CÓDIGOS Y CONDENAS: LA PREDICCIÓN DE CONDUCTAS PUNIBLES EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

Javier Augusto Torres López[1]

La integración de la inteligencia artificial en el ámbito legal, especialmente en el derecho penal, ha marcado un cambio significativo en la forma en que se abordan los procesos judiciales y la toma de decisiones. Esta columna explora el uso de algoritmos para la predicción del comportamiento delictivo, y destaca su potencial para mejorar la eficiencia judicial y reducir sesgos humanos. Sin embargo, surgen controversias relacionadas con la imparcialidad y el sesgo inherentes a los datos utilizados para entrenar estos algoritmos, lo que plantea dilemas éticos y legales. Se examinan preocupaciones sobre discriminación, falta de representación equitativa en conjuntos de datos y la ausencia de claridad en la toma de decisiones algorítmicas. Además, se discuten los desafíos éticos vinculados a la responsabilidad en caso de errores y la amenaza a la privacidad individual.

SUMARIO:

I. Introducción

[1] Abogado graduado de la Universidad Libre, con especialización en Derecho Procesal Penal de la Universidad Externado y un máster en Derecho Penal y Procesal Penal obtenido en la Universidad Carlos III de Madrid. Además, ha completado estudios avanzados en Corporate Compliance en la Universidad de los Andes. Abogado litigante. Columnista del boletín académico de Diálogos Punitivos.

La historia del derecho penal ha sido moldeada por la necesidad de prevenir y retribuir, a través de una sanción, la comisión de conductas punibles por parte de los ciudadanos[2]. En el ámbito judicial, esa necesidad se ve reflejada en procesos (lentos y excesivamente formalistas) que pretenden analizar la existencia de responsabilidad de una persona frente a un hecho concreto.

En el imaginario de algunos ciudadanos, un proceso ante un estrado judicial se desarrolla «en un espacio y en una atmósfera que parecen conscientemente sustraídos al paso del tiempo (edificios antiguos, jueces y abogados togados que recitan una serie de fórmulas arcaicas, voluminosos legajos…) y cuya legitimidad viene en gran parte asentada precisamente en el respeto a una serie de tradiciones seculares»[3]. No obstante, la llegada de la inteligencia artificial (IA, en adelante)[4] introduce elementos novedosos al sistema de justicia penal que pueden modificar esta percepción, y que pueden propender por una administración de justicia óptima y eficaz.

La IA ha surgido como una fuerza disruptiva, dando forma y redefiniendo los paradigmas establecidos en el derecho penal. En esta era de análisis algorítmicos, se han creado sistemas de calificación de riesgos para la predicción de comportamientos delictivos. Estas herramientas[5], alimentadas por datos históricos, intentan anticipar quiénes podrían ser potenciales infractores a la ley penal, lo cual supone la promesa de una justicia más eficiente y precisa. Sin embargo, esta promesa enfrenta preocupaciones sobre sesgos algorítmicos, «falta de explicabilidad»[6] y el riesgo de perpetuar injusticias sistemáticas.

---

[2] Enrique Peñaranda Ramos, «La pena: nociones generales», en *Introducción al derecho penal*, cord. Juan Antonio Lascuraín Sánchez (Navarra: Arazandi, 2015), 259-260.

[3] José Ignacio Solar Cayón, «Reflexiones frente a la aplicación de la inteligencia artificial en la administración de justicia». *Teoría Jurídica Contemporánea* 6 (2021): 2, https://repositorio.unican.es/xmlui/bitstream/handle/10902/24149/ReflexionesSobreLaAplicaci%C3%B3n.pdf?sequence=1.

[4] «Es la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de decisiones, tal y como lo haría un ser humano». En: Lasse Rouhiainem, *Inteligencia artificial: 101 cosas que debes saber soy sobre nuestro futuro* (Barcelona: Alienta, 2018), 17.

[5] También denominadas RATs (risk assessment tools)

[6] Según la UNESCO, el principio de explicabilidad «hace referencia al hacer inteligible los resultados de los sistemas de inteligencia artificial. La habilidad de la inteligencia artificial también hace referencia a la comprensión de los datos, procesos y comportamientos de los distintos bloques algorítmicos y cómo cada uno de ellos contribuye al resultado del sistema. Así, la explicación está estrechamente relacionada con la transparencia, ya que los procesos y subprocesos que conducen a los resultados deberían ser comprensibles y trazables, apropiados para el contexto». En: Lucía Ortiz de Zárate Alcarazo, «Explicabilidad (de la inteligencia artificial)». *Eunomía, Revista en Cultura de la Legalidad,* n.° 3 (2022): 335, https://e-revistas.uc3m.es/index.php/EUNOM/article/view/6819.

Ciertamente, la capacidad predictiva de la IA plantea profundos dilemas morales, éticos y legales. Por un lado, la promesa de prevenir y anticipar delitos antes de que ocurran, basada en patrones de comportamiento y datos masivos, ha llevado a concebir a la IA como una gran aliada en contra de la criminalidad, aunque también ha encendido las alarmas al prever riesgos en su uso frente a los derechos de los ciudadanos. Esto ha suscitado una serie de cuestionamientos: ¿es ético el ejercicio de la acción penal en contra de un ciudadano por delitos que aún no ha cometido con base en predicciones algorítmicas?, ¿cómo equilibramos la prevención de crímenes con el respeto a la presunción de inocencia y a los derechos individuales?, ¿es conveniente el desconocimiento, «opacidad»[7], de los factores que determinan la toma de esta clase de decisiones?, ¿hasta qué punto podemos confiar en la capacidad de la inteligencia artificial para prever comportamientos delictivos y tomar decisiones cruciales que afectan la vida de los ciudadanos?

En este sentido, con el propósito de acercarnos a esas inquietudes, en esta columna se abordará el uso de la inteligencia artificial en el contexto legal, los algoritmos predictivos en la comisión de conductas punibles y las controversias que han surgido alrededor de ello. Finalmente, se tomará postura frente a las problemáticas planteadas.

II. Los algoritmos predictivos de riesgo y sus bondades

La IA ha desempeñado un papel relevante en el ámbito legal, particularmente en el derecho penal, y ha transformado la manera en que se abordan los procesos y las decisiones judiciales[8]. Ofrece una gama de posibilidades, desde la optimización de procesos hasta la toma de decisiones más informadas. Incluso, su uso se extiende al campo probatorio, en donde ha permitido analizar en

[7] Cuando hablamos «de opacidad respecto a los algoritmos estamos haciendo referencia a la falta de transparencia motivada por la existencia de una especie de caja negra que carece de capacidad explicativa y dificulta su correspondiente inteligibilidad». En Javier Blázquez Ruiz, «La paradoja de la transparencia en la IA: Opacidad y explicabilidad. Atribución de responsabilidad». *Revista Internacional de Pensamiento Político – I Época* 17 (2022): 267, https://www.upo.es/revistas/index.php/ripp/article/view/7526/6376.

[8] Frank A. Pasquale y Daniell Keats Citron, «The second society: Due process for automatted predictions», *Legal Studies Research Paper Washington Law Review* 89 (2014): 18, https://ssrn.com/abstract=2376209.

tiempos reducidos inmensas cantidades de datos electrónicos. Esto ha sido de gran utilidad para resaltar el papel de la evidencia digital en las investigaciones criminales[9].

Uno de los usos más destacados de la IA en el campo del derecho penal es la predicción del comportamiento delictivo. Los algoritmos de IA analizan grandes conjuntos de datos para identificar patrones y predecir posibles delitos, lo que puede ser útil para asignar recursos policiales o determinar la libertad condicional[10]. En su esencia, estos algoritmos se basan en la recopilación y el análisis de datos provenientes de registros criminales, datos demográficos, historiales escolares, empleo, residencia, entre otros. Esta información se alimenta de un modelo matemático que busca patrones para predecir la probabilidad de que un individuo cometa un delito en el futuro, o que predican la potencial comisión de un delito en una zona geográfica específica[11]. Estos modelos, a través de *machine learning,* buscan identificar a las personas con mayor riesgo, esto permite a los sistemas judiciales tomar decisiones más informadas sobre libertad condicional, sentencias, aplicación de medidas cautelares, medidas de aseguramiento o de seguridad.

Asimismo, se han desarrollado algoritmos que sirven de apoyo para los cuerpos policiales, de tal manera que puedan recibir información automatizada y en tiempo real acerca de «por ejemplo, las áreas en las que deben desplegarse operativos policiales»[12].

Defensores de los sistemas algorítmicos de predicción penal argumentan que estos ofrecen una herramienta valiosa para las fuerzas del orden, permitiéndoles anticipar crímenes, identificar posibles reincidencias, asignar recursos de manera más eficiente y aplicar estrategias preventivas frente a la comisión de punibles[13]. Los algoritmos, mediante el análisis de patrones y correlaciones en grandes conjuntos de datos, intentan detectar delincuentes potenciales, antes de que cometan un delito. Esta

[9] Facundo Barrios, «Resúmenes: XVIII Semana del derecho y la criminalística. Inteligencia artificial Deux Ex Machina». *Memorias forenses*, n.º 7 (2023): 1-2, https://doi.org/10.53995/25390147.1590.
[10] Nuria Belloso Martín, «Algoritmos predictivos al servicio de la justicia: ¿una nueva forma de minimizar el riesgo y la incertidumbre?». *Revista da Facultade Mineira de Direito* 22, n.° 43 2019): 16-17, https://periodicos.pucminas.br/index.php/Direito/article/view/20780/16029.
[11] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Armas de destrucción matemática: Cómo los datos masivos aumentan la desigualdad y amenazan la democracia). (Madrid: Capitán Swing Libros, 2017), 55-62.
[12] Marcela del Pilar Roa Avella, Katherin Dinas-Hurtado y Jesús Eduardo Sanabria-Moyano, «Uso de algoritmo COMPAS en el proceso penal y los riesgos a los derechos humanos», *Revista Brasileira De Direito Processual Penal* 8, n°.1 (2022): 280, https://revista.ibraspp.com.br/RBDPP/article/view/615.
[13] Belloso Martín, «Algoritmos predictivos al servicio», 26-27.

capacidad predictiva basada en el conocimiento, sostienen, «incrementa su eficacia para prevenir delitos e incidentes relacionados con la seguridad, y desarticular redes y grupos delictivos»[14].

Algunos ejemplos de estos algoritmos son la Public Safety Assessment (PSA), Level of Service Inventory Revised (LSI-R), Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)[15], HART, CAS[16]. PRISMA[17], entre otros. Estas herramientas se evidencian, mayoritariamente, en el ordenamiento jurídico de Reino Unido y de Estados Unidos, en donde su uso ha sido propuesto por diversas universidades y adoptado por diferentes Estados[18].

Los algoritmos de predicción penal tienen el potencial de mejorar la precisión en la toma de decisiones judiciales. El utilizar modelos matemáticos y estadísticos permite que los algoritmos puedan analizar grandes conjuntos de datos y detectar patrones[19] que podrían pasar desapercibidos para un juez o un sistema humano. Esto podría ayudar a identificar mejor los riesgos potenciales de reincidencia y contribuir a una evaluación más objetiva del riesgo de un individuo en particular.

Otra ventaja es la posibilidad de reducir los sesgos humanos en el sistema judicial. Los jueces y otros actores del sistema pueden estar influenciados por prejuicios conscientes o inconscientes al tomar decisiones sobre la libertad condicional, las sentencias o la fijación de la fianza. Los algoritmos de predicción penal, si se diseñan adecuadamente, pueden minimizar estos sesgos al centrarse únicamente en datos relevantes, sin verse afectados por factores subjetivos como la raza, la religión, el sexo, el género o la apariencia física. Además, estos algoritmos podrían contribuir a una distribución más eficiente de los recursos públicos destinados a los sistemas judiciales al predecir qué individuos se beneficiarían de más programas de rehabilitación o de programas alternativos al

[14] José Luis González-Álvarez, Jorge Santos-Hermoso y Miguel Camacho-Collados, «Policía predictiva en España. Aplicación y retos futuros», *Behavior & Law Journal* 6, n°.1 (2020): 38, https://www.behaviorandlawjournal.com/BLJ/article/view/75/90.

[15] «Es entendido como una herramienta estructurada que valora el riesgo de reincidencia del procesado y las necesidades criminológicas del sujeto». En: Lucía Martínez Garay, «Peligrosidad, algoritmos y due process: El caso State v Loomis», *Revista de Derecho Penal y Criminología* 3, n°. 20 (2018): 485, https://revistas.uned.es/index.php/RDPC/article/view/26484/20947

[16] Laura Notaro, «"Algoritmos predictivos" y justicia penal desde una perspectiva italiana y europea», en *Derecho penal, inteligencia artificial y neurociencias*, coord. José Miguel Peris Riera y Antonella Massaro (Roma: Roma TrE-PRESS, 2023), 193-198, https://romatrepress.uniroma3.it/wp-content/uploads/2023/02/7.-Laura-Notaro.pdf.

[17] Fiscalía General de la Nación, «Herramienta prisma: perfil de riesgo de reincidencia para la solicitud de medidas de aseguramiento», *Dirección de políticas públicas y estrategia de la Fiscalía General de la* Nación https://www.fiscalia.gov.co/colombia/wp-content/uploads/Perfil-de-riesgo-de-reincidencia-para-solicitudes-de-medida-de-aseguramiento.pdf

[18] *Ibid.*, 193.

[19] Roa Avella, Dinas-Hurtado y Sanabria-Moyano, «Uso de algoritmo COMPAS», 280-281.

encarcelamiento, lo que aumentaría las probabilidades de resocialización y reintegración exitosas y reduciría la reincidencia[20].

En Colombia, el uso de estas herramientas en el sistema de justicia penal no ha pasado desapercibido[21]. Incluso, la Corte Constitucional ha indicado que son «… una rama de la inteligencia artificial que, valiéndose de programas y *software* especializado, puede analizar toda esa información para identificar patrones y realizar predicciones. Esto permite que los computadores realicen este proceso de manera autónoma»[22].

Organizaciones privadas y entes gubernamentales han desarrollado *softwares* de automatización para el desarrollo de sus actividades misionales. Por ejemplo, la Fiscalía General de la Nación (FGN) anunció en el año 2019 la implementación de una herramienta tecnológica denominada PRISMA, que tiene como propósito principal el predecir el riesgo de reincidencia criminal de quienes se predique la necesidad de imponer una medida de aseguramiento en el marco de un proceso penal. La herramienta referida, un *software* algorítmico predictivo elaborado por la Dirección de Políticas y Estrategia de la FGN, posee un modelo de aprendizaje supervisado que le permite calcular cuantitativamente la probabilidad de reincidencia de un procesado y su peligrosidad, con base en los delitos cometidos, en sus características individuales y en sus antecedentes penales[23].

De lo anterior se entiende que su utilidad se concentrará en la fundamentación cuantitativa del fin constitucional de protección a las víctimas del delito o a la comunidad[24], cuando se evidencie la existencia de riesgos en relación con la peligrosidad del procesado. El uso de este instrumento, según fue indicado, permitirá una utilización más proporcional de las medidas de aseguramiento de carácter intramural, pues se busca que las solicitudes de imposición que se presenten ante la judicatura se concentren en aquellos individuos con altos niveles objetivos de reincidencia[25].

[20] *Ibid.*, 280.
[21] Yesid Reyes Alvarado y Andrés Felipe Díaz Arana, «Tecnologización del sistema de justicia penal en Colombia» (Manuscrito), *Departamento de Derecho Penal y Criminología. Universidad Externado de Colombia,* 2023.
[22] C. Const., Sent. C.406, nov. 17/2022. M. P. Cristina Pardo Schlesinger.
[23] Fiscalía General de la Nación, «Herramienta PRISMA».
[24] Natalia Moreno Blanco, «¿Efectivización de los cupos carcelarios?: aproximación al Sistema Prisma de la Fiscalía General de la Nación» (tesis de grado, Universidad de los Andes, 2019), 25-30, https://repositorio.uniandes.edu.co/entities/publication/83c142ed-7fdf-4580-ab26-c91ef609d7b9
[25] *Ibid.*, 29.

III. Cuatro peligros principales en el uso de algoritmos de predictibilidad penal

Las herramientas de predicción en el derecho penal no están exentas de desafíos y controversias. Incluso, su uso ha sido catalogado como peligroso para el cabal desarrollo de los procesos judiciales. Por ello, aquí se presentan algunas de estas controversias:

Imparcialidad con base en información sesgada

La preocupación principal gira en torno a la imparcialidad y al sesgo inherente en los datos utilizados para entrenar estos algoritmos[26]. Autores como Virginia Eubanks han destacado, por ejemplo, cómo la falta de representación diversa en los conjuntos de datos puede llevar a decisiones discriminatorias, y perpetuar y ampliar las desigualdades existentes[27]. Esta dificultad también ha sido conocida como el dilema de la imputación de datos[28].

Este dilema parte de la base de que los datos históricos usados para el perfilamiento criminal predictivo reflejan y perpetúan los sesgos que hay en el sistema judicial. Esto significa que los algoritmos, al basarse en estos datos, pueden reproducir y amplificar prejuicios contra ciertos grupos étnicos, socioeconómicos o raciales[29]. Si los datos históricos muestran un patrón de discriminación hacia una comunidad específica, el algoritmo también puede reflejar y perpetuar esa discriminación, y generar así decisiones sesgadas y no equitativas[30].

Por ejemplo, si determinadas comunidades han experimentado un escrutinio policial desproporcionado en el pasado, los algoritmos podrían tender a señalar esas áreas como «de alto riesgo», lo que crearía un ciclo de discriminación que afectaría negativamente a esas comunidades. Este sesgo podría traducirse en una mayor presión policial en áreas ya estigmatizadas y contribuiría

[26] Martínez Garay, «Peligrosidad, algoritmos y due process», 496-497.
[27] Virginia Eubanks, *Automating inequality: How high-tech tolos profile, pólice, and punish the poor* (New York: St. Martin´s Press, 2018), 14-18.
[28] Javier Valls Prieto, «Sobre la responsabilidad penal por la utilización de sistemas inteligentes», *Revista Electrónica de Ciencia Penal y Criminología*, n°. 24-27 (2022): 4, http://criminet.ugr.es/recpc/24/recpc24-27.pdf.
[29] Eubanks, *Automating inequality: How High-tech*,18.
[30] Valls Prieto, «Sobre la responsabilidad penal», 20-21.

a la perpetuación de desigualdades y prejuicios[31]. Frente a este punto, el Gobierno de España, en su portal de «Datos Abiertos», ha indicado que

> Los sistemas algorítmicos opacos que incorporan estereotipos pueden aumentar la invisibilización y la discriminación al ocultar, o bien apuntar, a personas o poblaciones vulnerables. Un sistema algorítmico opaco es aquel que no permite el acceso a su funcionamiento. […] La discriminación puede surgir cuando las decisiones algorítmicas se basan en datos históricos, que normalmente incorporan asimetrías, estereotipos e injusticias, porque en el pasado existieron más desigualdades. El efecto de «basura entra basura sale» se produce si los datos están sesgados, como suele pasar con el contenido en línea. Asimismo, las bases de datos con sesgos o incompletas pueden ser incentivos de la discriminación algorítmica. Pueden aparecer sesgos de selección cuando los datos de reconocimiento facial, por ejemplo, se basan en rasgos de hombres blancos, mientras que las usuarias son mujeres de piel oscura, o en contenido en línea generado por una minoría de agentes, lo que dificulta la generalización[32].

Al respecto, cabe citar el caso de PREDPOL, un *software* predictivo utilizado en Estados Unidos[33], cuyo uso generó mayor presencia policial en barrios en los que habitaban, de manera predominante, personas latinas y afrodescendientes al considerarlos potencialmente peligrosos. Esto ocurrió en la medida en que el algoritmo reflejaba «los valores, prejuicios y puntos de vista de quienes participaron en su diseño»[34].

Por otro lado, como se mencionó, la imparcialidad también puede verse comprometida debido a la falta de representación equitativa en los conjuntos de datos. Si la información de ciertos grupos sociales no es tenida en cuenta, los algoritmos pueden no captar adecuadamente sus experiencias y, por lo tanto, no podrían predecir con precisión los patrones delictivos en esas comunidades minoritarias[35]. La imputación de datos, o el relleno de lagunas en los conjuntos de datos, puede introducir sesgos adicionales si se realiza de manera inadecuada[36]. Por ejemplo, si un grupo

[31] Tarcizio Silva, *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais* (Sao Paulo: Edições Sesc, 2022).
[32] «Invisibilización y discriminación algorítmica», *Datos Abiertos*, 6 de octubre de 2023, https://datos.gob.es/es/blog/invisibilizacion-y-discriminacion-algoritmica#:~:text=Por%20el%20contrario%2C%20la%20discriminaci%C3%B3n,conjuntos%20de%20datos%2C%20generando%20injusticia.
[33] Paula Guerra Cáceres, «Algoritmos entrenados para ser racistas», *Pikara Magazine*, 23 de noviembre de 2022, acceso el 3 de diciembre de 2023, https://www.pikaramagazine.com/2022/11/algoritmos-entrenados-para-ser-racistas/#:~:text=El%20sesgo%20de%20PredPol%20es,de%20dise%C3%B1o%20de%20un%20algoritmo.
[34] Guerra Cáceres, «Algoritmos entrenados»
[35] A este fenómeno se le ha denominado también *invisibilidad algorítmica*.
[36] Eubanks, *Automating inequality: How High-tech* ,34.

específico de personas ha sido sistemáticamente pasado por alto en los informes policiales, la imputación de datos podría basarse en suposiciones erróneas y arrojaría conclusiones sesgadas. Esto podría resultar en un aumento de la presión policial en áreas que no necesariamente reflejan una mayor tasa de delincuencia, sino simplemente una más alta presencia policial.

En suma, la implementación de algoritmos de predicción delictiva sesgados puede socavar la confianza en el sistema de justicia y exacerbar las tensiones sociales y las desigualdades existentes. El uso de algoritmos sesgados puede llevar a decisiones injustas, como detenciones erróneas o perfiles injustificados. Esto no solo afecta a los individuos directamente involucrados, sino que también contribuye a la erosión de la confianza pública en las instituciones gubernamentales.

Incremento en la dependencia de algoritmos predictivos - ausencia de responsabilidad

Otra de las críticas expuestas sobre el uso de los sistemas de predictibilidad penal es la dependencia en estos sistemas y la ausencia de responsabilidad de los operadores jurídicos. Al respecto, Brett Frischmann y Evan Selinger han argumentado que el uso excesivo de la IA puede socavar la responsabilidad humana y la transparencia en la toma de decisiones legales, y plantear interrogantes sobre quién es responsable en caso de errores o decisiones cuestionables[37].

La responsabilidad ética y legal se ve comprometida cuando la toma de decisiones se orienta bajo los parámetros determinados por sistemas de IA altamente complejos. En caso de errores o determinaciones cuestionables, surge la pregunta: ¿quién es responsable? La atribución de la responsabilidad se vuelve difusa, ya que la cadena de decisiones involucra tanto a los diseñadores de la IA como a los usuarios y a los propios algoritmos[38]. Esta falta de claridad puede afectar negativamente la rendición de cuentas y la capacidad de corregir posibles injusticias.

Además, la dependencia excesiva de la IA en el derecho penal plantea desafíos éticos inherentes. La inteligencia artificial no posee conciencia ni comprensión moral, lo que puede resultar en decisiones que carecen de empatía y consideración de factores contextuales. Esto suscita preocupaciones sobre la equidad de género y la concepción de justicia en la aplicación de la ley,

[37] Brett Frischmann y Evan Selinger, *Re-Engineering Humanity* (Cambridge: Cambridge University Press, 2018), https://www.cambridge.org/core/books/reengineering-humanity/379F3C68F6AAC6C0C3998C14DACC38CF

[38] Erick Rincón Cárdenas y Valeria Martínez Molano, «Un estudio sobre la posibilidad de aplicar la inteligencia artificial en las decisiones judiciales», *Revista Direito GV* 19 (2023), https://www.scielo.br/j/rdgv/.

campos en los que se ha avanzado ampliamente en los últimos años y que podrían verse afectados por este uso de algoritmos.

Falta de transparencia

Así mismo, la opacidad en el funcionamiento de estos algoritmos también genera preocupaciones significativas. Muchos de estos modelos son «cajas negras»[39], lo que significa que sus procesos de toma de decisiones no son fácilmente comprensibles para los humanos. Esta falta de transparencia plantea interrogantes sobre la responsabilidad y la capacidad de rendición de cuentas en casos en los que estos algoritmos influyen en decisiones que impactan las vidas de las personas.

Frente a la opacidad de los algoritmos, Bonsignore Fouquet ha indicado que esta puede adoptar tres formas distintas: «En primer lugar, tenemos la opacidad derivada del secreto público o privado, que impide el escrutinio interno del algoritmo [...]. En segundo lugar, tenemos la opacidad derivada de la falta de conocimientos técnicos sobre el funcionamiento de un algoritmo o la interpretación de código informático. Dado que este campo de conocimiento está todavía reservado a un sector reducido y crecientemente especializado de la población [pues] tratar con algoritmos y programas complejos, en general, resulta esotérico para la mayoría de personas, entre ellas los juristas. [...] Por último, encontramos un tercer tipo de opacidad relativo al propio funcionamiento de los algoritmos de machine learning, cuya peculiaridad estriba en el hecho de que incluso aquellos sujetos que poseen los conocimientos técnicos requeridos pueden llegar a ser incapaces de interpretar los motivos por los que el programa produce un determinado resultado»[40].

En este contexto, surge la preocupación de que la IA, al realizar tareas complejas y sensibles en el ámbito legal, pueda socavar la transparencia inherente al proceso judicial. La opacidad algorítmica, donde los procesos de toma de decisiones no son claros ni comprensibles para los seres humanos, supone un desafío significativo[41]. La falta de transparencia dificulta la identificación de posibles errores o sesgos en las decisiones legales automatizadas, lo que lleva a una disminución de la confianza en el sistema judicial.

---

[39] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA and London, England: Harvard University Press, 2015), 270-275, https://www.degruyter.com/document/doi/10.4159/harvard.9780674736061.c8/html.

[40] *Dyango Bonsignore Fouquet, «Sobre inteligencia artificial, decisiones judiciales y vacíos de argumentación», Teoría & Derecho. Revista de Pensamiento Jurídico, n°. 29 (2021): 264, https://teoriayderecho.tirant.com/index.php/teoria-y-derecho/article/view/554.*

[41] Pasquale, *The Black Box Society,* 245.

Afectación al derecho de la intimidad

Por último, la privacidad de los individuos está en juego cuando se recopilan y utilizan grandes cantidades de datos personales para predecir comportamientos futuros. Existe el riesgo de que estos sistemas vulneren la privacidad y la autonomía de las personas, ya que pueden influir en decisiones que afectan su libertad y derechos fundamentales[42].

Los derechos a la intimidad y al *habeas data*, en muchas regulaciones, se encuentran protegidos como derechos fundamentales, ya sea mediante disposiciones constitucionales, leyes o a través de interpretaciones judiciales. El uso de tecnologías de predicción del comportamiento criminal, basadas en grandes cantidades de datos personales, plantea desafíos para garantizar que estas prácticas cumplan con los principios y límites establecidos por estas normas jurídicas[43]. Esto crea un escenario en el que los ciudadanos se sienten constantemente observados y evaluados, lo que socava su expectativa razonable de privacidad. En términos jurídicos, este tipo de vigilancia podría considerarse como una violación del derecho a la intimidad de los ciudadanos, que busca proteger a las personas de intromisiones injustificadas en sus asuntos personales[44].

Uno de los problemas centrales es la preocupación por la vigilancia masiva y la invasión de la privacidad. La recopilación extensiva de datos personales para predecir comportamientos criminales puede resultar en perfiles detallados de individuos, incluyendo información altamente sensible.

Estas inquietudes no son aisladas. Por ejemplo, vale la pena recordar las críticas que se lanzaron a Google en su conferencia anual Google I/O en el 2018. En esta, el desarrollador Alphabet Inc. mostró una versión beta de la herramienta Duplex, «un servicio experimental que permite a un asistente digital, realizar llamadas telefónicas, agendar citas, generar escritura automática de correos electrónicos, entre otras funciones»[45]. Para los usuarios, según se indicó, una herramienta que facilita ahorrar tiempo y esfuerzo a partir del uso de IA.

Si bien fue de buen recibo entre los adeptos por las herramientas de IA, ciudadanos ajenos a estos círculos criticaron fuertemente el uso de Duplex y sus implicaciones. Dentro de ellas, se planteó la vulnerabilidad de los datos y la información, pues estas herramientas tienen como propósito tácito la

[42] Valls Prieto, «Sobre la responsabilidad penal», 11.
[43] *Ibid.*, 16.
[44] *Ibid.*, 18.
[45] Bloomberg, «Inteligencia artificial de Google causa asombro y preocupación», *Portafolio*, 12 de mayo de 2018, https://www.portafolio.co/innovacion/el-robot-de-google-que-causo-estupor-517059.

recopilación de datos de los usuarios con la intención de ofrecer servicios comerciales adicionales a los ya prestados. Esta estrategia comercial, según algunos, no garantiza que la información entregada de manera voluntaria por los usuarios se custodie y administre en las formas en que obliga la ley.

En este punto, no se puede olvidar que Google ha sido reconvenido en varias oportunidades por diferentes autoridades en el mundo —entre ellas las colombianas— con relación al cumplimiento de los estándares en materia de *habeas data* para el uso y administración de los datos que les son confiados, como consecuencia de los servicios que brindan. A través de la Resolución 53593 de 2020, la Superintendencia de Industria y Comercio determinó que la política de tratamiento de información que maneja Google incumple con un 52,63 % de los requisitos que exige la regulación colombiana[46]. Por ello, se ordenó a esta compañía la adopción de estrictos mecanismos y procedimientos efectivos que garantizaran de manera adecuada la recolección, tratamiento y administración de los datos personales de sus usuarios residentes en Colombia.

Los peligros planteados no se han quedado solamente en el campo teórico. De hecho, existen ya precedentes judiciales respecto del uso de algoritmos para la determinación de riesgos en el campo del derecho penal que han dejado en evidencia tanto los beneficios que podrían traer como también las limitaciones que poseen estas herramientas y los inconvenientes que ocasionarían en la práctica jurídica.

IV. El caso State Wisconsin vs. Loomis

Wisconsin vs. Loomis ha sido catalogado como el primer caso en el que un tribunal de justicia ha tenido que pronunciarse con relación a la admisibilidad del uso de herramientas de inteligencia artificial dentro del proceso penal[47]. Eric Loomis fue acusado por la comisión de cinco delitos al estar involucrado en un tiroteo. Fue imputado por cargos de posesión de armas de fuego, intento de fuga y por conducir un vehículo sin el consentimiento de su propietario. Para fundamentar la pretensión de condena, la fiscalía aportó, entre otros elementos, un informe del algoritmo predictivo COMPAS.

[46] Superintendencia de Industria y Comercio, Resolución 53593 de 2020, «Por la cual se imparten órdenes dentro de la actuación administrativa 19-202397 en contra de Google LLC», 3 de septiembre de 2020.
[47] Supr. Court of Wisconsin, 881 NW2d 749 (Wisconsin 2016). Disponible en: https://www.courts.ca.gov/documents/BTB24-2L-3.pdf

En él se estableció que el acusado presentaba una calificación negativa pues tenía un alto riesgo de reincidencia.

Si bien Loomis no aceptó los cargos relacionados con el tiroteo y la tenencia de armas, admitió haber conducido un vehículo ajeno e intentar huir cuando fue detenido por un oficial de tránsito. En consecuencia, el juez de primera instancia lo condenó penalmente al ser considerado un peligro para la seguridad pública, y le impuso una pena de seis años de prisión, además de una pena de cinco años bajo libertad vigilada[48].

La decisión fue apelada por la defensa al considerar que el informe del algoritmo COMPAS era inadmisible como prueba para la imposición de la pena. Al respecto, se indicó que el informe de riesgos «(1) viola el derecho del acusado a ser sentenciado con base en información imprecisa, en parte debido a la naturaleza patentada de COMPAS, lo que impide evaluar su exactitud»[49], pues los resultados del algoritmo no eran susceptibles de contradicción. Adicionalmente, como es un instrumento patentado y posee un secreto comercial, no se divulga cómo se determinaron los riesgos mencionados en el informe y de dónde provenía su calificación; «(2) viola el derecho del acusado a una sentencia individualizada»[50], pues el *software* trabaja basándose en estadísticas grupales, por lo cual no era posible determinar la información específicamente al sentenciado; y «(3) utiliza indebidamente evaluaciones de género en las sentencias»[51].

Si bien todos los cargos presentados por la defensa fueron negados, la Corte Suprema de Wisconsin precisó que existe la posibilidad de que los algoritmos predictivos de riesgo amenacen las garantías sustanciales y procesales de los acusados, pues las partes no poseen información suficiente para contradecir los resultados de los informes y la calificación que realice de sus riesgos. Estos algoritmos se caracterizan por su principio de opacidad, por lo cual «no es posible establecer el peso, la valoración y ponderación exacta que un algoritmo de esta clase realiza con relación a las diferentes variables»[52].

[48] Roa Avella, Dinas-Hurtado y Sanabria-Moyano, «Uso de algoritmo COMPAS», 287.
[49] *Ibid.*, 287.
[50] *Ibid.*
[51] *Ibid.*, 288.
[52] *Ibid.*, 290.

A pesar de lo anterior, no deja de ser paradójico que el máximo órgano de justicia del Estado de Wisconsin haya admitido, y por ende valorado esta prueba, a pesar de que reconoció que el empleo de estos algoritmos trae consigo muchas limitaciones, debilidades e inconvenientes[53].

V. Toma de postura

El uso de algoritmos predictivos de riesgos genera dilemas. ¿Cómo se reconcilian con los principios básicos del sistema judicial, como el derecho a un juicio justo y el derecho a la defensa?, ¿es ético delegar decisiones cruciales a entidades no humanas sin un debido proceso legal?

El uso de herramientas para la predicción de las conductas punibles no es un asunto nuevo para el derecho penal. En 1876 Cesare Lombroso ya las nombraba en el derecho penal a través de su teoría del delincuente nato. Según esta teoría, hay personas que nacen con algunas características biológicas y psicológicas que las predisponen a la delincuencia[54]. En este sentido se podría reconocer a un potencial delincuente por ciertos signos físicos, como una frente inclinada, orejas grandes, etc. Como se puede observar, esta teoría se basa en estereotipos y prejuicios, lo que podría significar prácticas discriminatorias en el sistema de justicia penal.

Si bien no se pueden desconocer las utilidades que podría traer la implementación de *softwares* predictivos de riesgos penales, tampoco se puede negar hoy que su uso puede llevar a prácticas discriminatorias que no están alejadas de la realidad que planteó Lombroso en el siglo XIX.

Esta clase de herramientas tecnológicas para la predicción de la comisión de delitos puede implicar más inconvenientes que beneficios para el sistema de justicia penal. Esto, no solo por los peligros que ya fueron mencionados en acápites anteriores, sino, además, porque podría representar un retroceso en los principios de un derecho penal de corte liberal[55] como el que tenemos en la actualidad. Por un lado, el principio del derecho penal de acto y no de autor podría verse afectado.

---

[53] Belloso Martín, «Algoritmos predictivos al servicio de la justicia», 21.
[54] Nodier Agudelo Betancur, «Evolución del método dogmático», *Lecciones de Derecho Penal. Parte General*, (Bogotá: Universidad Externado de Colombia, 2012), 192.
[55] Carlos Kunsemuller, *El Derecho Penal Liberal. Los Principios Cardinales* (Valencia, Tirant Lo Blanch, 2018).
El derecho penal de corte liberal es una rama del sistema legal que refleja los principios fundamentales del liberalismo en el ámbito de la justicia criminal. Este enfoque se basa en la idea central de proteger los derechos individuales y limitar la intervención del Estado en la vida de los ciudadanos, incluso cuando se trata de la imposición de sanciones penales.
En el marco del derecho penal liberal, la principal función del sistema de justicia criminal es la protección de los derechos fundamentales de los individuos, como la vida, la libertad y la propiedad. Se enfoca en castigar conductas que infringen esos derechos y amenazan la paz y seguridad de la sociedad. Sin embargo, la intervención del Estado se limita a lo estrictamente necesario para garantizar la justicia y evitar abusos de poder.

Al respecto, es importante recordar que en el derecho penal de autor «el sujeto responde por su ser, por sus condiciones sicofísicas o su personalidad, que se consideran peligrosos para la sociedad, por su supuesta inclinación natural al delito, con un criterio determinista, de modo que el sujeto resulta condenado por la naturaleza a sufrir las condenas penales, por obra del destino y, por tanto, de modo fatal o inevitable. En este orden de ideas no es relevante que aquel cometa infracciones, sino que tenga la potencialidad de cometerlas»[56].

El derecho penal de autor y la predicción de riesgos penales a través de la inteligencia artificial pueden relacionarse, considerando que ambas temáticas giran alrededor de la identificación de potenciales actos delictivos. El derecho penal de autor se focaliza en el individuo, sus características físicas, de dónde proviene y de sus circunstancias personales para determinar su propensión a cometer delitos. Por otro lado, los *softwares* de inteligencia artificial utilizados en la predicción de riesgos penales pueden incorporar tanto rasgos individuales, raza, género, ideología política, etc., como patrones de comportamiento para prever la ocurrencia de ciertos delitos[57].

En principio, podría entenderse que esta clase de herramientas tecnológicas contravienen el derecho penal de acto, que ha inspirado al derecho penal moderno, y presupone que «el sujeto responde por sus actos conscientes y libres, es decir, por la comisión de conductas conocidas y queridas por él mismo, previstas expresa y previamente en la ley como contrarias a bienes fundamentales de la sociedad y de sus miembros, y que hacen a aquel merecedor de una sanción»[58]. Sin embargo, debe recalcarse que, a diferencia del derecho penal de autor, la inteligencia artificial se centra en evidencias empíricas, cuantitativas y patrones detectados en datos existentes, por lo cual, las predicciones que emitan estos algoritmos, en parte, se podrían justificar, y defender sus resultados ante los estrados judiciales.

Por otro lado, el uso inadecuado de algoritmos de predicción puede cambiar la naturaleza del sistema de justicia penal al centrarse más en la anticipación y la prevención que en la responsabilidad individual. Esto puede desplazar el énfasis del castigo por hechos concretos, hacia la prevención de futuros delitos y plantear cuestionamientos sobre el respeto al principio de legalidad. Esto podría traducirse en la afectación de garantías fundamentales de este principio, como lo es el de *nullum*

[56] Sentencia C-077/06.
[57] Luis Alberto Gómez Castrillón, «La predicción del crimen: de Lombroso al Big Data», *Derecho Penal Contemporáneo,* n°. 69, (2019). Disponible en: https://xperta.legis.co/visor/rpenal/rpenal_55a5e37c113e46ea8f966b12592dfebe
[58] Sentencia C-077/06.

crimen nulla poena sine culpa[59]*.* Es decir, que las personas que sean seleccionadas por esta clase de herramientas tecnológicas, no lo serán por los actos que hayan cometido, sino por actos que potencialmente ocurrirán, y que, por lo tanto, no han generado todavía ningún daño antijurídico que sea susceptible de atención del derecho penal.

Desde un punto de vista ético, el uso de sistemas algorítmicos en el ámbito penal suscita preguntas fundamentales sobre la autonomía, la privacidad y la presunción de inocencia. La capacidad de un algoritmo para predecir la propensión de una persona a cometer un delito antes de que ocurra plantea la posibilidad de castigar a individuos por crímenes que aún no han cometido, lo que erosiona el principio de la presunción de inocencia[60]. Ante esto, no puede olvidarse que el uso de cualquier herramienta informática en el derecho debe ajustarse a las normas. En este sentido, no será posible el uso de herramientas, o incluso la adopción de decisiones que contravengan el principio de legalidad y el respeto del principio de culpabilidad, pues únicamente podrá ser considerada una persona culpable de un delito si hay pruebas suficientes que así lo indiquen[61]. A este respecto, los algoritmos de predicción de riesgos penales no deberían usarse para predecir la culpabilidad sin una base empírica sólida.

Frente a ello, no cabe duda de que se presenta un desafío para los desarrolladores de estos *softwares*. Por un lado, deben ser capaces de explicar cómo funcionan sus herramientas y cuán acertadas y confiables son las calificaciones que emiten de los riesgos. Esto requiere una comprensión más sólida de lo que está sucediendo en «la caja negra» del algoritmo y una capacidad para explicarlo en términos que los profesionales del derecho y los operadores jurídicos puedan entender, de tal manera que las decisiones que sean orientadas por esta clase de sistemas puedan ser explicadas a los ciudadanos.

Sin embargo, la responsabilidad para el uso adecuado de estas herramientas de evaluación de riesgos (Risk Assessment Tools o RATs, por sus siglas en inglés) no recae exclusivamente en aquellos que las fabrican. También existe un grado de responsabilidad por parte de las instituciones gubernamentales que son, al final, quienes las usarán en los sistemas de justicia penal. La convergencia de esfuerzos entre el sector privado y el público para el éxito en la implementación de

[59] Aforismo que consagra el principio de legalidad desarrollado por Paul Johann Anselm von Fauerbach, cuya traducción es «No hay delito ni hay pena sin ley».
[60] Solar Cayón, «Reflexiones frente a la aplicación», 28.
[61] Roa Avella, Dinas-Hurtado y Sanabria-Moyano, «Uso de algoritmo COMPAS», 293.

esta clase de herramientas puede implicar que los estándares de optimización y eficiencia en la justicia se eleven sin que se afecten derechos de los ciudadanos.

Una muestra de lo anterior son los esfuerzos de la Comisión Europea para la Eficacia de la Justicia (CEPEJ). Por ejemplo, en el año 2018 la CEPEJ emitió la *Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno*. De su contenido se puede extraer la necesidad de estas herramientas en los sistemas de justicia, siempre y cuando se garanticen principios esenciales como la no discriminación y el rechazo frente a cualquier IA que intensifique alguna discriminación entre individuos o grupo de individuos; así como la transparencia, la imparcialidad y la equidad a través de inteligencias artificiales que contengan métodos de procesamiento de datos accesibles y comprensibles, y que permitan auditorías externas[62]. Asimismo, el Parlamento Europeo, a través de la Resolución 2020/2016(INI) de 6 de octubre de 2021, en su *Informe sobre la inteligencia artificial en el derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales*, ha insistido en la implementación de la inteligencia artificial en el derecho penal y su utilización por parte de las autoridades policiales y judiciales[63].

VI. Reflexión final

La tecnología puede ofrecer avances significativos en los sistemas de justicia penal alrededor del mundo, pero su aplicación necesita ser guiada por principios éticos, legales y constitucionales. El uso de algoritmos predictivos debe equilibrar la eficiencia con el respeto a los derechos individuales y a los principios básicos de la justicia. La confianza en la inteligencia artificial en este contexto tiene que ir de la mano con la transparencia, la responsabilidad y la salvaguarda de los derechos fundamentales de los ciudadanos. La puesta en marcha de estas herramientas debe ser cuidadosamente regulada para evitar consecuencias negativas y garantizar un sistema de justicia que respete los valores fundamentales de una sociedad libre y justa.

[62] Commissione Europea Per L'efficienza Della Giustizia (CEPEJ), Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, adottata dalla CEPEJ nel corso della sua 31.ª Riunione plenaria (Strasburgo, 3-4 dicembre 2018) https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348

[63] Parlamento Europeo, Informe – A9-0232/2021, «Informe sobre la inteligencia artificial en el Derecho Penal y su utilización por las autoridades policiales y judiciales en asuntos penales», Resolución (20202/2016(INI)).

La implementación de algoritmos de predicción de riesgos penales en los sistemas de justicia penal puede ser una herramienta útil para mejorar la eficiencia operativa, identificar patrones de criminalidad y prever la posible reincidencia de los ciudadanos frente a algunos delitos. Sin embargo, no debemos ignorar que la incorporación de estas tecnologías en el sistema de justicia penal debe realizarse de forma que se respeten los derechos fundamentales de las personas implicadas. Para ello, resultará de gran importancia la colaboración entre el sector público y el privado para desarrollar e implementar normas claras y comprensibles que rijan el uso de estos algoritmos.

Asegurarse de que los algoritmos sean justos y que no perpetúen la discriminación o la injusticia es un desafío importante que deberá abordarse en las discusiones que se avecinen. Finalmente, los principios básicos del sistema de justicia penal, como el debido proceso, la presunción de inocencia y la proporcionalidad de la pena, deben seguir siendo respetados en todos los aspectos del sistema de justicia penal, incluyendo el uso de algoritmos de predicción de riesgos penales.

En última instancia, cualquier uso de algoritmos de predicción en el sistema de justicia penal debe estar guiado por un compromiso de hacer justicia de la forma más justa, eficiente y humana posible. Esto requerirá una cuidadosa consideración y un balance entre los beneficios potenciales de estas herramientas y la necesidad de proteger los derechos fundamentales y las libertades de todas las personas.

VII. Bibliografía

Agudelo Betancur, Nodier. «Evolución del método dogmático». En *Lecciones de Derecho Penal. Parte General.* Bogotá: Universidad Externado de Colombia, 2012.

Barrios, Facundo. «Resúmenes: XVIII Semana del derecho y la criminalística. Inteligencia artificial Deux Ex Machina». *Memorias forenses*, n.º 7 (2023): 1-2, https://doi.org/10.53995/25390147.1590.

Belloso Martín, Nuria. «Algoritmos predictivos al servicio de la justicia: ¿una nueva forma de minimizar el riesgo y la incertidumbre?». *Revista da Facultade Mineira de Direito* 22, n.° 43 (2019).

Blázquez Ruiz, Javier. «La paradoja de la transparencia en la IA: Opacidad y explicabilidad. Atribución de responsabilidad». *Revista Internacional de Pensamiento Político – I Época* 17 (2022).

Bloomberg. «Inteligencia artificial de Google causa asombro y preocupación». *Portafolio*, 12 de mayo de 2018, https://www.portafolio.co/innovacion/el-robot-de-google-que-causo-estupor-517059.

Bonsignore Fouquet, Dyango. «Sobre inteligencia artificial, decisiones judiciales y vacíos de argumentación». *Teoría & Derecho. Revista de Pensamiento Jurídico*, n.° 29.

Eubanks, Virginia. *Automatización de la desigualdad: cómo las herramientas de alta tecnología perfilan, vigilan y castigan a los pobres*. Nueva York: St. Martin´s Press, 2018.

Frischmann, Brett y Evan Selinger. *Reingeniería de la humanidad*. Cambridge: Cambridge University Press, 2018.

Gómez Castrillón, Luis Alberto. «La predicción del crimen: de Lombroso al Big Data», *Derecho Penal Contemporáneo*, n.° 69 (2019).

González-Álvarez, José Luis, Jorge Santos-Hermoso y Miguel Camacho-Collados. «Policía predictiva en España. Aplicación y retos futuros». *Behavior & Law Journal* 6, n.° 1 (2020).

Guerra Cáceres, Paula. «Algoritmos entrenados para ser racistas», *Pikara Magazine*, 23 de noviembre de 2022, https://www.pikaramagazine.com/2022/11/algoritmos-entrenados-para-ser-racistas/#:~:text=El%20sesgo%20de%20PredPol%20es,de%20dise%C3%B1o%20de%20un%20algoritmo.

Kunsemuller, Carlos. *El Derecho Penal Liberal. Los Principios Cardinales*. Valencia: Tirant Lo Blanch 2018.

Martínez Garay, Lucía. «Peligrosidad, algoritmos y debido proceso: El caso Estado vs. Loomis». *Revista de Derecho Penal y Criminología* 3, n.° 20 (2018).

Moreno Blanco, Natalia. ¿Efectivización de los cupos carcelarios?: aproximación al Sistema Prisma de la Fiscalía General de la Nación. Tesis de grado, Universidad de los Andes, 2019, https://repositorio.uniandes.edu.co/entities/publication/83c142ed-7fdf-4580-ab26-c91ef609d7b9.

Notaro, Laura. «"Algoritmos predictivos" y justicia penal desde una perspectiva italiana y europea». En *Derecho penal, inteligencia artificial y neurociencias*, coords. José Miguel Peris R. y Antonella Massaro. Roma: Roma TrE-PRESS, 2023.

O'Neil, Cathy. «Armas de destrucción matemática: Cómo los datos masivos aumentan la desigualdad y amenazan la democracia». Madrid: Capitán Swing Libros, 2017.

Ortiz de Zárate Alcarazo, Lucía. «Explicabilidad (de la inteligencia artificial)». *Eunomía, Revista en Cultura de la Legalidad*, n.° 22 (2022).

Pasquale, Frank A. y Daniell Keats Citron. «La segunda sociedad: debido proceso para predicciones automatizadas». *Legal Studies Research Paper Washington Law Review* 1, n.º 89 (2014).

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA y Londres, Inglaterra: Harvard University Press, 2015.

Peñaranda Ramos, Enrique. «La pena: nociones generales». En *Introducción al derecho penal*, cord. Juan Antonio Lascuríin Sánchez. Navarra: Arazandi, 2015.

Reyes Alvarado, Yesid y Andrés Felipe Díaz Arana. «Tecnologízación del sistema de justicia penal en Colombia. Departamento de Derecho Penal y Criminología». Universidad Externado de Colombia. (Manuscrito), 2012.

Rincón Cárdenas, Erick y Valeria Martínez Molano. «Un estudio sobre la posibilidad de aplicar la inteligencia artificial en las decisiones judiciales». *Revista Direito GV* 19 (2023).

Roa Avella, Marcela del Pilar, Katherin Dinas-Hurtado y Jesús Eduardo Sanabria-Moyano. «Uso de algoritmo COMPAS en el proceso penal y los riesgos a los derechos humanos». *Revista Brasileira De Direito Processual Penal* 8, n.°1 (2022).

Rouhiainem, Lasse. *Inteligencia artificial: 101 cosas que debes saber sobre nuestro futuro*. Barcelona: Alienta, 2018.

Silva, Tarcizio. *Racismo algorítmico: inteligencia artificial y discriminación en las redes digitales*. Sao Paulo: Edições Sesc, 2022.

Solar Cayón, José Ignacio. «Reflexiones frente a la aplicación de la inteligencia artificial en la administración de justicia». *Teoría Jurídica Contemporánea* 6 (2021).

Valls Prieto, Javier. «Sobre la responsabilidad penal por la utilización de sistemas inteligentes», *Revista Electrónica de Ciencia Penal y Criminología*, n.° 24-27.

Jurisprudencia y citación legal (Colombia)

Superintendencia de Industria y Comercio, Resolución 53593 de 2020. 3 de septiembre de 2020.