

Ciudad de Córdoba, 20 de junio de 2024

XXXII CONGRESO NACIONAL DE DERECHO PROCESAL

Comisiones penales 1

Inteligencia artificial: proceso penal y derechos fundamentales (arts. 75, inc. 19 y 22, CN)

Uso de la inteligencia artificial en la prevención y persecución del delito: posibles conflictos para el proceso penal. - Afectación de garantías individuales de los investigados. Control de la legalidad del método. Reproducción en juicio y control de parte. Posibles dilemas éticos.

Ponencia:

El empleo de la IA en el marco de la Prevención e Investigación del delito

Breve síntesis de la propuesta:

Por medio de la presente ponencia pretendemos analizar la aplicación de medidas de investigación, potenciadas por el uso de Inteligencia Artificial, para la prevención e investigación del delito. Detallando brevemente el panorama actual; los posibles riesgos que se desprenden de su implementación, la postura de los tratados internacionales y de la Corte Interamericana de Derechos Humanos sobre la materia, para delimitar los principios y caracteres que deberían regir la implementación de estas modernas herramientas del proceso penal.

Nombre del autor: Ferrer Guillamondegui Ramón Agustín¹.

Correo electrónico: aferrer@mpf.gov.ar

Postulo para concursos de los premios Asociación Argentina de Derecho Procesal y Fundación de Estudios Superiores e Investigación (FUNDESI)

¹ Abogado-Especialista en Derecho Procesal por la Facultad de Derecho de la Universidad Nacional de Córdoba; Especialista en Crimen Organizado, Corrupción y Terrorismo por la Fundación General de la Universidad de Salamanca (España); Especialista en Justicia Constitucional y DDHH - IDC - Universidad de Bolonia; Maestrando en Derecho Procesal, Universidad Siglo XXI.

El empleo de la IA en el marco de la Prevención e Investigación del delito

Sumario: Introducción - Algunos ejemplos de Inteligencia artificial aplicada a la prevención e investigación del delito - Posibles efectos del uso de IA en la prevención e investigación del delito - El abordaje desde la óptica de los Tratados Internacionales - El criterio de la Corte Interamericana de Derechos Humanos - Principios y caracteres vinculados a la aplicación de IA en el proceso penal – Conclusiones

Introducción

El crimen, constituye un flagelo atemporal, que afecta con distinta entidad a todos los países del mundo y ello responde en parte, al hecho de que la creatividad criminal es maleable, flexible o adaptable, por lo que toma provecho prontamente de los avances y nuevas herramientas que brinda la tecnología. Por otra parte, las leyes que determinan el margen de actuación lícito de los organismos encargados de la prevención e investigación penal, se caracterizan por mantener una tendencia conservacionista y se actualizan cuando la problemática ya ha tomado entidad tal que afecta el orden social en su conjunto.

Esta particular realidad, genera como consecuencia, que los medios tradicionales de investigación tengan una escasa tasa de éxito en la persecución, atento a las facilidades que brindan los avances tecnológicos para eludir dichas investigaciones, lo que constituye un gran incentivo para la delincuencia. Frente a este panorama, muchos países han comenzado a regular legislativa o jurisprudencialmente medios extraordinarios de investigación, potenciados por el uso de inteligencia artificial (en adelante IA), como mecanismo para lograr mayor eficiencia y eficacia en las tareas de prevenir, investigar y sancionar estos ilícitos.

En el marco del presente trabajo, pretendemos analizar, en primer lugar, algunas de las herramientas de IA que actualmente se aplican; precisar cuáles son los posibles riesgos que conlleva su empleo; como así también, determinar si dichas medidas son acordes al sistema convencional y finalmente pretendemos establecer los principios y caracteres que debería respetar el uso o empleo de estas medidas en el marco de un proceso penal.

Algunos ejemplos de Inteligencia Artificial aplicada a la prevención e investigación del delito

Son numerosos los países han incursionado en el empleo de la IA como apoyo de las funciones de disuasión e investigación del delito. El análisis de estas aplicaciones nos permite tomar conocimiento del estado actual de la materia, tanto en nuestro país como en el mundo, de los beneficios y riesgos que se desprenden de su implementación.

En tal sentido, se ha recurrido a dicha tecnología para generar mapas del delito y predicción del crimen, con el objeto de predecir las áreas de la ciudad donde resulta más probable que se cometa un delito y de esta forma reforzar la prevención en dichas áreas, por lo que permite administrar y gestionar los recursos de las fuerzas de seguridad de una manera más eficiente y eficaz². Otras ciudades, incluso van más allá y utilizan la IA combinada con cámaras de circuito cerrado de videovigilancia para supervisar una diversidad de ambientes y actividades con el objeto de determinar las probabilidades de que una persona determinada se predisponga a cometer un delito, lo que les permite focalizar la prevención sobre dicho sujeto³. Estas herramientas, utilizadas por China en forma general, también han sido empleadas por los Estados Unidos en forma focalizada, para detectar posibles terroristas, por medio de un programa denominado FAST. Este programa analiza en forma remota, el pulso, la respiración, la temperatura de la piel, las expresiones faciales y pautas de comportamiento; luego de lo cual determina el grado de probabilidad de la persona se predisponga a concretar un ataque terrorista.⁴

² A modo de ejemplo podemos mencionar el software que utilizan algunas ciudades de Estados Unidos, denominado PredPol, <https://www.forbes.com.mx/predpol-el-primer-software-de-prediccion-del-crimen/>. Con similar finalidad, algunas ciudades españolas utilizan el software denominado Eurocop Cube, <https://iahuawei.xataka.com/asi-como-ia-puede-ayudar-crear-sociedad-justa/>; Alemania emplea una aplicación denominada Precobs; Italia, que utiliza XLAW; Gran Bretaña por su parte, emplea un software denominado Hart, desarrollado por la Universidad de Cambridge <https://www.lavanguardia.com/tecnologia/20190318/461013536935/inteligencia-artificial-vigilancia-predictiva-policia.html>

³ Un ejemplo de ello es la aplicación Cloud Walk, utilizada por China, identifica a las personas y sigue sus movimientos y dependiendo de los lugares que visite o frecuente establece el nivel de riesgo que representa el sujeto. Conforme lo consultado en Hernández M. Inteligencia Artificial y Derecho Penal. Actualidad Jurídica Iberoamericana N° 10 bis, junio 2019, ISSN: 2386-4567, pp. 792-843. Más recientemente el país asiático ha recurrido a Sense Time un sistema de vigilancia mediante inteligencia artificial de China conocido como "sistema de crédito social ciudadano.

⁴ Redacción RFID-Spain.com (26 de septiembre, 2008) "El Departamento de Seguridad Nacional de EEUU anunció que posee un nuevo detector de ansiedad para descubrir terroristas"; recuperado de

Por otra parte, México ha comenzado a utilizar drones para efectuar patrullajes, identificación y seguimiento de sospechosos lo que le ha permitido el arresto de 500 criminales, gracias a las imágenes grabadas por los drones, las cuales son aplicadas a un sistema que, a través del reconocimiento facial, permite identificar los datos de la persona. Según los estudios realizados, esta implementación ha logrado reducir en un 10 % del índice de criminalidad general y un 30 % de robos domésticos con respecto al 2017.⁵

También se ha utilizado la inteligencia artificial para la detección de posibles denuncias falsas, a modo de ejemplo, la Policía Nacional de España, utiliza la aplicación Veripol⁶, que es capaz de calcular la probabilidad de que una denuncia sea falsa, al analizar en el texto las palabras, expresiones, conceptos y características de la descripción de los hechos y al compararlo con denuncias cuya falsedad se ha comprobado, arroja un porcentaje de probabilidad e indica al personal policial cuales son los puntos sobre los que deben pedirse precisiones al denunciante.

Otra de las herramientas que dotadas de inteligencia artificial para la detección de mentiras es iBorderCtrl, un sistema financiado por la Unión Europea, destinado al control fronterizo del territorio comunitario; que analiza el lenguaje no verbal de los viajeros, sus expresiones faciales, en tiempo real, mientras estos responden a las preguntas de los agentes fronterizos de los aeropuertos. Lo que permite determinar si la persona está diciendo la verdad o está mintiendo, ayudando así a detectar comportamientos sospechosos. Lo cual se ve reforzado por el análisis de datos biométricos como huellas dactilares, para ayudar a corroborar la identidad de las personas.⁷

También se ha utilizado para detectar posibles vinculaciones o patrones comunes entre denuncias e investigaciones, para determinar conexidades,

<http://www.rfid-spain.com/articulo/61380//policia/el-departamento-de-seguridad-nacional-de-eeuu-anuncio-que-posee-un-nuevo-detector-de-ansiedad-para-descubrir-terroristas>

⁵ Hazel Villalobos Fonseca; El desarrollo tecnológico en materia policial: una receta de éxito para la prevención del delito Revista de Relaciones Internacionales, Estrategia y Seguridad; versión impresa ISSN 1909-3063. doi.org/10.18359/ries.4243

⁶ Este programa tiene una precisión superior al 90%; conforme nota titulada "VERIPOL: la herramienta de la Policía para detectar denuncias falsas"; de fecha 26 Marzo, 2019. Recuperado de <https://confilegal.com/20190326-veripol-la-discreta-herramienta-que-la-policia-nacional-utiliza-para-detectar-denuncias-falsas-empieza-a-dar-sus-frutos/>,

⁷ Conforme nota publicada por Justo Álvaro en <https://blogthinkbig.com/veripol-iborderctrl-inteligencia-artificial-mentiras>, consultada el 13/12/2020

que pueden surgir por el lugar de comisión del delito, por la identidad de la persona denunciada o las características de identificación brindadas, por el modus operandi del caso y también por el tipo de arma empleada y los vehículos utilizados.⁸ Por su parte, en nuestro país, el Ministerio Público de la Provincia de Buenos Aires se encuentra en tratativas para implementar dicho sistema, conforme se desprende del Informe de Gestión del organismo⁹.

En otro sentido, se ha implementado para detectar posibles pedófilos, mediante la creación de un personaje virtual, que por medio de un chatbot autónomo e imágenes o videos generados por realidad virtual, simula ser de una niña de 10 años, con rasgos filipinos, a la cual denominaron “Sweetie”, para que los delincuentes sexuales que pretendían tomar contacto con ella por medio de video-llamadas, creyeran que estaban hablando con una niña de verdad. Es el propio sistema el que recibe las propuestas, determina la modalidad de las conversaciones, videos e imágenes que se envían, recopila la información en los casos en que detecte situaciones delictivas.¹⁰

Finalmente, debemos referir al uso de malware o software maliciosos, por parte del estado, que implican el uso de virus informáticos o troyanos, denominados Network Investigative Technique (NIT), que se infiltran en las computadoras o dispositivos del investigado, recopilan información y la remiten a los organismos encargados de la investigación. Sobre el uso de estos sistemas, en Estados Unidos se han generado debates, uno de ellos con motivo de la Operación Pacifier, que se enfocó en la red de abuso infantil en una deep web conocida como Playpen. El troyano permitió romper el anonimato que brindaba la red e identificar a los usuarios; al ser sometidos a juicio, la defensa argumentó que la orden que habilitaba el uso del troyano excedía la jurisdicción de la magistrada que la emitió y que la operación constituía una búsqueda ilegal, sin embargo, los procedimientos se validaron

⁸ Es el caso de Colombia, que utiliza un software denominado Fiscal Watson y actualmente opera en las ciudades de Ibagué, Bogotá, Cali y Bucaramanga; conforme Flórez Rojas, M.L. y Vargas Leal, J. (2020). El impacto de herramientas de inteligencia artificial: un análisis en el sector público en Colombia. En C. Aguerre, (Ed.). Inteligencia Artificial en América Latina y el Caribe.

⁹ Informe de Gestión 2019 Pag. 95 y ss. del informe consultado en <https://www.mpba.gov.ar/files/content/Informe%20de%20Gestion%202019.pdf>, el 14/12/2020

¹⁰ Muñoz I. (13 marzo, 2018) Sweetie, la niña virtual que caza a pedófilos cibernéticos, quiere colaborar con la Policía; recuperado de <http://www.upsocl.com/mundo/esta-es-sweetie-una-cazadora-de-pedofilos-que-busca-ayudar-a-la-policia-a-proteger-ninos-indefensos/>

en función de la buena fe de los agentes del FBI y la gravedad de los delitos investigados justificaban la admisión de la evidencia obtenida.¹¹

Posibles efectos del uso de IA en la prevención e investigación del delito

En el plano social: Se advierte que el uso de estas técnicas tiene entidad para afectar derechos individuales y sociales, el empleo de sistemas de videovigilancia dotados de IA para generar sistemas de clasificación social (como ocurre en China) y/o el uso de virus informáticos que recopilen y analicen información personal en forma constante (spyware) tiene un efecto paralizador sobre derechos humanos y libertades fundamentales, incluida la participación pública y con ella la libertad de expresión, libertad de reunión, de manifestación.

Ello debido a que, estas modernas técnicas de vigilancia generan el efecto de un panóptico¹² digital, que potencia la sensación de exposición y de control, reduciendo el ámbito de libertades individuales. Por lo que, crea un clima de autocensura y miedo, en el que todos los individuos pueden ser tratados como sospechosos; implican una operación de pesca masiva, al ser aplicado en forma generalizada y sin una sospecha razonable previa que justifique dicha recopilación de información. Por tal motivo, la mayoría de los países prohíben el uso o empleo de sistemas de IA para la evaluación o clasificación de personas físicas o grupos de personas, en función de su comportamiento social o de sus características personales o de personalidad conocidas, deducidas o previstas¹³

En lo relativo a las garantías individuales: si bien resulta evidente que la implementación de medios de investigación potenciados por IA, tiene entidad para afectar derechos fundamentales, se debe considerar que tales derechos no son absolutos y en tal sentido se ha pronunciado la Corte Interamericana

¹¹ Se puede consultar el caso United States of America, Plaintiff, v. Jay Michaud, Defendant. Caso NO. 3:15-cr-05351-RJB – de fecha 28/01/2016. Similares argumentos se utilizaron para validar la orden en el caso United States of America, v. Alex Levin, Defendant Criminal Action NO. 15-10271-WGY 05-05-2016; en el cual se reafirmó la facultad estatal de recurrir al uso de técnicas de hacking judicialmente aprobadas para la investigación de crímenes graves.

¹² Diseño arquitectónico carcelario, efectuado por el filósofo Jeremy Bentham, para generar la sensación de control permanente en los internos y de esta forma facilitar el orden interno, pues la sensación de ser observado disminuía la predisposición de los presos a infringir las normas. La idea es retomada por Michel Foucault, en su obra Vigilar y castigar de 1975.

¹³ Conforme el Art. 5 inc C de las normas armonizadas en materia de inteligencia artificial Por parte del Parlamento Europeo https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_ES.pdf; pag. 185.

al señalar que: el derecho a la vida privada no es un derecho absoluto y, por lo tanto, puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias. Por ello, las mismas deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias en una sociedad democrática.¹⁴ Por lo cual, si bien este aspecto condiciona la modalidad de implementación, no resulta un óbice para la regulación.

En el marco del proceso: Por otra parte, el uso de herramientas dotadas de inteligencia artificial, en el marco de un procedimiento, puede generar situación de indefensión, en aquellos casos en los que se empleen herramientas de IA que emplee algoritmos de caja negra¹⁵. Pues, en estos casos, estaremos frente a una conclusión de la que se desconocen los motivos o el análisis interno que llevó al sistema a arrojar ese resultado, por lo que el acusado, no tendrá opciones reales de rebatir o impugnar la decisión que ofrezca la prueba algorítmica.¹⁶

Otro de los inconvenientes, está dado por la denominada asimetría o desequilibrio cognoscitivo; pues los organismos estatales, tendrán los fondos suficientes como para garantizar el acceso a la tecnología más moderna, que no estará al alcance de la defensa¹⁷.

Finalmente, existen riesgos vinculados a la reducción del valor de la prueba colectada, la que estará supeditada al resultado que se desprenda de una batalla entre expertos, ingenieros, programadores, informáticos o peritos que analicen y concluyan sobre la fiabilidad del sistema IA utilizado en el caso, frente a otros que nieguen o minimicen la verosimilitud de los resultados, lo que obligaría al juez a tener que tomar una posición de árbitro en una

¹⁴ Corte Interamericana de Derechos Humanos caso Fernández Prieto Y Tumbeiro Vs. Argentina, sentencia de 1 de Septiembre de 2020, parr. 105.

¹⁵ Aquellos en los que el programa brinda los resultados para el cual fue diseñado, sin informar el procedimiento, los motivos o las razones por las cuales arribó a ese determinado resultado y por los cuales descartó otros posibles

¹⁶ En similar sentido se pronuncia Nieva Fenoll al resaltar la importancia de la “desclasificación de los algoritmos” como garantía fundamental del sistema y del derecho de defensa, pues no es posible elaborar una mínima estrategia de defensiva si no se puede conocer cómo decide la máquina. Nieva Fenoll, J. (2018). Inteligencia artificial y proceso judicial, Marcial Pons, 2018.

¹⁷ Quattrocchio, S. (2019). Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo. Revista Ítalo-española de Derecho Procesal, vol. 2, 1 y ss.(pag. 12)

discusión que no versará sobre aspectos jurídicos, sino sobre materias que le resultan absolutamente ajenas a su formación letrada¹⁸.

El abordaje desde la óptica de los Tratados Internacionales

Si bien, la mayoría de los tratados internacionales, suscriptos por nuestro país, tienden a proteger al ciudadano frente a posibles excesos o ejercicios abusivos del poder punitivo del estado; también podemos advertir que existen otros, que han promovido la regulación de medios especiales de investigación, para garantizar mayor eficiencia y eficacia en la investigación de delitos complejos. En tal sentido, la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas, aprobada en Viena, el 19 de diciembre 1988, ya preveía en su Art., 3 apartado 6 que las Partes se esforzarán por asegurarse de que las facultades legales relativas al enjuiciamiento de personas, se ejerzan para dar la máxima eficacia a las medidas de detección y represión respecto de los delitos contemplados en ella, teniendo debidamente en cuenta la necesidad de ejercer un efecto disuasivo en lo referente a la comisión de esos ilícitos. Además, el Artículo 24 de la citada convención, alude a que las medidas que esta prevé no constituyen una limitación para los Estados, que podrán adoptar otras más estrictas o rigurosas, si resultan convenientes o necesarias para prevenir y eliminar el tráfico ilícito.

Por su parte, la Convención Internacional contra la Delincuencia Organizada Transnacional, celebrada en Palermo en diciembre del año 2000, hace expresa alusión a técnicas especiales de investigación, en el primer apartado de su art. 20, mencionando la vigilancia electrónica o de otra índole, con objeto de combatir eficazmente la delincuencia organizada. En el mismo sentido, la Convención de las Naciones Unidas contra la Corrupción, adoptada en Nueva York, el 31 de octubre de 2003, prevé en su Artículo 50 diversas técnicas especiales de investigación y alude entre otras a la vigilancia electrónica o de otra índole.

En función de lo analizado, podríamos afirmar que los tratados internacionales, si bien no regulan expresamente el uso de inteligencia artificial, en el marco de la investigación penal, implícitamente, toleran la

¹⁸ Ob. Cit. (pág. 16)

regulación de medios para determinados ilícitos vinculados al crimen organizado. Ello, pese a que su implementación implique afectar, en mayor medida, derechos y garantías individuales, pero exige que estos medios conlleven una justificación objetiva, legítima, razonable y proporcionada.

El criterio de la Corte Interamericana de Derechos Humanos

Recientemente, el organismo internacional se ha pronunciado en el Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia¹⁹ y entre los fundamentos brindados se expresa su preocupación por el empleo recurrente de softwares de captura de datos y vigilancia de dispositivos por parte de los servicios de inteligencia, lo que facilita prácticas como el monitoreo masivo de individuos, que a menudo se realiza de manera clandestina, permitiendo una interferencia arbitraria y abusiva en su vida privada sin justificativa legítima²⁰.

Sin embargo, no prohíbe el uso de tales herramientas, pero establece parámetros para su empleo, al indicar que, los servicios de inteligencia deben demostrar la existencia de interés público, con el fin de evitar que el uso responda a intereses personales o privados o se realicen sin objetivos legítimos. Reforzando este punto expresa que la consolidación del sistema internacional de protección de los derechos humanos ha puesto fin a los tiempos en que la invocación de justificaciones como la defensa de la seguridad nacional y el orden público legitimaba a los Estados para intervenir discrecionalmente en los derechos y garantías de los ciudadanos. Las circunstancias que autorizan la restricción del ejercicio de un derecho deben estar claramente prescritas por la ley, de conformidad con el artículo 30 de la Convención²¹.

Además, establece que dicha Ley debe prever las condiciones y restricciones para su empleo, de acuerdo con los estándares de derechos humanos. Además, su uso debe estar sujeto a criterios de necesidad, razonabilidad y proporcionalidad, así como al debido control judicial previo, para anticipar y mitigar posibles riesgos para los derechos fundamentales de

¹⁹ Corte IDH. Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 18 de octubre de 2023. Serie C No. 506.

²⁰ Ob cit párrafos 106 y 107

²¹ Ob cit párrafo 116.

las personas afectadas; inhibir usos potenciales indebidos, abusivos o ilícitos y exigir una mayor rendición de cuentas por parte de los servicios de inteligencia²².

Principios y caracteres vinculados a la aplicación de IA en el proceso penal

En función de los parámetros detallados precedentemente, se pueden esbozar los principios que deberían regir la aplicación de las herramientas dotadas de inteligencia artificial, en el marco de la prevención e investigación del delito, orientados a evitar su empleo arbitrario y reforzar su carácter excepcional.

Entre los principios que deben regir su aplicación, se encuentran el de necesidad, razonabilidad y proporcionalidad. Con relación al primero de ellos, podrá considerarse necesaria la disposición de estos medios, cuando sean indispensables para conseguir el objetivo propuesto; lo que implica que la información y los datos que permitirían obtener estas herramientas de investigación, no se podrían obtener por los medios tradicionales. En cuanto a la razonabilidad, puede ser analizada desde el punto de vista de la investigación, en el sentido de que sea adecuado según las particularidades y complejidades que presente la investigación. Finalmente, la proporcionalidad exige que la investigación posea una entidad tal que justifique la implementación de estas medidas.

Además, se desprenden una serie de caracteres que deben regir la aplicación de estas técnicas, como ser la Legalidad, por cuanto debe estar habilitado legalmente el empleo del medio de investigación que pretenda emplearse; Jurisdiccionalidad, dado que la decisión sobre su aplicación y el control de la implementación debe ser efectuado por un órgano jurisdiccional, cuando la medida tenga entidad para afectar derechos y garantías constitucionales (lo que ocurrirá por ejemplo si se decide emplear un troyano o sistema de video vigilancia cerrado; pero no en los casos en los que la IA se limite a determinar correlaciones entre investigaciones, o generar mapas del delito); Excepcionalidad, lo cual implica que el empleo de IA en el proceso no debe ser la regla, su procedencia no debe operar como la primera opción de

²² Ob cit. párrafo 108

los organismos encargados de llevar a cabo la investigación penal, vinculado con dicho carácter se encuentra el de Subsidiariedad, pues solo deberá recurrirse a ella cuando su implementación sea estrictamente indispensable para conseguir el objetivo propuesto y este no pueda alcanzarse por otros medios menos lesivos; Idoneidad del medio empleado para alcanzar los fines perseguidos, en tanto se encuentre acreditado el porcentaje de fiabilidad de la información obtenida por dicha herramienta y, finalmente, el de Temporalidad, que implica que su implementación debe poseer un lapso temporal determinado o determinable; la utilización que se dispone debe ser concreta y precisa.

Conclusiones

Conforme a lo expuesto, se puede advertir que:

- El uso de la inteligencia artificial, tiene potencial para mejorar la eficiencia y la eficacia de la prevención e investigación del delito.

- Numerosos países han comenzado a implementarla, con distintos objetivos y alcances, logrando resultados satisfactorios.

- Los riesgos que se derivan de su implementación, podrían eliminarse o restringirse, por medio de la prohibición de determinados usos de la IA, que impliquen riesgos inaceptables; por medio de la previsión normativa y la exigencia de una autorización judicial previa, para aquellos que puedan afectar garantías constitucionales; y por medio de la restricción del empleo de herramientas que empleen algoritmos de caja negra.

- Los Tratados Internacionales y la propia Corte Interamericana de Derechos Humanos, no prohíben el uso de estas herramientas, pero establecen condiciones para su aplicación, entre las cuales se pueden mencionar la previsión legal, el respeto a los criterios de necesidad, proporcionalidad y razonabilidad.

- Además de ello, la implementación de herramientas de IA en el marco del proceso penal, deberá respetar los caracteres de Legalidad; Jurisdiccionalidad; Excepcionalidad; Subsidiariedad y Temporalidad