La inteligencia artificial (IA) y la evidencia digital en el Proceso Penal
Artificial intelligence and digital (IA) and digital evidence in Criminal Proceedings.

Por. **Hernández, Plinio**
Universidad de Panamá
Centro Regional Universitario de Coclé
Panamá
Correo: plinio.hernandez@up.ac.pa / leyesatuservicio@gmail.com
ORCID: https://orcid.org/0009-0008-3679-4312

Entregado: 22 de mayo del 2024
Aprobado: 8 de julio del 2024
DOI https://doi.org/10.48204/j.aderecho.n54.a6418

Resumen

El presente artículo analiza como la Inteligencia Artificial (IA) está transformando los procesos penales en el análisis y procesamiento de la evidencia digital, utilizando patrones que podrían pasar desapercibidos para los humanos, mediante algortimos entrenados para detectar actividades sospechosas y/o delictivas.

El uso del la IA en el manejo de la evidencia digital debe manejarse por supuesto respetando derechos humanos y éticos; garantizandole al proceso penal transparencia, prohibiendo sesgoz discriminatorios, privacidad y ayudando al juez en la valoración de evidencias.

Abstract

This article analyzes how Artificial Intelligence (IA) is transforming criminal processes in the analysis and processing of digital evidence, using patterns that could go unnoticed by humans, through algorithms trained to detect suspicious and/or criminal activities.

The use of AI in the management of digital evidence must of course be managed respecting human and ethical rights; guaranteeing transparency in the criminal process, prohibiting discriminatory biases, privacy and helping the judge in the evaluation of evidence.

Palabras clave: Evidencia digital, inteligencia artificial, proceso penal, algoritmos, privacidad, principios, ciberdelincuencia.

Key words: Digital evidence, artificial intelligence, criminal process, algorithms, fundamental guarantees, principles, cybercrime.

I. Introducción

La Inteligencia Artificial (en adelante IA), tiene la capacidad de procesar grandes volúmenes de datos y extraer pratones significativos, lo que ha traído nuevas posbilidades en la investigación y análisis de las evidencia digitales.

La evidencia digital incluye datos obtenidos de dispositivos electrónicos, redes sociales y otras plataformas en línea, posicionándose en los procesos penales.

Sin embargo, la naturaleza de éstas evidencias plantea desafíos únicos en términos de autenticidad, integridad y admisibilidad en el juicio. A medida que los penalistas se enfrentan a estas nuevas realidades, la comprensión, aceptación y estudio de la interacción de la IA y la evidencia digital se convierte en un requisito indispensable para el abogado digital del siglo XXI.

Finalmente éste artículo se propone analizar la vinculación entre la IA y la evidencia digital en el proceso penal, a fin de proporcionar nuevos conocimientos que permita al penalista comprender que podemos tener de aliado a la tecnología para la búsqueda de la verdad y la justicia, por supuesto dejando claro la imperiosa necesidad de la urgente capacitación en el tema, su uso responsable y ético.

II. La Evidencia Digital en el Proceso Penal

La evidencia digital ha puesto al proceso penal ante una encrucijada jurídica con relación a la adapción de los medios probatorios tradicionales a la era digital. Existe diferencia entre evidencia física y evidencia digital, en primer término la evidencia física es tangible mientras que la evidencia digital no lo es (sí podrá serlo el soporte que la almacena pero no el dato en sí). Esta última es volátil, ya que es fácil modificarla, eliminarla, alterarla, lo que es necesario contar con herramientas de recolección más sofisticadas y de personal experto- a diferencia de la evidencia física que puede tomarse simplemente. Cabe explicar que cuando un usuario elimina un archivo en una computadora o dispositivo móvil existe la posibilidad de recuperarlo, por lo que existen archivos que, aunque a primera vista estén borrados pueden recuperarse mediante técnicas forenses, lo que involucra mayor complejidad para las evidencias digitales.

La evidencia física a diferencia no es posible obtener la clonación exacta como sucede con la evidencia digital.

La Corte Interamericana de Derechos Humanos ha señalado que los medios probatorios no deben ser ajenos a los avances tecnológicos.

Una de las principales diligencias judiciales de investigación consiste en ordenar la clonación y análisis forense de los discos duros y elementos periféricos de equipos informáticos aprehendidos tras un registro, así como de cualquier otro dispositivo de comunicación o almacenamiento.

La información que puede contener un archivo 8documento, video, fotos) no es solo la que un simple usuario puede observar sino que existen metadatos que no son conocidos por el ojo del usuario.Son los datos acerca de los datos, pro ejemplo, en una foto el dato que percibe cualquier persona es la imagen, pero los metadatos es la información como las coordenadas GPS del lugar en donde se tomó la foto, el modelo de la cámara que se utilizó, la fecha y hora, el software que se implementó para editar la imagen, el usuario utilizado, etc.

Los metadatos se pueden observar y recolectar mediante herramientas forenses como: software EXIF reader, EXIF Viewer, EXIF Image Viewer, FIV Forensic Image Viewer, entre otros, con éstos software se han podido descubrir archivos de imagen que contenían fotos a la cual se le habían agregado mendajes que eran practicamente invisibles al ojo humano.

Dado que es posible alterar un archivo siendo muy difícil su detección, existe una herramienta forense mediante un algorimo matemático de autenticación hexadecimal denominado HASH, que transforma cualquier bloque arbitrario en una seire de caracteres con una longitud fija; éstas son MD5, SHA1 y SHA256, significa que el archivo sufre alguna modificación, por más mínima que sea, el resultado que arroja el algoritmo es completamente diferente permitiendo detectar aquellas modificaciones realizadas al archivo.

III. BIT BIT

Es la copia forense, herramienta que permite copiar de manera total y exacta la información contenida en un disco rígido, en una o más copias; que deben ser manipuladas por expectos forenses en manejo de evidencia digital.

Como consecuencia la pérdida de la información es casi imposibl y permite a la defensa, fiscalía, el juez y el querellante tener accseso a las bit bit, las cuales pueden garantizarseles que son copias exactas de la original, lo que resulta ser una característica ventajosa de la evidencia digital, gracias al algoritmo conocido como HASH.

IV. Necesidad de adoptar un éstandar internacional para la admisibilidad de la evidencia digital.

La evidencia digital requiere una análisis minucioso y detallado de cómo se crea, recolecta, protege y finalmente como se presenta en el proceso penal, para que sea admitida.

La mayoría de las cortes federales de los Estados Unidos de Norteamérica han evaluado la admisibilidad de las evidencias digitales si se logra demostrar que la misma cumple con el Federal Rule of Evidence, son un conjunto de normas que regulan la admisibilidad de pruebas en los tribunales federales, fue adoptada en 1975, estas reglas abarcan aspectos como la relevancia de la evidencia, los privilegios, la competencia de los testigos.

La adopción de un estándar internacional para la evidencia digital permitirá claridad y consistencia para la recolección y presentación de evidencia, integridad y autenticidad, mejora de prácticas forenses aumentando la confianza en los resultados obtenidos.

V. Principios del G8 para el manejo y lineamientosde la evidencia digital.

Los principios del G8 para el manejo de la evidencia digital es vital para asegurar la integridad y validéz de los resultados en el contexto forense. Estos principios ratificados por los países miembros del G8, se enfocan en la aplicación rigurosa de técnicas forenses y procedicimientos estandarizados.

En primer lugar, se enfatiza que todos los procedimientos forenses genrales deben aplicarse al tratar con evidencia digital. Asegurando que las prácticas utilizadas sean consistentes y confiables. Además, se establece que la recolección de la evidencia digital no debe alterar su contenido, lo que es crucial para mantener la autenticidad de la prueba.

Otro principio es que cualquier persona que acceda a la evidencia digital original debe estar debidamente entrenada.

Esto minimiza el riesgo de manipulación accidental y asegura que la evidencia se maneje correctamente. Asimismo, toda actividad relacionada con la recolección, almacenamiento y transferencia de evidencia debe ser documentada de manera meticulosa, lo que permite una revisión y auditoría efectivas.

Finalmente, establece que la responsabilidad sobre la evidencia digital recae en quien la posee, garantizando que se mantenga la cadena de custodia y se eviten posibles disputas sobre la validez de la evidencia presentada en un juicio. Estos lineamientos son esenciales para fortalecer la confianza en el uso de la evidencia digital en los procesos penales, promoviendo un enfoque más sistemático y profesional forense.

VI. El Proyecto "CTOSE" de la Unión Europea (UE).

El Proyecto CTOSE (Cyber Tools On-Line Search of Evidence) es una herramienta o guía de trabajo de la Comisión Europea; los puntos centrales son la recolección, análisis, almacenamiento y presentación de la evidencia digital. El principal interés de los países miembro como Francia, Inglaterra, Italia; etc, es contar con un esquema claro de Savoir Faire para el intercambio de evidencia digital en la comunidad europea.

VII. Principios para la admisibilidad de la evidencia digital.

Debe cumplir con los siguientes principios;

1. **Autenticidad:** una evidencia digital debe ser auténtica siempre y cuando se cumplan con dos (2) elementos. El primero que se haya generado y registrado en el lugar de los hechos y la segunda que no tenga signos de alterabilidad, es decir que los registros corresponda a la realidad y que sea un fiel reflejo de la original.
2. **Confiabilidad:** es confiable la evidencia digital si proviene de fuentes creíbles y verificables; significa equiparar el hecho con la arquitectura de computación en correcto funcionamiento. Es decir una prueba digital será confiable siempre y cuando el sistema que la produce no haya sido alterado y que esté en correcto funcionamiento al momento de recibir, almacenar o generar la prueba.

Para que el funcionamiento del sistema sea adecuado es necesario que cuente con una función que sincronice el registro de las acciones de los usuarios y que a su vez cuente con un registro centralizado e íntegro de los mismos.

3. **Suficiencia:** una prueba digital es suficiente si esta es completa, para ello es necesario contar con mecanismos de integridad, sincronización y centralización que permita observar una imagen completa de la situación objeto de análisis. Es necesario para lograr eso hacer una verdadera correlación de eventos definida como el establecimiento de relaciones coherentes y consistentes entre diferentes fuentes de datos para establecer y conocer eventos ocurridos en una arquitectura o procesos.

VIII. Apego y respeto por las leyes y reglas del poder judicial

Toda evidencia digital debe cumplir con los requisitos enunciados en nuestros códigos de procedimientos. No sólo deberá ser auténtica, confiable y suficiente sino que debe respetar toda la normatividad legal vigente.

IX. Ventajas del uso de IA para la investigación forense de la evidencia digital.

La IA puede ayudar a identificar, documentar e interpretar volúmenes masivos de evidencia digital a través de herramientas de procesamientos de datos, machine learning.

Una de las principales ventajas al utilizar IA en la recolección. De evidencias digitales es que permite al perito informático forense analizar grandes volúmenes de información y encontrar patrones y conexiones que serían muy difíciles detectar manualmente; por ejemplo, si se investiga fraudes financieros. La IA puede analizar en segundos millones de transacciones para identificar patrones inusuales o sospechosos.

Además puede ayudar con precisión y confiabilidad al recolectar la evidencia digital; ya que utiliza algoritmos avanzados y técnicas de aprendizajes automáticos para un caso específico a resolver.

Otra ventaja de utilizar IA en la recolección de evidencia digital es su capacidad para aprender y perfeccionarse a medida que se procesan más datos, los algoritmos se hacen más precisos. Es importante tener en cuenta que el tratamiento de la evidencia digital requiere conocimiento y cumplir con marcos de prácticas existentes llevadas a cabo por profesionales informáticos forenses quienes están certificados en el tratamiento de las mismas.

No olvidemos que la prueba digital presenta especificidades propias que la hacen diferentes a otros tipos de pruebas, es muy frágil ya que puede ser fácilmente eliminada o modificada sin dejar rastros, reproducible porque pueden hacerse copias de esa información y ser siempre original, y anónima ya que no se puede vincular a una persona, excepto que tenga firma digital incoporada en el documento. Por lo que crucial estar capacitado y seguir los pasos para su recopilación donde la información recabada sea la misma en el tiempo y garantice la cadena de custodia (quien la extrajo, porqué, a quién se la entregó, etc).

X. Cómo se recopila la evidencia digital.

La evidencia digital debe tener validéz y no tener vicios de nulidad y es aquí donde el especialista debe ser cuidadoso.

Debe recopilar la evidencia digital en la escena, respetando las técnicas de recopilación, preservación y conservación manteniendo la integridad para su correcto análisis posterior.

A continuación, detallo los pasos en la recolección de la evidencia digital:

Paso 1: Asegurar la Escena. Para asegurar la escena el perito informático forense no debe permitir entrar o salir del área hasta que se haya recopilado la evidencia digital. Debe asegurar que los dispositivos digitales no sufran adulteraciones para poder iniciar la trazabilidad de la evidencia.

Paso 2: Identificar los dispositivos. Una vez que la escena está segura, el siguiente paso es identificar los dispositivos digitales que contengan evidencia relevante en teléfonos inteligentes, computadoras portátiles, tablets, cámaras y otros dispositivos digitales; que tengan datos relacionados con el delito que se desee analizar.

Paso 3: Documentar los dispositivos. Una vez identifica los dispositivos digitales; el siguiente paso es documentarlo.

Debe tomar nota detallada de la marca y modelo de cada uno, su condición física y cualquier otra información relevante y útil en la investigación.

Paso 4: Recopilar los dispositivos. Una vez que se han documentados los dispositivos el siguiente paso es recolectarlos, implica que hay que preservarlos; franjarlos, si no son equipos y son archivos los que se encuentren; hay que calcular el hash de cada uno de ellos; luego proceder a retirar con cuidado cada dispositivo de la escena y colocarlo en lugar seguro para ser transportados, asegurando el inicio de la cadena de custodia y el correcto resguardo de los elementos.

Paso 5: Obtención de la Evidencia. Una vez que se ha recolectado los dispositivos, el siguiente paso es la obtención de la evidencia. Implica tener que hacer una copia (forense) de los datos almacenados en ellos y resguardarlos en lugar seguro.

Esto garantizaría que los datos originales no se alteren o dañen debido a lo frágil que es las pruebas digitales; por lo que éste paso es fundamental.

Paso 6: Analizar la Evidencia. Una vez preservada la evidencia, el siguiente paso es analizarla, lo que implica revizar los datos almacenados y buscar información relevante, mediante softwares de IA para analizar gran cantidad de datos en tiempo record.

XI. Panamá y la evidencia digital.

Panamá es miembro del Convenio de Budapest para la Ciberdelincuencia de Budapest desde el año 2014.

Además el artículo 311 del Código Procesal de Panamá " Libro Tercero" relativo al procedimiento de investigación regula las interceptaciones de comunicaciones, se refiere a comunicaciones cibernéticas, seguimientos satelitales, vigilancia electrónica y comunicaciones telefónicas.

Desde entonces Panamá ha considerado los delitos cibernéticos y la creación de unidades especializadas para investigar estos delitos.

La adhesión de Panamá al Convenio de Budapest ha facilitado la cooperación con otros países en la lucha contra la ciberdelincuencia, permitiendo el intercambio de información y asistencia técnica en investigaciones.

Estos cambios reflejan el compromiso de Panamá hacia la adecuación de su derecho interno a fin de dar respuestas a los desafíos que plantea la ciberdelincuencia en un entorno digital en constante evolución.

XII. La Cooperación entre Estados dentro dem Marco del Convenio de Budapest.

El Convenio sobre Ciberdelincuencia (2001) " Convenio de Budapest (STE 185)" constituye el primer y único instrumento internacional que regula las evidencias digitales en materia penal, elaborado por el Consejo Europeo, con participación de Canadá, Estados Unidos de Norteamérica, Japón, entre otros; abierto en Budapest, Hungría en noviembre de 2001.

El Convenio de Budapest tiene el objetivo de armonizar y estandarizar una política criminal entre todos sus Estados miembros; que permita agilizar la persecución, asistencia en la persecución de los delitos cibernéticos trasnfronterizos.

De forma general los artículos del 25 al 28 se establecen lineamientos para la cooperación y asistencia mutua entre Estados para llevar a cabo investigaciones y recolección de evidencias digitales.

El Segundo Protocolo del Convenio de Budapest del Consejo Europeo, se refiere al aumento en la cantidad de delitos en el ciberespacio, debido a equipos digitales más sofisticados y mucho más avanzados que ponen a los usuarios en estado de vulnerabilidad, como por ejemplo el caso de la computación en la nube, lo cual acarrea enormes retos en materia de territorialidad y jurisdicción.

El Convenio de Budapest pretende ajustarse a los más altos estándares de justicia criminal internacional que facilite la investigación y aseguramiento de las evidencias digitales de forma eficaz y eficiente, dentro de parámetros legales internacional que garantice la protección individual y los derechos en el ciberespacio.

Conclusiones

- Concluimos indicando que la inteligencia artificial en la investigación forense digital permitirá automatizar tareas como la extracción, análisis y procesamiento de evidencias digitales a una velocidad y precisión sin precedentes. Esto revolucionará

significativamente los procesos penales al facilitar la identificación de pruebas claves que de manera manual y al ojo humano serían casi indetectables.

- La capacidad de la IA de analizar grandes volúmenes de datos y detectar patrones sutiles la convertirá en herramientas invaluables para los jueces, fiscales y defensores dentro del proceso penal.
- Los algoritmos de IA serán capaces de descubrir relaciones complejas entre metadatos aparentemente conexos, revelando la verdad oculta de los hechos delictivos.
- La IA garantizará la cadena de custodia digital manteniendo cada paso en el manejo de evidencia digital, asegurando la integridad de las mismas en el proceso penal.
- La evidencia digital, al ser menos sujeta a interpretaciones subjetivas, hará que los juicios sean más transparentes y las decisiones judiciales más fundamentadas.

Bibliografía

Rodrigo, F. M. (2021). LA EVIDENCIA DIGITAL EN EL PROCESO PENAL Y LA PRESERVACIÓN DE LOS DERECHOS FUNDAMENTALES. *Revista Acadêmica - Escola Superior do Ministério Público do Ceará* , 13(1), 135–161.

Universidad de los Andes. (2004). Evidencia Digital en el contexto internacional, la necesidad de un Estándar. *https://repositorio.uniandes.edu.co/server/api/core/bitstreams/32db101d-dfc6-4bb8-88c5-fe3d8a38c242/content*.

Romeo, P. R. (s.f.). La inteligencia artificial, una aliada en la investigación informática forense. *https://www.eldial.com/publicador/pdf/DC32A5.pdf*.

Espejo, P. A. (2023). La Incorporación de la Prueba Digital en el Proceso Penal Colombiano. *https://repository.unilibre.edu.co/bitstream/handle/10901/29366/La%20Prueba%20Digital%20en%20el%20Ordenamiento%20Colombiano%20%281%29.pdf?sequence=1&isAllowed=y*.

El Pacto Europa-Latinoamerica. (2022). LA PRUEBA ELECTRÓNICA EN EL MARCO NACIONAL Y EN EL INTERNACIONAL EN LATINOAMÉRICA. *https://elpaccto.eu/wp-content/uploads/2022/08/Publicacion-prueba-electronica-EL-PAcCTO.pdf*.

Abreu Valencia, F. A. (2022). International Cooperation on Cybercrime and Digital Evidence. *http://portal.amelica.org/ameli/journal/501/5013317002/5013317002.pdf*.