRIETO, J. (2017). *Problemas jurídico-penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante Inteligencia Artificial*, Dykinson, Madrid, pág. 9. El autor expone que en el año 2012 se crearon 2,72 zettabytes y se esperaba que dicha cantidad se doblase en dos años. Sin embargo, se superó ampliamente esa previsión.

³⁹ KOBIS, N., STARKE, C., y RAHWAN, I. "Artificial Intelligence as an Anti-Corruption Tool...", cit., pág. 6.

⁴⁰ Véase, a modo ejemplificativo, BARBOSA JAIME, J.C. (2023). "El papel de la Inteligencia Artificial en la lucha contra la corrupción", en Carrillo del Teso, A.E., y Pahul Robredo, G. (Dirs.), *La lucha contra la corrupción: gestión de riesgos y paradigmas globales*, Colex, A Coruña, págs. 135-138.

⁴¹ LÓPEZ ITURRIAGA, F.J., y PASTOR SANZ, I. (2017). "Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces", *Social Indicators Research*, n.º. 140, págs. 975 y ss.

se aplican herramientas digitales e IA en proyectos piloto para detectar el fraude y las evasiones fiscales en la contratación pública. El Instituto Mexicano para la Competitividad junto a la Inteligencia Participativa utilizó consultas automatizadas en millones de registros de datos para analizar los procedimientos de contratación del Gobierno para identificar los riesgos de corrupción⁴². Por su parte, Ucrania, a través del sistema abierto de contratación electrónica PROZORRO, identifica licitaciones con alto riesgo de corrupción. Mediante unos indicadores determinados, el programa es capaz de detectar ofertas o compras sospechosas de ser ilegales que se denuncian ante las autoridades competentes, mejorando la posición de Ucrania en los rankings internacionales anticorrupción⁴³.

A pesar de los grandes avances científicos y el interés por las organizaciones nacionales e internacionales en la cuestión, el impacto en el desarrollo de nuevas tecnologías para localizar los signos de corrupción pública y así prevenirla continúan estando poco estudiados. Así, en lo siguiente, se expondrán las dos principales iniciativas que hacen uso de la IA anticorrupción y, dentro de las mismas, los instrumentos concretos que, a nuestro juicio, son los más interesantes por los resultados obtenidos.

2. INICIATIVAS ANTICORRUPCIÓN SEGÚN EL AGENTE QUE LAS LLEVA A CABO

2.1. *Top-down*

En este caso, las instituciones gubernamentales son las que desarrollan la acción contra las actividades corruptas. Para ello, establecen nuevas regulaciones y procedimientos dentro de la Administración, introducen nuevas leyes o modifican las ya existentes. Los actores principales son investigadores criminales, fiscales anticorrupción, *compliance officers* y auditores⁴⁴, entre otros agentes que en el seno de las entidades públicas actúan firmemente contra las corruptelas.

Los sistemas de IA de tal índole presentan la ventaja de mejorar la eficiencia en comparación con los mecanismos manuales previos, en tanto permiten detectar de forma automática un posible incidente corrupto tras la revisión de un conjunto muy amplio de datos. Dicha tarea conllevaría mucho tiempo y esfuerzo si la ejecutase una persona, por lo que la IA en

⁴² AARVIK, P. *Artificial Intelligence-a promising anti-corruption tool in development settings?*..., cit., pág. 5.

⁴³ *Ibd.*, pág. 7.

⁴⁴ KOBIS, N., STARKE, C., y RAHWAN, I. "Artificial Intelligence as an Anti-Corruption Tool...", cit., pág. 9.

este ámbito aparece como una poderosa herramienta para aquellos que trabajan en la lucha contra la corrupción dentro de la Administración⁴⁵. De hecho, los sistemas de este tipo son muy utilizados en materia de detección de fraude, evaluación de riesgos y vigilancia predictiva. En relación con esto último y, a pesar de las bondades que presentan tales sistemas, con su uso se corre el peligro de un posible reforzamiento de las estructuras de poder existentes, lo cual lleva aparejados nuevos riesgos de corrupción, por cuanto quien ostenta el poder es el poseedor de los datos y puede hacer un uso fraudulento de los mismos.

La principal característica del *top-down* es la existencia de una infraestructura técnica de acceso y la agregación de datos sensibles combinados con poderosos algoritmos que permiten una vigilancia y control sin precedentes. Lo inmediatamente apuntado tiene el peligro de conducir al llamado efecto “gran hermano” donde se usa la IA para consolidar el poder y socavar las instituciones democráticas⁴⁶; y, aunque la IA anticorrupción se creó para mitigar el daño que esta lacra produce, como se viene señalando, se encuentra en manos de instituciones que ostentan sus propios intereses. De modo que, según aumenta el uso de aplicaciones inteligentes, lo hace también el riesgo de que los algoritmos se utilicen intencionadamente con fines de manipulación, censura o discriminación⁴⁷. Por ese motivo, consideramos que la implantación de semejantes técnicas en las instituciones, debe ir acompañada de garantías de buen uso y alejar en lo posible la acción humana del control y gestión de los datos.

Una experiencia de este tipo fue la puesta en marcha en Brasil para predecir la corrupción de la Administración local con los datos presupuestarios municipales desde el año 2001 hasta 2012. El análisis se centró en una variable binaria que identificaba lo que los desarrolladores consideran pequeña corrupción (p.ej., adquisiciones ilegales, fraude o favoritismo). La matriz X contenía las características del presupuesto mientras que en la Y se definieron a nivel de municipio-año los periodos sujetos a auditoría. Los años en los que se apreciaba corrupción se incluyeron como 1 y 0 los que no. Con esta información, para alcanzar el objetivo planteado, se entrenó el sistema de IA para que fuese capaz de proporcionar la probabilidad de que una localidad fuese corrupta basándose en las características presupuestarias obtenidas de los datos pú-

⁴⁵ *Ibd.*, págs. 6-7.

⁴⁶ KOBIS, N., STARKE, C., y RAHWAN, I. (2022). “The promise and perils of using Artificial Intelligence to fight corruption”, *Nature Machine Intelligence*, n.º. 4, págs. 6-7.

⁴⁷ AARVIK, P. *Artificial Intelligence-a promising anti-corruption tool in development settings?*..., cit., pág. 25.

blicos. Los programadores no tuvieron en consideración los elementos demográficos, porque observaron que aquellos son más eficaces en este caso. Determinaron las categorías más relevantes para identificar la corrupción, siendo aquellas que se refieren a los gastos y tasas de agricultura, servicios públicos, transporte y las acciones legislativas del Gobierno local; otras señales específicas provenían de la arbitrariedad en el uso de fondos públicos en situaciones que son más difíciles de monitorizar. El modelo atendía la presencia de déficit presupuestario y superávit o, lo que es lo mismo, la unión entre corrupción pública y deuda.

Una contribución decisiva del mecanismo de IA presentado es la capacidad de medir la corrupción de todos los municipios brasileños. Los resultados a los que se llegó mostraron que el 42% de las localidades auditadas presentaban algún tipo de corrupción. No solo eso, sino que además fue capaz de predecir la corrupción en las localidades que no se sometieron a auditoría. Por las conclusiones extraídas, el sistema tuvo una gran repercusión política, al barajarse la posibilidad de introducir sistemas de auditorías periódicas a nivel municipal, lo cual se entendía que contribuiría a reducir la corrupción. El problema que plantea esto es que tras la primera auditoría, cabía la posibilidad de que las cuentas presupuestarias contuvieran menos información sobre corrupción o que la misma estuviera manipulada. Por ese motivo, los encargados de la puesta en marcha del mecanismo sostienen que sería más efectiva la introducción de un sistema de auditorías mixto, es decir, planificadas con el mantenimiento de algunas aleatorias, porque aquellas sirven para detectar y disuadir la corrupción en los municipios con riesgo elevado, mientras que las aleatorias coadyuvarían a la disuasión incluso en los municipios con riesgo bajo y servirían para alterar los parámetros del algoritmo dirigiendo la siguiente ronda de auditorías guiadas hacia las localidades de las que se tuviera sospecha de una posible acción corrupta por parte de los agentes de la Administración⁴⁸.

Otro estudio similar, esta vez llevado a cabo en Italia, arrojó resultados parecidos. Los investigadores utilizaron la técnica de árboles de decisión para predecir y prevenir el delito antes de que tuviera lugar a fin

⁴⁸ Véase, más ampliamente, ELLIOT A., GALLETTA, S., y GIOMMONI, T. (2021). "A Machine Learning Approach to Analyze and Support Anti-Corruption Policy", *CESIFO Working Paper*, n.º. 9015, Center for Economic Studies and Ifo Institute, Munich, págs. 1 y ss. A resultados similares llegaron años antes COLONNELLI, E., GALLEGO, J., y PREM, M. "What predicts corruption?...", cit., págs. 1 y ss., cuyo estudio se centró igualmente en la realización de auditorías aleatorias en los municipios brasileños, considerando los datos proporcionados por la Agencia Federal Anticorrupción.

de reducir la criminalidad y usar los recursos públicos de forma más eficiente. Para ello, se utilizaron los datos del *Sistema d'Indagine* y los archivos del Ministerio del Interior italiano que contienen registros de todos los ilícitos cometidos en el territorio nacional a nivel local. Dependiendo de la variable de resultado, concluyeron que el sistema es capaz de predecir entre el 70 y el 80% de la corrupción en este ámbito. El pronóstico depende de los valores de algunas variables, principalmente de las referidas a las características de los mercados laborales y de viviendas locales, así como el historial previo de delitos de cuello blanco⁴⁹.

En vista de los buenos resultados que arroja la investigación sobre la introducción de algoritmos de IA basados en las técnicas *top-down*, puede concluirse la relevancia que tienen para predecir la corrupción en el seno de la Administración Pública, puesto que incluso con una lista no muy extensa de elementos susceptibles de análisis, los beneficios son importantes⁵⁰. No obstante, todo va a depender de la calidad de los datos y los sesgos que contengan, los cuales pueden provenir de los propios gestores de la información, por lo que habría de ser cautelosos a la hora de otorgar credibilidad absoluta a los resultados obtenidos por el sistema.

2.2. *Bottom-up*

Dado que, como acabamos de apuntar, puede suceder que aquellos que ostentan el acceso y control a los datos públicos podrían tener alguna intención espuria y los intentasen ocultar o manipular para que las corruptelas no sean descubiertas, las iniciativas *bottom-up* aparecen como una importante alternativa a las basadas en *top-down*⁵¹. Tanto es así que desde la Comisión Europea, específicamente desde el Servicio de información Comunitario sobre Investigación y Desarrollo (CORDIS), se están desarrollando importantes proyectos que ponen en práctica mecanismos basados en aquellas haciendo uso de las nuevas tecnologías, otorgando capacidad de actuación a la población. Como ejemplo, véase "*bottom-up initiatives and anti-corruption technologies: how citizens use ICTs to fight corruption*", que comenzó el 1 de julio de 2019 y está previsto que se desarrolle hasta el 31 de diciembre de 2024⁵².

⁴⁹ DE BLASIO, G., D'IGNAZIO, A., y LETTA, M. *Predicting Corruption Crimes with Machine Learning...*, cit., págs. 2 y ss.

⁵⁰ *Ibd.*, pág. 15.

⁵¹ KOBIS, N., STARKE, C., y RAHWAN, I. "The promise and perils of using Artificial Intelligence to fight corruption...", cit., pág. 8.

⁵² CORDIS, s.f., *bottom-up initiatives and anti-corruption technologies: how citizens use ICTs to fight corruption*. Recurso electrónico obtenido a través de la Web: <https://>

En este caso, es la sociedad civil la que toma el testigo en la lucha anticorrupción, buscando reducir las oportunidades corruptas analizando el contexto socio-cultural y apoyando los esfuerzos de las organizaciones sociales, ONG's y el periodismo de investigación. Este sistema permite a los ciudadanos organizarse mejor y ejercer mayor control sobre el Gobierno⁵³. De forma que, en lugar de que este último asuma el papel de vigía que vela por la ciudadanía, es la acción social la que actúa para revisar su actividad.

El principal inconveniente que plantean estas iniciativas es en relación al medio de obtención de los datos con los que se entrena el algoritmo. En dicha línea, debe tenerse en cuenta que los mismos provienen mayoritariamente de los que hace públicos la Administración y, aunque se están digitalizando cada vez más, muchos quedan sin revelar o, en caso de que estén publicados, no se les da la difusión suficiente. Por ese motivo, se achaca a las iniciativas *bottom-up* que no sean capaces de desarrollar todo su potencial⁵⁴. No solo eso, sino que han de llegar a la ciudadanía y demás instituciones implicadas en la lucha anticorrupción para que sean efectivas y, en muchas ocasiones, esto no sucede.

En otro orden de cosas, es esencial la fuente de datos a utilizar, que puede provenir, como acaba de indicarse, de su publicación por parte del propio Gobierno o de una fuga de datos como ocurre en el caso de *Wikileaks*, de iniciativas *crowdsourcing* y de información ofrecida por los medios de comunicación.

2.2.1. Sistema DOZORRO en Ucrania

Este proyecto utiliza datos proporcionados por la Administración aunque la acción proviene de la ciudadanía. El germen de la iniciativa

cordis.europa.eu/project/id/802362/results, [consultado el día 24 de enero de 2023]. La Unión Europea es muy activa en la lucha contra el fraude y la corrupción y ya desde el año 2004 desarrolla el programa Hércules. Véase el Reglamento (UE) 2021/785 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Programa de la Unión contra el Fraude y se deroga el Reglamento (UE) n.º 250/2014. En relación a dicho programa, RABUZIN, K., y MODRUSAN, N. (2019). "Prediction of Public Procurement Corruption Indices using Machine Learning Methods", *Proceedings of the 11th International Joint Conference on Knowledge Management*, pág. 333. Estos últimos entienden que el citado programa contribuye a aumentar la cooperación internacional y la coordinación a nivel comunitario entre los Estados Miembros de la UE y la OLAF, mejorando la competitividad de la economía de la región y asegurando la protección del dinero de los contribuyentes.

⁵³ KOBIS, N., STARKE, C., y RAHWAN, I. "The promise and perils of using Artificial Intelligence to fight corruption...", cit., pág. 8.

⁵⁴ *Ibd.*, pág. 9.

surge con la creación del Portal de Contratación Pública PROZORRO, instigado por Transparencia Internacional Ucrania, que pretendía crear un ecosistema de múltiples componentes. La plataforma permitió acortar el cuello de botella por corrupción y el ahorro a la economía nacional de 2.500 millones de dólares en tan solo tres años⁵⁵.

Antes de su puesta en marcha no existía una base de datos generalizada de violaciones en la contratación del país, por lo que no había estadísticas. La información de las acciones relativas a esta cuestión estaba dispersa puesto que permanecía, como suele ocurrir, en documentos oficiales no digitalizados o se publicaba en las páginas web de las agencias de supervisión, lo cual favorecía el olvido rápido de la información porque no se recogía en un único lugar. Así, un grupo de voluntarios apoyados tanto por empresas como por las autoridades del país lanzaron un sistema piloto de contrataciones electrónicas que se oficializó en agosto de 2016, momento a partir del cual cada contrato público debía subirse al portal, donde se incluyen todas las fases por las que pasa. De modo que el principal logro estriba en la introducción de máxima transparencia y acceso a la información en el ámbito de la contratación. En tal línea, uno de los fundamentos esenciales del programa es “todo el mundo ve todo”. Los resultados son alentadores porque la publicación de datos abiertos ha permitido a la sociedad cambiar completamente la aproximación al monitoreo de la contratación y aumentar significativamente su eficacia⁵⁶.

Unos meses después del lanzamiento oficial de PROZORRO, la sociedad presentó una nueva forma de monitorizar la contratación pública integrada completamente en el anterior, denominada DOZORRO, que consiste en una plataforma de comentarios de extremo a extremo para introducir y reaccionar a las violaciones en el sector de la contratación, con el objetivo de dar voz a aquellos cuyos derechos están siendo violados, ya sea un contribuyente o una empresa afectada por una contratación fraudulenta⁵⁷. La finalidad es unir a los defensores de la asignación efectiva de dinero público para garantizar el cumplimiento de reglas equitativas en la contratación pública y el mejor valor para los bienes, servicios y obras realizadas en beneficio de la ciudadanía⁵⁸. Se registran

⁵⁵ OPSI. (s.f). *DOZORRO*. Recurso electrónico obtenido de la Web: oecd-opsi.org/innovations/dozorro, [consultado el día 19 de marzo de 2023].

⁵⁶ OECD-OPSI. (2019). *Dozorro Story. From an idea of a Platform to the Biggest Monitoring Community in Ukraine*. Recurso electrónico obtenido a través de la Web: oecd-opsi.org/wp-content/uploads/2019/04/DOZORRO-STORY-ENG.pdf, [consultado el día 21 de marzo de 2023], pág. 7.

⁵⁷ OPSI. *DOZORRO...*, cit.

⁵⁸ *Ibd.*

todas las acciones y los usuarios del portal pueden analizar cómo trabaja una determinada entidad.

Concluida la prueba piloto, se verificó la viabilidad del sistema. En el primer mes se procesaron más de ochocientas contrataciones, lo que vino a permitir la detección de las infracciones más comunes en el país, cuáles eran las agencias de supervisión que trabajaban de forma efectiva y aquellas que no, las estructuras que intentaban hacer sus contrataciones más eficientes y reaccionar a los errores o violaciones rápidamente. En vista de tales resultados positivos, aquel se oficializó. Los agentes implicados son muy diversos e incluyen activistas sociales, periodistas de investigación, autoridades, entidades contratantes, agentes del Gobierno e investigadores⁵⁹.

El sistema cuenta con unos indicadores de buenas prácticas y de riesgo. Con estos últimos se desarrolló el mecanismo de IA y *machine learning* para detectar de forma automática las acciones fraudulentas. El entrenamiento de la red neuronal se llevó a cabo por expertos que definieron las prioridades de diversas combinaciones de factores de riesgo que consideraron esenciales para dicha tarea. Una de las ventajas que presenta es que no es un sistema de fórmulas predeterminadas, lo que permite su ajuste automático cuando aparezcan nuevos elementos sospechosos⁶⁰. De modo que DOZORRO es capaz de calcular el peso relativo de factores de riesgo de millones de procedimientos de contrataciones incluidos en la plataforma virtual, teniendo en cuenta y adaptando sus predicciones a aquellos elementos que inicialmente no fueron considerados perniciosos. El sistema está diseñado actualmente para realizar diagnósticos posteriores, es decir, una vez el ilícito se ha consumado. Sin embargo, uno de los retos que se plantean los desarrolladores es que pueda usarse de forma preventiva para detectar errores y violaciones antes de que tengan lugar⁶¹. Con ello, las empresas contratantes podrán eliminar los potenciales problemas en el momento y de forma más precisa e, igualmente, serán capaces de elegir los procedimientos menos cuestionables.

Los desarrolladores del programa concluyeron que la publicación de los datos contribuyó a aumentar la concienciación ciudadana, lo cual tiene un efecto positivo, puesto que cuando la población secunda la acción, se producen mayores cambios y reacciones más rápidas frente a las vio-

⁵⁹ OECD-OPSI. *Dozorro Story. From an idea of a Platform to the Biggest Monitoring Community in Ukraine...*, cit., págs. 4 y 12-13.

⁶⁰ AARVIK, P. *Artificial Intelligence-a promising anti-corruption tool in development settings?*..., cit., pág. 7.

⁶¹ *Ibd.*, pág. 19; y OECDE-OPSI. *DOZORRO...*, cit.

laciones⁶². Sin embargo, ha de tenerse en cuenta que la accesibilidad a los datos abiertos no aumenta necesariamente el nivel de confianza en las instituciones públicas, puesto que aquellos deben llegar a la ciudadanía. En semejante sentido, una de las cuestiones positivas de la iniciativa expuesta es la implicación de la sociedad, al ser la población civil uno de los agentes decisivos para la viabilidad del proyecto. Junto a lo anterior, otro aspecto favorable es que no requiere de intervención personal a la hora de detectar una eventual acción corrupta en la contratación pública. Esta afirmación trae causa del hecho de que antes de que comenzase a funcionar DOZORRO, el Servicio de Auditoría Estatal ucraniano había desarrollado 35 indicadores de riesgo para ayudar a evaluar qué ofertas necesitaban ser inspeccionadas. El problema surgía una vez se conocían tales indicadores, puesto que las empresas fraudulentas tomaban medidas para evitar las auditorías⁶³. Así las cosas, el hecho de que el mecanismo sea capaz de adaptarse a nuevas fórmulas y combinaciones de elementos sospechosos, permite evitar que sea manipulado, aumentando con ello su eficacia.

En vista de los grandes resultados obtenidos hasta el momento y la capacidad de detección automática del sistema, implicando a todos los agentes interesados, esta iniciativa pionera desarrollada en Ucrania aparece con la esperanza de potenciar la prevención de la corrupción, al menos en el sector en el que se implantó. En tal línea, consideramos que sería de gran utilidad su extensión hacia otras actividades no vinculadas con la contratación pública.

2.2.2. Botivist

Otro mecanismo significativo en la lucha contra la corrupción es botivist. Este sistema de IA utiliza bots, entendidos como agentes autónomos que juegan un papel importante en la comunicación colectiva online⁶⁴, con el fin de fomentar la participación ciudadana. En esta ocasión, la iniciativa partió de activistas anticorrupción latinoamericanos que pretendían reclutar nuevos voluntarios para que se uniesen a la causa reportando, por ejemplo, casos de corrupción a nivel local, a través de la red

⁶² OECD-OPSI. *Dozorro Story. From an idea of a Platform to the Biggest Monitoring Community in Ukraine...*, cit., pág. 23.

⁶³ AARVIK, P. *Artificial Intelligence-a promising anti-corruption tool in development settings?*..., cit., p. 7.

⁶⁴ YOUNG, A., SELANDER, L., y VAAST, E. (2019). "Digital Organization for Social Impact: Current Insights and Future Research Avenues on Collective Action, Social Movements, and Digital Technologies", *Information and Organization*, n.º. 29, pág. 3.

social twitter⁶⁵. En semejante línea, debe destacarse el papel fundamental que tienen las aplicaciones virtuales hoy día, pues su auge, la creciente accesibilidad y la actual dependencia a las mismas favorecen la implicación de muchas personas en acciones del estilo, teniendo la ventaja de conllevar menores costes de participación y el fomento de nuevos canales de información⁶⁶. En tal sentido, compartir información es fundamental para el éxito de acciones coordinadas y colectivas semejantes, motivo por el que las redes sociales aparecen como instrumentos eficaces al fin planteado, en tanto los flujos de información son capaces de traspasar las barreras tradicionales y tener incluso alcance internacional.

Volviendo de nuevo a botivist y la forma en la que se puso en marcha, indicar que en una fase inicial, un grupo de activistas definió el problema social para el que buscaban nuevos voluntarios, la corrupción. Una vez concretado, los bots se entrenaron para identificar a los potenciales voluntarios que fueron escogidos por los términos que utilizaban cuando publicaban un tweet, por lo que tenían en cuenta aquellos usuarios de la red social que hacían uso de conceptos sobre corrupción y activismo. Una vez seleccionados, la herramienta los mencionaba en un tweet⁶⁷ utilizando distintas estrategias para lograr una mayor participación: directa, solidaria, ganancia y pérdida. En la primera se hacen preguntas directas para encontrar la solución al problema planteado; en la segunda se apela a sentimientos de solidaridad y empatía; desde la tercera se llama a la acción con incentivos de cualquier tipo que los voluntarios recibirían en caso de participar; y, por último, la basada en la pérdida, incluye un posible perjuicio que sufriría el usuario si decidiese no participar, siendo la más efectiva la directa⁶⁸.

Los resultados son bastante positivos, puesto que la amplia mayoría de los usuarios, concretamente el 81%, respondieron a la llamada de botivist, aportando propuestas relevantes y comenzaron a interactuar y colaborar entre ellos. En total, al momento en el que se hicieron públi-

⁶⁵ SAVAGE, S., MONROY-HERNÁNDEZ, A., y HOLLERER, T. (2016). "Botivist: Calling Volunteers to Action Using Online Bots", *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*, vol. 27, pág. 813.

⁶⁶ YOUNG, A., SELANDER, L., y VAAST, E. "Digital Organization for Social Impact...", cit., págs. 2-3.

⁶⁷ WOLLEY, S., y KUMLEBEN, M. (2020). "Social Bots for Peace: Combating Automated Control with Automated Civic Engagement?", *Social Media as a Space for Peace Education. The Pedagogic Potential of Online Network*, Palgrave Macmillan, Suiza, pág. 214.

⁶⁸ SAVAGE, S., MONROY-HERNÁNDEZ, A., y HOLLERER, T. "Botivist: Calling Volunteers to Action Using Online Bots...", cit., pág. 814.

cos los resultados, 175 voluntarios respondieron e hicieron más de 1.200 contribuciones. Esta elevada tasa de respuesta si se compara con otras técnicas de comunicación, sugiere que dichos mecanismos podrían ser productivos para ayudar a los activistas anticorrupción a reclutar voluntarios y así fomentar la lucha contra esta lacra social.

2.2.3. Experiencia en España con mapas auto-organizados

Las redes neuronales son algoritmos de aprendizaje de los que se infieren patrones de un amplio volumen de ejemplos. Son capaces de predecir y descubrir relaciones ocultas de forma rápida y económica, lo cual los hace valiosos en la formulación e implementación de políticas. Por su parte, los mapas auto-organizados (SOMs) son una red neuronal de la que pueden extraerse pautas de conducta de un amplio conjunto de datos que permiten su visualización gráfica para predecir la corrupción⁶⁹.

En nuestro país se han desarrollado sistemas de IA en materia de detección y prevención de la corrupción basados en esta técnica de mapas auto-organizados. Resalta el modelo puesto en marcha por López Iturriaga y Pastor Sanz, quienes ofrecen un mecanismo de predicción de la corrupción basado en factores económicos. En este caso, los datos que utilizaron provenían de un medio de comunicación, pues se sirvieron de la base de datos creada por el diario *El Mundo*, que contiene información sobre todos aquellos ilícitos en los que estaba implicado un político o funcionario público español desde el año 2000 hasta el 2012, pudiendo haber recaído ya sentencia o estar esperando el veredicto. Es especialmente significativo el periodo de estudio escogido, dado que entre los años 2007 y 2012 España estuvo sumida en una gran crisis económica, aplicándose medidas para reducir el gasto público y el déficit y durante la cual, afloraron distintos casos de corrupción que provocaron una gran alarma y rechazo social (p.ej., casos Andrach, Astapa, ERES en Andalucía, entre otros). Los investigadores proponen un modelo de alerta temprana de la corrupción para predecir si es probable que aparezca en alguna de las provincias españolas en un horizonte temporal de hasta tres años, dados ciertos determinantes económicos y políticos. Los más importantes

⁶⁹ ADAM, I., y FAZEKAS, M. "Are emerging technologies helping win the fight against corruption?...", cit., pág. 11. Para los autores en cita, el uso de mapas auto-organizados por parte de las autoridades públicas encargadas de combatir la corrupción les permitiría trabajar de forma más eficiente y efectiva, en tanto las tecnologías de IA podrían hacer la aplicación de la Ley más eficaz. Ello permitiría una focalización adecuada de los recursos.

son: la fiscalidad inmobiliaria, deuda per cápita, medidas del servicio de la deuda, crecimiento de las entidades de depósito, crecimiento poblacional, variación en el número de compañías registradas, aumento del precio de la vivienda, tasa de desempleo y su crecimiento, tiempo en el que un mismo partido se mantiene en el poder y Gobiernos en mayoría. Con estas variables, usaron tres mapas auto-organizados, que consisten en una aproximación de redes neuronales para predecir la corrupción en diferentes extensiones temporales. Observaron también que el número de casos de corrupción puede correlacionar con la población o la actividad económica de una región. Así, las de mayor tamaño serían proclives a más corrupción porque el número de políticos es superior. El modelo provee diversos perfiles de riesgo dependiendo del estado económico de una región condicionado al tiempo de predicción. El resultado es un mapa final o sistema de alerta temprana, tras la combinación de los tres SOMs. Estamos ante una herramienta visual que determina la probabilidad de que en una provincia exista alguna forma de corrupción. Lo esencial del modelo es que es capaz de generalizarse, es decir, implantarse en otros países con elevadas garantías de éxito, especialmente en aquellos que tienen problemas de corrupción más severa⁷⁰.

La eficacia de los árboles de redes neuronales se pone de manifiesto en otros estudios y mecanismos desarrollados fuera de nuestras fronteras. Así, el sistema *Random Forest*, que utiliza una serie de variables extraídas de distintas agencias como Transparencia Internacional⁷¹, es muy similar al desplegado en España y ha obtenido resultados muy positivos, en tanto es capaz de revelar predictores de la corrupción importantes y las relaciones complejas entre variables⁷².

Al igual que ocurría en la experiencia ucraniana, los desarrolladores del modelo de mapas auto-organizados en España entienden que la mejor forma de prevenir la corrupción es garantizando la transparencia y la digitalización de la información, haciéndola accesible a la ciudadanía, como responsable de llevar a cabo un conjunto de acciones para perseguir y castigar las actividades corruptas, principalmente las ejecutadas

⁷⁰ Véase, en mayor amplitud, LÓPEZ ITURRIAGA, F.J., y PASTOR SANZ, I. "Predicting Public Corruption...", cit., págs. 975 y ss.

⁷¹ MELO LIMA, M.S., y DELEN, D. "Predicting and explaining corruption across countries...", cit., pág. 3.

⁷² Entre otros, *ibid.*, p. 12; ELLIOT A., GALLETTA, S., y GIOMMONI, T. "A Machine Learning Approach to Analyze and Support Anti-Corruption Policy...", cit., págs. 1 y ss.; y UTOMO, V.G., y otros. (2021). "Analyze Corporate Anti-Corruption Disclosure with Feature Selection", *2021 International Seminar on Application for Technology of Information and Communication (iSemantic)*, págs. 234-237.

por los funcionarios⁷³. Hay otros elementos que han de tenerse en cuenta para que la IA sea efectiva, no estando exenta tampoco de controversias y problemas en su utilización. Por ese motivo, en el apartado siguiente se abordarán tales cuestiones.

IV. ELEMENTOS FUNDAMENTALES PARA LA UTILIZACIÓN DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL Y PROBLEMAS ASOCIADOS

1. DIGITALIZACIÓN, TRANSPARENCIA Y ACCESO A DATOS ABIERTOS

Como se desprende de lo expuesto hasta el momento, la IA revela un gran potencial en el ámbito de prevención de la corrupción, al ser capaz de predecir el riesgo de que tenga lugar sin necesidad de intervención humana en el proceso de toma de decisiones. Sin embargo, para garantizar la viabilidad de los sistemas, se requiere el acceso a los datos y que estos sean de calidad.

En tal sentido, la digitalización es fundamental para el buen funcionamiento de los sistemas de IA. Es la transición del mundo real al virtual y consiste en la introducción de tecnologías digitales en todas las esferas de la vida pública: desde la comunicación normal entre personas hasta el desarrollo de empresas de alta tecnología. La influencia de las nuevas técnicas de información y comunicación se considera un paso lógico en el desarrollo de la realidad legal y socio-política, llegando a ser uno (si no el que más) de los factores más importantes en el crecimiento económico de un país⁷⁴. El uso de medios digitales ayuda a crear canales de comunicación directos y más transparentes entre los funcionarios y la ciudadanía; además tiene impacto en la percepción de la corrupción, puesto que la población confía más en el Gobierno cuando tiene libre acceso a las TIC y a los datos publicados⁷⁵. No obstante, tanto la digitalización como el uso de las nuevas tecnologías pueden producir el efecto contrario, es decir, que se lleguen a utilizar con fines fraudulentos, de manipulación, censura o discriminación⁷⁶, a lo que se añaden los peligros que conllevan

⁷³ LÓPEZ ITURRIAGA, F.J., y PASTOR SANZ, I. "Predicting Public Corruption with Neural Networks...", cit., pág. 993.

⁷⁴ HALAI, A., y otros. (2021). "Digital Anti-Corruption Tools and Their Implementation in Various Legal Systems Around the World", *SHS Web of Conferences* 100, 03005, ISCSAI, pág. 2.

⁷⁵ *Ibd.*, p. 3.

⁷⁶ AARVIK, P. *Artificial Intelligence-a promising anti-corruption tool in development settings?*..., cit., pág. 25

los posibles *hackeos* y la adulteración a una escala tal que no es posible controlar, como sí ocurre con los documentos en papel. De modo que las redes criminales e incluso el Gobierno pueden hacer uso de tales mecanismos⁷⁷ con fines espurios.

A pesar de lo inmediatamente señalado, la digitalización de los procedimientos burocráticos se muestra como un instrumento capaz de reducir la corrupción, en tanto pone a disposición de la ciudadanía todos los datos relativos a una determinada actividad pública. Por otro lado, permite a los Estados establecer cuerpos efectivos anticorrupción y adaptarse a los requerimientos de la sociedad. A pesar de todo, la introducción de herramientas anticorrupción en el ámbito digital es imposible sin la apertura de los Gobiernos y el acceso libre a la red y a la información sobre las instituciones estatales, lo cual contribuiría al aumento de la confianza social en el Gobierno y mejoraría la calidad de los servicios públicos⁷⁸. En tal línea y, vinculada estrechamente con la digitalización, está la transparencia, crucial para reducir la corrupción, siendo uno de los métodos más importantes para garantizar el acceso a los datos abiertos⁷⁹ que permiten detectar, predecir y prevenir prácticas que en el pasado podrían haber quedado escondidas tras una cortina de opacidad de documentos físicos. En dicho sentido, la tecnología aparece como una aliada fiable de la población y de los Gobiernos que pretenden acabar con la corrupción porque, combinada con la política, puede cambiar el proceso de elaboración legislativa de la prestación de servicios públicos⁸⁰. Los datos abiertos pueden aumentar la transparencia del Gobierno al revelar información sobre adquisiciones presupuestarias, propiedad del terreno, educación y medicina, estadísticas delictivas, informes financieros de agencias gubernamentales y del Estado, contratos gubernamentales, contratación internacional, etc., lo cual desalentaría a aquellos que pretenden llevar a cabo alguna acción corrupta⁸¹. Portales como *Opentender* son fundamentales para el desarrollo de una cultura de datos abiertos que favorece una mayor transparencia, en este caso concreto, sobre las licitaciones en el ámbito europeo. Se basa en un sistema de mapas inte-

⁷⁷ MIRÓ LLINARES, F. "Inteligencia Artificial y justicia penal...", cit., pág. 103; ADAM, I., y FAZEKAS, M. "Are emerging technologies helping win the fight against corruption?...", cit., pág. 4; y HALAI y otros. "Digital Anti-Corruption Tools...", cit., pág. 6.

⁷⁸ HALAI y otros. "Digital Anti-Corruption Tools...", cit., pág. 6.

⁷⁹ PETHERAM, A. (2019). *The Next Generation of Anti-Corruption Tools: Big Data, Open Data & Artificial Intelligence*, Oxford Insights, Research Report, pág. 6.

⁸⁰ HALAI y otros, "Digital Anti-Corruption Tools...", cit., pág. 6.

⁸¹ PETHERAM, A. *The Next Generation of Anti-Corruption Tools...*, cit., pág. 8; y HALAI y otros, "Digital Anti-Corruption Tools...", cit., pág. 5.

ractivos, en los que se incluyen datos del total de licitaciones de un país, así como de los compradores y proveedores desde el año 2009 hasta la actualidad⁸². Este portal está vinculado al proyecto *Digiwhist* que desarrolla una comprensión extensiva de la corrupción en el sector público basado en las denominadas *red flags* o banderas rojas de la corrupción, entendidas como insumos dentro del proceso de adquisición que correlacionan con la corrupción, medida con la adjudicación recurrente de contratos en una empresa. Establecen relaciones de entrada-salida de dichos insumos que permiten identificar automáticamente el contrato correspondiente, la empresa beneficiaria del mismo y la cantidad de dinero público involucrada. El objetivo es aumentar la confianza en el Gobierno y mejorar la eficiencia del gasto público en Europa, a través de la recopilación, estructuración, análisis y amplia difusión sistemática de la información sobre la contratación pública y los mecanismos que aumentan la responsabilidad de los funcionarios. Además de *Opentenders*, *Digiwhist* está ligado al Observatorio de Legislación Europea en materia de Transparencia (*EuroPAM.eu*) y a un *software* de evaluación de riesgos⁸³. Sin embargo, la transparencia no solo ha de ir unida a los datos que el Gobierno hace públicos, sino también al funcionamiento de los sistemas de IA, tal como pone de manifiesto la ONU en la Recomendación sobre la Ética de la Inteligencia Artificial, puesto que la falta de la misma podría conducir a una toma de decisiones poco efectiva que conculcaría algunos derechos y libertades fundamentales. Por ello, en la citada Recomendación se establece la necesidad de que los individuos puedan acceder a las razones por las que se ha tomado una decisión que les afecta. Continúa alegando que una mayor transparencia contribuye, entre otras cosas, el escrutinio público que favorece el descenso de la corrupción y la discriminación.

2. ALGUNAS CONTROVERSIAS SOBRE EL USO DE SISTEMAS INTELIGENTES

La aplicación de la IA en la lucha contra la corrupción tiene ciertas restricciones determinadas por los principios clave del desarrollo de la IA en general. Principalmente, su uso no puede violar los derechos y las libertades fundamentales, debiendo garantizarse la seguridad de los datos⁸⁴. Los desarrolladores y programadores de los sistemas deben proteger la transparencia de sus algoritmos analíticos y prevenir posi-

⁸² <https://opentender.eu/start>.

⁸³ <http://digiwhist.eu/about-digiwhist/>.

⁸⁴ En este caso, no se profundizará en este punto, sino que en el presente apartado se hará una breve mención a algunos de los inconvenientes que pueden plantearse en la

bles violaciones a los susodichos derechos⁸⁵. Así, la necesidad de respetarlos a lo largo de todo el ciclo de vida del sistema de IA ya se puso de manifiesto en el año 2019 por parte del Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial, en las Directrices Éticas para una IA Fiable. Igualmente, la Comisión Europea se muestra comprometida con esta cuestión, lo cual pone de manifiesto en la Propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, de 21 de abril de 2021 (COM(2021) 206 final). En tal línea, destacar que uno de los requisitos para el buen uso de los mecanismos inteligentes es la fiabilidad, la cual se sustenta igualmente en el respeto a los mencionados derechos que proveen unos principios éticos para el adecuado funcionamiento de aquellos.

Para evitar que se deslegitimen los esfuerzos anticorrupción utilizando sistemas de IA, los Estados deben salvaguardar la privacidad de los individuos implicados que puede verse comprometida en el caso de que se produzca una fuga de datos⁸⁶; así como los demás derechos vinculados a la protección de datos personales, habiendo paralelamente de garantizar ante todo la transparencia y la promoción de datos abiertos, incluso mediante la creación de repositorios de libre acceso, al tiempo que se lleven a cabo campañas de sensibilización social que den a conocer a la ciudadanía la existencia de tales iniciativas.

La posible colisión entre los derechos y libertades con el uso de sistemas inteligentes tiene su origen, como se establece en el Libro Blanco de la Comisión sobre la Inteligencia Artificial, en los defectos existentes en el diseño general de los mismos o en el uso de datos sesgados que no han sido corregidos previamente⁸⁷. Los prejuicios y la discriminación son riesgos intrínsecos a cualquier actividad social y económica. Ha de tenerse en cuenta que el mecanismo está entrenado por personas, por lo que tanto la subjetividad como los errores pueden producirse. El problema aparece desde el momento en el que la técnica tiene efectos muy amplios y es capaz de afectar y discriminar a numerosos individuos sin que exis-

materia, puesto que esta labor escapa en mucho de nuestro objeto de estudio y daría para un estudio independiente y centrado exclusivamente en los mismos.

⁸⁵ VORONTOV, S., y otros. (2020). "The use of Artificial Intelligence to Combat Corruption", *Slovak Republic Media Education*, vol. 60, n.º. 4, pág. 758.

⁸⁶ KOBIS, N., STARKE, C., y RAHWAN, I. "Artificial Intelligence as an Anti-Corruption Tool...", cit., pág. 11.

⁸⁷ ADAM, I., y FAZEKAS, M. "Are emerging technologies helping win the fight against corruption?...", cit., pág. 11.

tan sistemas de control social como los que rigen la conducta humana. Como el entrenamiento de la IA depende de los datos, es fundamental la calidad de los mismos para garantizar un uso y desarrollo adecuado de aquella, teniendo presentes los criterios de validez y fiabilidad⁸⁸. Para lograr dicho objetivo, tal como pone de manifiesto la UNESCO en el Estudio Preliminar sobre la Ética de la Inteligencia Artificial, debe exponerse a la máquina a diversas bases de datos porque, aunque pueda parecer que los algoritmos son imparciales, objetivos y justos, no sucede así, motivo por el cual deben desarrollarse con bases de datos que sean lo más asépticas posible, es decir, que no estén sesgadas.

Así las cosas, si se salvan los indicados problemas (entre otros como la colisión con el derecho fundamental a la protección de datos de carácter personal o la privacidad) que pueden derivarse de la puesta en marcha de mecanismos de IA en la lucha contra la corrupción, aquellos aparecen como instrumentos útiles en este sentido y, podría legitimarse su uso en un Estado social y democrático de Derecho como el nuestro. Nos encontramos ante una herramienta capaz de detectar de forma temprana patrones de corrupción para prevenir un posible ilícito del estilo. No obstante, algunos autores identifican un optimismo tácito sobre su efectividad⁸⁹. Por la falta de abundante evidencia empírica, puesto que el estudio de la materia se encuentra en una fase inicial, su impacto real es muy difícil de evaluar; si bien creemos que es capaz de influir positivamente si contribuye de manera decisiva en los esfuerzos anticorrupción, respetando los principios y límites establecidos normativamente, en especial los derechos y libertades de la ciudadanía y no es utilizada por los individuos e instituciones en su propio beneficio o en el de terceros.

V. CONCLUSIONES

La aplicación de la IA en la lucha contra la corrupción aparece con grandes esperanzas de éxito, principalmente en cuanto a prevención de este ilícito se refiere. Si se tienen en cuenta los graves perjuicios que tiene a todos los niveles, unido a las serias dificultades que plantea su detección, sobre todo en el ámbito público, por la opacidad y oscurantismo que le caracterizan, los mecanismos basados en dichas técnicas aparecen

⁸⁸ KOBIS, N., STARKE, C., y RAHWAN, I. "Artificial Intelligence as an Anti-Corruption Tool...", cit., pág. 12.

⁸⁹ ADAM, I., y FAZEKAS, M. "Are emerging technologies helping win the fight against corruption?...", cit., pág. 12.

con la promesa de una mayor capacidad predictiva que permite, a la postre, prevenir las corruptelas antes incluso de que tengan lugar.

Los mecanismos analizados que se han puesto en marcha en este sentido arrojan resultados prometedores, en tanto son capaces de predecir actos corruptos futuros. A pesar de todo, se debe ser cautelosos a la hora de asumir completamente los resultados de los sistemas como veraces, porque en muchos casos pueden ser erróneos o poco fiables, pudiendo suceder que, especialmente en las iniciativas *top-down*, los datos con los que se entrene el algoritmo estén sesgados, desde el momento en el que los individuos encargados de los mismos pueden manipularlos en su propio beneficio. Por tal motivo, los sistemas basados en *bottom-up* se muestran más efectivos, al implicar decisivamente a la ciudadanía en la lucha anticorrupción, pues aquellos que ostentan algún cargo público se alejan de la gestión de los datos. Para que estos sean eficaces, se precisa que la información llegue a la población. Con el objetivo de que ello suceda, los datos deben recogerse en repositorios de libre acceso a los que se les dé la publicidad suficiente para que la población sea capaz de ejercer un control más eficaz en las acciones del Gobierno.

Una cuestión decisiva en este punto es la digitalización, fundamental para la viabilidad de los sistemas inteligentes en general y, más concretamente, en la lucha anticorrupción. Cuanta más información se encuentre disponible en plataformas virtuales, mayor control se tendrá sobre la actividad de los agentes públicos, en tanto se fomenta la transparencia. Esta última es esencial para prevenir la corrupción en la Administración, pues el hecho de que se conozcan todas las acciones de una determinada entidad, permite su supervisión de forma eficiente. Pero la transparencia no ha de afectar solamente a los datos públicos, porque los sistemas de IA también deben preservarla, puesto que es uno de los principios fundamentales para garantizar el éxito de los mismos. En dicha línea, la Inteligencia Artificial presenta multitud de controversias y algunos problemas que pueden derivarse de su aplicación, especialmente en materia de derechos y libertades esenciales (como la privacidad y la protección de datos personales, entre otros), que son susceptibles de conculcarse o verse limitados de gravedad. Por ese motivo, los individuos deben conocer que se ha tomado una decisión que les afecta utilizando un mecanismo inteligente y todos los elementos implicados en el proceso de toma de esa decisión. Por otro lado, a la hora de programar y entrenar el algoritmo, debe tenerse en consideración los documentos de las organizaciones internacionales y la normativa existente en la materia, que recogen una serie de principios y directrices éticas para su uso adecuado. Además,

deben reducirse los sesgos, utilizando bases de datos que sean lo más objetivas posible. Con ello las decisiones del instrumento serán más fiables, evitándose o, mejor dicho, reduciéndose los errores que pueden conducir a detecciones falsas.

A pesar de todo lo anterior, aún falta mucha investigación sobre el potencial que la IA tiene en materia anticorrupción, encontrándose actualmente en una primera fase, por lo que se precisan más estudios que permitan arrojar resultados determinantes sobre la viabilidad o no de su implementación para prevenir este tipo delictivo. Sin embargo, las conclusiones a las que llegan los proyectos que se han puesto en marcha hasta ahora son positivas y nos hacen pensar que, tal vez en un futuro no muy lejano, se generalice el uso de técnicas inteligentes con tal finalidad. Eso sí, para que ello tenga lugar, los diseños han de respetar los principios y garantías esenciales para su adecuado desempeño, teniendo siempre presentes los derechos y libertades ciudadanas que no han de conculcarse.