VIGILANCIA A TRAVÉS DE LA INTELIGENCIA ARTIFICIAL Y EL *BIG DATA:* RETOS Y OPORTUNIDADES PARA GARANTIZAR LOS DERECHOS HUMANOS

Oswaldo Rosalío Aguilar Rivera*

* Académico del Instituto Nacional de Ciencias Penales.

PALABRAS CLAVE *KEYWORDS*

Inteligencia artificial	*Artificial Intelligence*
Derechos humanos	*Human rights*
Macrodatos	*Big data*
Vigilancia	*Surveillance*
Víctimas	*Victims*

Resumen. La vigilancia a través de la inteligencia artificial y el *big data* se ha vuelto común. Diversos sistemas tecnológicos y digitales se han desarrollado de manera gradual, hasta superar los mecanismos de supervisión éticos y normativos para garantizar el respeto a los derechos humanos. En este artículo se exploran las tendencias del desarrollo, uso y vigilancia de las tecnologías de la información en materia de inteligencia artificial, para dar un diagnóstico desde un enfoque real y normativo. Se mostrarán los excesos, limitaciones y desafíos que enfrenta la vigilancia, así como la protección a los derechos humanos y la posible aparición de víctimas por violaciones a aquellos, a fin de coadyuvar al desarrollo de la investigación y la protección normativa de este fenómeno.

Abstract. Surveillance through artificial intelligence and big data has become common. Various technological and digital systems have been developed gradually, to overcome the ethical and regulatory supervision mechanisms to guarantee respect for human rights. This article explores the trends in the development, use and surveillance of information technologies in terms of artificial intelligence, to give a diagnosis from a real and normative approach. The excesses, limitations and challenges faced by surveillance will be shown, as well as the protection of human rights and the possible appearance of victims of human rights violations, to contribute to the development of the investigation and the normative protection of this phenomenon.

Fecha de recepción: 16 de enero de 2021
Fecha de aceptación: 12 de abril de 2021

SUMARIO:

I. COMPONENTES BÁSICOS DE LA IA: EL *BIG DATA*, ALGORITMOS, *MACHINE LEARNING*, *DEEP LEARNING* Y *BLACK BOX*

Para hablar de inteligencia artificial, hay que remontarse a sus inicios, cuando el hombre empezó a desarrollar tecnología en aras de mejorar procesos en busca de comodidad, ahorro de mano de obra y/o de recursos. Particular y desafortunadamente, la guerra siempre ha contribuido de manera rápida a implementar nuevas tecnologías para el combate y lo relacionado con él. En este rubro, puede mencionarse que, durante la Segunda Guerra Mundial, la máquina que inventó Alan Turing fue uno de los primeros artefactos de IA en utilizarse para descifrar códigos nazis. Funcionaba a través de un número finito de estados internos para realizar cualquier operación que estuviera representada mediante un algoritmo, y estos datos se almacenaban en una cinta bidireccional en forma de dos marcas, lo cual también creo un precedente no solo para los ordenadores que vendrían posteriormente, sino también para el *big data*.

Los *algoritmos* son el motor fundamental de esta tecnología: según la Real Academia Española, la palabra "algoritmo", del latín *algobarismus*, significa "conjunto ordenado y finito de operaciones que permite hallar la solución de un problema". En relación con la inteligencia artificial, estas operaciones se hacen posibles gracias a la cantidad de datos recolectados que pone en marcha este engranaje para resolver modelos complejos a partir de un problema determinado. De manera general, un algoritmo se compone de tres etapas: 1) datos de entrada; 2) un proceso lógico-formal; y 3) la solución

que se da según la problemática planteada. Así, podemos ejemplificar un algoritmo cuando un abogado espera la resolución de un asunto (dato de entrada); al notificarse, puede tomar distintos rumbos según sus intereses (proceso lógico-formal); y, si es abogado del imputado y la sentencia es condenatoria, hay una alta probabilidad de que interponga un recurso de apelación; y si, por el contrario, la sentencia es absolutoria, no promoverá recurso alguno (soluciones).

Estos procesos, que son comunes en la vida diaria, suelen ser recogidos por la inteligencia artificial, con el valor agregado de que, entre más complejo y más datos disponibles haya, sale de la esfera de resolución inmediata del hombre e ingresa en la de las máquinas, que son capaces de resolver en cuestión de segundos.

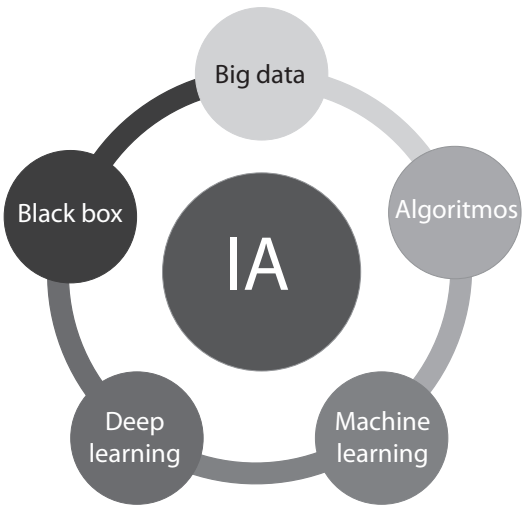
La recolección de datos de la cual se sirve la inteligencia artificial para generar los procesos traducidos en algoritmos se conoce como *big data*. Aunque el término se usó por primera vez en 1997, sus antecedentes se remontan a 1958, cuando Hans Peter Lung, investigador de IBM, utilizó el término *business intelligence* (inteligencia de negocios), que en la década de 1980 se utilizó para referirse a sistemas de *software* que intervenían en la toma de decisiones de negocios, con base en la recogida de análisis de datos o hechos. Al final de esa década surgió el término *data mining* (minería de datos), como analogía a la extracción de yacimientos, tales como bancos de datos, de lo cual se obtiene un conocimiento en concreto, equiparado como un material valioso. En 1989 empezó a utilizarse la expresión *knowledge discovery in databases* (descubrimiento de conocimiento en bases de datos), que no es otra cosa que delimitar el valioso resultado final de esa extracción (Niño e Illarramendi, 2015).

Otro integrante de suma trascendencia de la IA es el *machine learning* (aprendizaje automático), que es la capacidad de un sistema o máquina para aprender automáticamente a partir de la experiencia de la extracción de datos y la resolución de problemas de acuerdo con experiencias programadas, presentes o futuras. Con procesos más profundos, y entendido como subcampo del *machine learning*, se desarrolló el *deep learning* (aprendizaje profundo), que se define como "la actividad automática de adquisición de conocimiento a través de máquinas que usan varios niveles para la extracción". El adjetivo "profundo" no se aplica en sí al conocimiento adquirido, sino a la forma en el que el conocimiento se adquiere (Gómez Gil, 2015).

Un concepto que mueve a debatir sobre la posibilidad de violentar derechos humanos a través de la inteligencia artificial es *black box* (caja negra), que funciona con los algoritmos programados y el análisis proporcionado por el *big data*, y cuyas entradas y operaciones no son visibles para el usuario y, en algunos casos, ni para el propio operador; en pocas palabras, es impenetrable, por lo que "esta alta dimensionalidad evita que los humanos conozcan cómo la IA está tomando sus decisiones o predice cómo tratará los nuevos datos" (Bathaee, 2018).

Estos términos se estiman fundamentales para la comprensión de la inteligencia artificial, y servirán para el desarrollo de este artículo.

Gráfico 1.



Fuente: Elaboración propia

II. VIGILANCIA POR INTELIGENCIA ARTIFICIAL Y EL *BIG DATA*

Con el avance tecnológico en materia de inteligencia artificial, cada vez son más los mecanismos de los que la humanidad se auxilia para llevar a cabo todo tipo de tareas. Es común convivir con medios tecnológicos que dan respuestas rápidas y precisas a muchas necesidades; desde una búsqueda sencilla en Google hasta una instrucción a los asistentes inteligentes, como

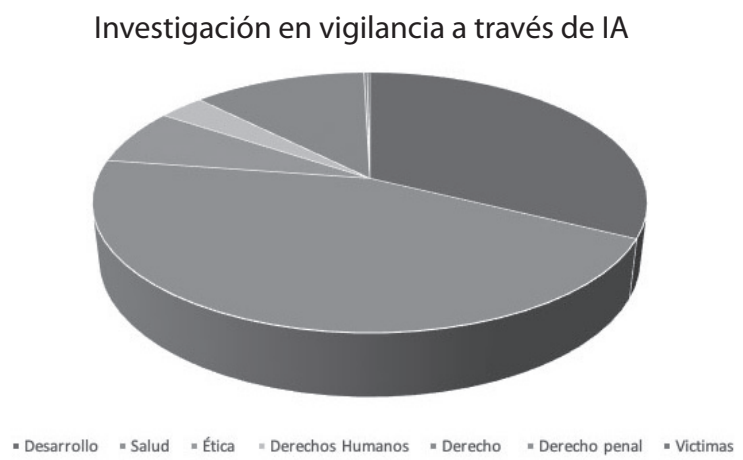
Siri o *Alexa*, mecanismos de IA hacen la vida más fácil. El desarrollo de este tipo de tecnología se vuelve determinante para "ayudar" de mejor manera al usuario. Para el uso de estos sistemas, solo es necesario tener un dispositivo a la mano y su correspondiente aplicación. Otros casos de utilización de inteligencia artificial son las páginas web, cámaras de videovigilancia en la calle, redes sociales, etcétera. Todo esto se genera a partir de una construcción social de la realidad que, de acuerdo con varios análisis interdisciplinarios, creó necesidades, como utilizar un navegador para evitar el tráfico o compartir un estado de ánimo en las redes sociales, y también obligaciones, como compartir los datos biométricos en algún trámite gubernamental como requisito para completarlo. Sin embargo, este desarrollo de la inteligencia artificial, ¿crece para informar oportunamente y, sobre todo, para proteger los derechos humanos de los usuarios que, poco a poco, han ido entregando su privacidad hasta quedar "vacíos"?

La vigilancia a través de la inteligencia artificial debe analizarse con base en el auxilio que aquella presta en la cotidianidad, ya que, bajo un esquema de facilitadora de tareas diarias o que se han vuelto indispensables para el usuario, a través del *big data* recolecta y concentra datos de cualquier tipo. Si bien es cierto que la vigilancia a partir de la geolocalización es una de las más importantes, no lo es menos el monitoreo de compras *online*, visitas a determinados sitios web y, más delicado aún, del modo de pensar a partir de las publicaciones que definen una postura política, social o religiosa, entre otras.

El *big data* es trascendental en el desarrollo de la inteligencia artificial y se define como "el acumulamiento de datos generados de manera masiva" (Casas Roma, Nin Guerrero, y Julbe López, 2019); plantea distintos retos, de los cuales no están exentas las ciencias penales y, particularmente, quienes pudieran tener la calidad de víctimas en el sistema penal acusatorio mexicano. Es de llamar la atención el grado de desarrollo de la inteligencia artificial en comparación con el de la protección de los derechos humanos relacionados con esta: en un estudio bibliográfico, partiendo de las variables en inglés *artificial intelligence* + *surveillance* (inteligencia artificial + vigilancia) dentro del buscador digital *Discovery Service* del sistema bibliotecario digital de la UNAM, delimitando la temporalidad entre los años 2016 y 2020, se encontraron 2,198 resultados, incluyendo publicaciones académicas, profesionales, revistas, noticias y materiales de conferencias. Posteriormente se agregaron filtros específicos por materia, arrojando la búsqueda lo siguiente; *artificial intelligence* + *surveillance* + *development* (inteligencia artificial

+ vigilancia + desarrollo): 393 resultados; *artificial intelligence* + *surveillance* + *health* (inteligencia artificial + vigilancia + salud): 548 resultados; *artificial intelligence* + *surveillance* + *ethics* (inteligencia artificial + vigilancia + ética): 85 resultados; *artificial intelligence* + *surveillance* + *human rights* (inteligencia artificial + vigilancia + derechos humanos): 39 resultados; artificial intelligence + surveillance + law (inteligencia artificial + vigilancia + derecho): 147 resultados; *artificial intelligence* + *surveillance* + *criminal law* (inteligencia artificial + vigilancia + derecho penal): 3 resultados; y *artificial intelligence* + *surveillance* + *victims* (inteligencia artificial + vigilancia + victimas): 2 resultados.

Gráfica 2.



Fuente: Elaboración propia.

De esta búsqueda preliminar puede apreciarse que los rubros con más investigación son el desarrollo de tecnologías y la salud, en comparación con los derechos humanos, el derecho penal y las víctimas. Cabe destacar que, por efectos de la pandemia del virus SARS-CoV-2 (COVID-19) (fines epidemiológicos), la vigilancia de la salud se ha incrementado considerablemente. Este balance lleva a pensar en lo siguiente: ¿cuáles son los sistemas de vigilancia por inteligencia artificial y el *big data* más desarrollados? ¿Están impactando a los derechos humanos de los usuarios? Ante la búsqueda de respuestas, es alarmante que los derechos humanos, las ciencias penales y la victimología sean un terreno olvidado en el mundo de la inteligencia artificial; de ahí el interés en desarrollar temas relacionados con estas materias, con el fin de prevenir violaciones a los derechos de los usuarios.

III. SISTEMAS DE VIGILANCIA A TRAVÉS DE IA MÁS DESARROLLADOS EN LA INVESTIGACIÓN

Sin duda, a partir del desarrollo de la inteligencia artificial se han detonado mecanismos de vigilancia con diversos fines y propósitos, y en este apartado se mencionarán, de acuerdo con los artículos seleccionados, cuáles son los sistemas de vigilancia más estudiados a partir del desarrollo de la IA.

Como se puede apreciar en la gráfica 2, en los últimos cinco años el 45% de la investigación ha girado en torno al desarrollo de la tecnología de vigilancia a través de la inteligencia artificial y, a su vez, ha sido primordial el segmento respectivo a la vigilancia por video, para distintos fines. La vigilancia a través de video, o *videovigilancia*, puede dividirse en dos segmentos: 1) la que se encarga de identificar y recolectar *imágenes de personas*, que involucra los sistemas de reconocimiento facial; y 2) la que recae en *objetos*.

El desarrollo de este tipo de investigación se ha encargado, en su mayoría, de crear técnicas cada vez más precisas para la recolección de datos: almacenamiento, distribución y análisis comparativos de los resultados que arroja la videovigilancia a través de la inteligencia artificial. El debate gira en torno a los servidores capaces de almacenar el *big data*, el procesamiento eficaz de esa información y, en casos mínimos, investigaciones que tratan de incrementar la seguridad de las personas. Llama la atención que, con el desarrollo de ciudades inteligentes, emergen nuevos conceptos de identificación, como el tránsito en puertos marítimos, carreteras, control de tráfico, control de estacionamientos y, en algunos casos, control de personas. Algunas investigaciones también desarrollan, con enfoque tecnológico, las detecciones de personas armadas en fracciones de segundo, a través de la combinación de cámaras de alta definición, algoritmos y bases de datos; sin embargo, a pesar de que el objetivo de dichas investigaciones sea mejorar la efectividad de la detención y, por tanto, inhibir el crimen, el desarrollo de esa tecnología carece de un enfoque garantista dirigido a los usuarios.

Otro tipo de vigilancia es la implementada por las redes sociales, a través de las cuales se recolecta todo tipo de información: páginas *web* visitadas; frecuencia, horarios y fines de la visita, por mencionar algunos ejemplos. Más allá de lo anterior, también existe la recolección de datos respecto de formularios a los que el usuario accede en la red, y que obtiene desde un registro para proporcionar información a cambio de datos personales, hasta el registro de datos en el comercio electrónico, pudiendo establecerse,

con ello, criterios de compra, de perfil y hasta pronósticos de necesidades en el futuro:

> …para predecir las tendencias, el Big Data emplea algoritmos que combinan información de las redes sociales y de la búsqueda en la web para identificar las preferencias de los consumidores. También se emplea en la fijación de los precios mediante un seguimiento de los competidores, el coste de los productos y otras variables; las empresas son capaces de analizar cómo varía la demanda ante subidas y bajadas de precio en tiempo real y finalmente, el Big Data potencia las ventas al ofrecer una experiencia personalizada y prevenir el abandono de la compra mediante un proceso de compra ajustado a las preferencias del consumidor. (Álvarez, 2018)

No menos aventurado es que, entre más datos personales recolectados, la inteligencia artificial puede crear un perfil más preciso y, por tanto, de control de las personas, no solo de sus compras, sino también de creencias políticas, sociales o religiosas, información que puede usarse con fines políticos o comerciales, entre otros. El desarrollo de este tipo de vigilancia pretende, sobre todo, generar mejores *softwares* de recolección de datos, mejores servidores de almacenamiento y procesadores más rápidos, que den respuesta inmediata a quien pudiera hacer uso de esa información; sin embargo, es limitado o nulo el enfoque que se da a la protección del usuario.

Es importante destacar que, con motivo de la pandemia de la COVID-19, se ha incrementado el desarrollo de investigación en el segmento vigilancia de la salud por IA y, si bien es cierto se han aplicado mecanismos muy eficaces de detección temprana de contagio, también es cierto que la investigación a partir de la limitación de libertades y el respeto a los derechos humanos ha pasado a un segundo plano. El debate de hoy se centra en qué país crea la tecnología más eficaz para la detección temprana del virus, con variables de mayor precisión en menor tiempo, lo que incluye también vigilancia por redes sociales, entre otros aspectos.

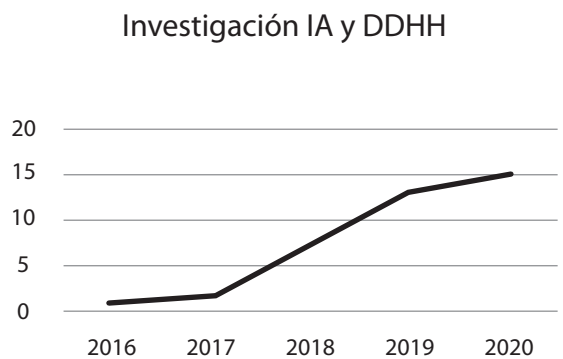
Entonces, en materia de sistemas de vigilancia más populares para la investigación, puede concluirse que el segmento más avanzado es el desarrollo tecnológico, pero solo con enfoque técnico y no necesariamente humanista.

IV. LOS DERECHOS HUMANOS COMO LA ASIGNATURA MENOS DESARROLLADA EN LA INVESTIGACIÓN SOBRE VIGILANCIA A TRAVÉS DE LA INTELIGENCIA ARTIFICIAL

Como se apuntó, una de las disciplinas relevantes para la investigación del fenómeno de vigilancia a través de la inteligencia artificial son los derechos humanos. Es fundamental que el tema de los derechos humanos se investigue a la par del crecimiento del fenómeno de la IA; al momento de elaborarse este trabajo, se observa mucha disparidad: mientras que el desarrollo tecnológico ocupa el 45% de la investigación, cuestiones tan relevantes como la salud, la ética, la ley y los derechos humanos, alcanzan el 55% restante. Más grave aún es que, de acuerdo con estas variables seleccionadas, la investigación entre el fenómeno de vigilancia por inteligencia artificial y su relación con los derechos humanos apenas alcance el 3% de la búsqueda realizada.

En los últimos años, el desarrollo de la inteligencia artificial ha alcanzado límites exponenciales, mientras que el de su relación con los derechos humanos es el siguiente:

Gráfica 3.



Fuente: Elaboración propia.

Tan solo en el cuatrienio 2016-2020, la publicación de artículos en el rubro *artificial intelligence* + *surveillance* + *human rights* fue de 39, mientras que en el rubro *artificial intelligence* + *surveillance* + *development* se elaboraron 393 publicaciones.

Por tanto, es evidente que existe una brecha en la investigación entre el desarrollo de la IA y el impacto de esta en los derechos humanos, sobre todo en cuanto a los tipos de vigilancia que se han mencionado.

V. EL DERECHO HUMANO A LA PRIVACIDAD: EL IMPACTO DE LA VIGILANCIA Y EL *BIG DATA*

La privacidad "es un elemento consustancial a la dignidad humana y, por esa misma razón, debe ser protegido por el derecho. En cambio, el derecho a la privacidad sí podría definirse cómo aquél que todo individuo tiene a separar aspectos de su vida privada del escrutinio público". (García Ricci, 2013)

El derecho a la privacidad es uno de los principales que giran en torno al uso de la inteligencia artificial y la recolección de datos. A nivel internacional, "la privacidad, consagrada en el derecho internacional de los derechos humanos y reforzada por una red sólida de las leyes y jurisprudencia de protección de datos nacionales y regionales, se ve significativamente afectada por la Inteligencia Artificial" (Fjeld, Achten, Hilligoss, Nagy y Srikumar, 2020). A modo de ejemplo: la videovigilancia es una de las tecnologías más desarrolladas en la investigación; en sociedades poco democráticas, se utiliza para restringir todo tipo de libertades de los ciudadanos, empezando por la de tránsito; los tiempos de los recorridos deambulatorios son procesados por la inteligencia artificial y recolectados por el *big data*, y terminan en análisis de identidad (racial, de género, por edad, situación familiar, laboral, etc.). Posteriormente, estos datos son procesados de la mejor manera que convenga al Estado para mantener el control, y que trastoca otros derechos humanos, como el de no discriminación. A partir de la selección programada por estos algoritmos, se pueden vulnerar los derechos que el Estado tendría que garantizar, no condicionar. Los algoritmos pueden estar sesgados (puesto que son programados por humanos), y ahí se encuentra la falla de inicio por lo que hace a los procesos objetivos de selección y de limitación; por ejemplo: ¿por qué se determina que una persona afroamericana tiene mayor probabilidad de delinquir que una caucásica? La respuesta es simple: porque un patrón humano dominante a partir de una construcción social determina esta discriminación, borrando toda posibilidad de garantizar el respeto a la dignidad de una persona y el libre albedrío. Estas víctimas de discriminación pueden terminar, con motivo de

la programación de algún algoritmo, como víctimas en un proceso penal donde también puedan ser condenadas a partir de patrones erróneos. El *big data* y los algoritmos pueden heredar o reflejar perjuicios y patrones de exclusión, o ser resultado de quienes han tomado decisiones anteriores más allá de la intencionalidad; se trata de un peligro objetivo que hay que prevenir (Barocas, 2016).

En el caso de las redes sociales, la inteligencia artificial, de acuerdo con el perfil del usuario y haciendo uso de algoritmos y procesos de *deep learning* a través del *big data*, puede compartir los datos de aquel para efectos comerciales, vulnerando así el derecho a la privacidad; por ejemplo, puede vender sus patrones de búsqueda, el tipo de perfiles que sigue para sugerirle compras por correo electrónico, mensajes de texto, *cookies* (archivos que crean los sitios visitados en internet, para que dichos sitios consulten la actividad previa del navegador), etcétera. ¿No tendría el usuario derecho a resguardar estos datos, a pesar de que existan corrientes que aseguran que, una vez publicada información en redes sociales, pasa al terreno de lo público? Esta violación al derecho a la privacidad, ¿convierte en víctima a los usuarios de redes sociales y puede llegar al extremo de originar un procedimiento penal? La respuesta parecería afirmativa, ya que la información compartida puede provocar, como se ha demostrado, linchamientos sociales por odio racial, cuestiones de género, etcétera. Basta que la información, de acuerdo con algoritmos programados, se "viralice" y llegue a antagonistas que generen un daño irreversible.

Los mecanismos de geolocalización, otro tipo de vigilancia, presuponen una violación al derecho a la privacidad; basta con tener un teléfono móvil y desplazarse por cualquier lugar. Inmediatamente, de acuerdo con la posición geográfica del usuario, pueden comenzar las sugerencias de compras, rutas o, peor aún, que esa información se comparta con el Estado o corporaciones de cualquier tipo para fines no comerciales, lo cual vulneraría, por ejemplo, el derecho humano a la seguridad; en México, en virtud del confinamiento debido a la COVID-19, se implementó, a la par de la geolocalización, el registro de lugares de asistencia a partir de un código QR (del inglés *Quick Response code*, "código de respuesta rápida").

De ello, el usuario no conoce, a pesar del acuerdo de confidencialidad y la protección de datos, cómo se usa su información y cómo se gestiona la base de datos en la cual se almacena aquella. "Se trata de tener localizados o geolocalizados a los contagiados (e incluso a los sanos, para que no se salten el confinamiento), y tener preparados recursos sanitarios para

asistirlos." (Cascón, 2020) ¿Solo para fines de control de la pandemia? Este ejemplo se relaciona con el derecho humano a la salud, y podría decirse que, si el tratamiento de estos datos fuere utilizado de buena manera, no solo evitaría actores del procedimiento penal que por alguna circunstancia pudieran terminar como víctimas o imputados, sino, ante la situación actual de salubridad en el mundo, como víctimas mortales. La vigilancia epidemiológica por inteligencia artificial y *big data*, lejos de generar víctimas por violación al derecho a la privacidad, debe ser un parteaguas positivo para demostrar que el uso de esta tecnología puede colaborar con la humanidad no solo para mejorar procesos, sino para salvar vidas. Hay que normar estos mecanismos de protección sin restringir derechos humanos.

VI. RETOS Y DESAFÍOS DE LA VIGILANCIA A TRAVÉS DE LA INTELIGENCIA ARTIFICIAL Y EL RESPETO A LOS DERECHOS HUMANOS

Cuestiones como transparencia, ética y legalidad se han desarrollado en la academia, pero no al ritmo de la investigación técnica que mejora constantemente a la vigilancia a través de la inteligencia artificial. De la consulta del material referido en esta investigación, se advierte que el uso de la vigilancia a través de inteligencia artificial pretende optimizar la vida diaria de los usuarios, y que aplicar esta tecnología supone muchos beneficios; la automatización de procesos con motivo del reconocimiento facial; el orden y la seguridad en las ciudades inteligentes; la vigilancia vehicular para disminuir el tráfico; las sugerencias de compras cuando existen ofertas; la interactuación a distancia con muchas personas a la vez; o la realización de trámites mediante un sistema de reconocimiento dactilar.

El avance tecnológico que ha logrado la IA es cada vez mayor, y sus beneficios son evidentes. Un ejemplo se observa en la vigilancia que se realiza actualmente en materia de salud; en regímenes autoritarios se controló la pandemia eficientemente gracias a esta tecnología. En Estados cuyas democracias son incipientes, se ha intentado implementar con algo de éxito; entonces, la pregunta que surge, partir del desarrollo de la investigación transversal para proteger los derechos humanos de los usuarios, es la siguiente: ¿puede lograrse un equilibrio entre la evolución de la vigilancia y la vigilancia de su uso? La respuesta sería afirmativa; si se logra esta armonía y se avanza conjuntamente en la investigación, tanto tecnológica como

humanística, se podría generar un círculo virtuoso que mejoraría los procesos y daría certeza a los usuarios para el uso de esta tecnología, amén de impedir los abusos por cualquiera que tenga en sus manos la información que recolectan esos medios de vigilancia.

Como se ha presentado en este artículo, existen escasas investigaciones con muchas preocupaciones acerca del impacto en los derechos humanos del uso de la vigilancia a través de la inteligencia artificial, y pocas respuestas que la ciencia que desarrolla estos conceptos pueda responder. Con la motivación de la investigación bajo este rubro (derechos humanos), se podrían generar numerosos beneficios a un espectro muy amplio de usuarios, que no solo entran en el rubro de vigilancia por IA, sino que se relacionan con otros aspectos, como la seguridad pública, la prevención del delito y la victimología. Por tanto, existe una gran brecha que llenar en lo referente al enfoque garantista que debería desarrollarse a la par de la inteligencia artificial, sobre todo en cuanto a cualquier tipo de vigilancia.

En conclusión, a partir del análisis de la investigación cuantitativa del fenómeno de vigilancia a través de la inteligencia artificial, se encuentra una disparidad entre desarrollo tecnológico y derechos humanos, que, de continuar, podría ocasionar graves consecuencias en las libertades de los individuos, y podría generar víctimas que tendrían que ser atendidas bajo la óptica del derecho penal y la victimología.

Por ello, con esta investigación se ha pretendido coadyuvar a eliminar esa brecha y generar, a la par del desarrollo tecnológico, mecanismos de protección a los derechos humanos de los usuarios que son, o pudieran ser, vigilados por la inteligencia artificial y, con ello, no solo protegerlos, sino también crear un ambiente de confianza, donde se pueda seguir utilizando la inteligencia artificial de manera beneficiosa.

VII. FUENTES DE CONSULTA

Álvarez Torre, L. (2018). *El Big data y el cambio en el modelo de negocio de las empresas de e-commerce: el caso de Amazon y Alibaba*. Madrid: Universidad Pontificia Comillas. Disponible en: https://repositorio.comillas.edu/xmlui/handle/11531/18640

Barocas, S. y Selbst, A.D. (2016). "Big Data's Disparate Impact". *California Law Review*, vol. 104, No. 3, June 2016.

Bathaee, Y. (2018). "The artificial Intelligence black box and the failure of intent and causation". *Harvard Journal of Law & Technology*, Vol. 31, No. 2, Spring 2018. 890-938.

Cascón-Katchadourian, J. (2020). "Tecnologías para luchar contra la pandemia Covid 19: geolocalización, rastreo, big data, SIG, inteligencia artificial y privacidad". Disponible en: https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/79450

Casas Roma, J., Nin Guerrero, J., y Julbe López, F. (2019). "*Big Data*: Análisis de datos en entornos masivos". Barcelona: Universitat Oberta de Catalunya.

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., y Srikumar, M. (2020). "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights - based Approaches to Principles for AI". Disponible en: https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y

García Ricci, D. (2013). "Artículo 16 constitucional. Derecho a la privacidad". En Ferrer Mac-Gregor Poisot, E. *et al.* (coords.), *Derechos Humanos en la Constitución: Comentarios de Jurisprudencia Constitucional e Interamericana*. Tomo I. México: Suprema Corte de Justicia de la Nación, Universidad Nacional Autónoma de México, Fundación Konrad Adenauer.

Gómez Gil, M. (2015). "Aprendizaje profundo. El poder del aprendizaje automático unido al poder de cálculo de las computadoras actuales". Disponible en: https://ccc.inaoep.mx/~pgomez/conferences/PggTSys16.pdf

Niño, M., e Illarramendi, A. (2015). "Entendiendo el Big Data: antecedentes, origen y desarrollo posterior". Disponible en: https://www.dyna-newtech.com/busqueda-NT/entendiendo-big-data-antecedentes-origen-y-desarrollo-posterior