ACADEMIC EXTRACT NOTICE

This document is an academic extract prepared exclusively for scholarly citation purposes.

Source document:
Gladys Liliana Gonzáles Obando, “Garantías procesales penales en la evidencia digital,”
Revista de Investigación de la Academia de la Magistratura, Vol. 3, No. 5 (Jul–Dec 2021),
Lima, Peru. ISSN 2707-4056 (online).

This extract (pages 1, 168, 169, and 174 from the original pagination) is included solely as
evidence for academic reference and citation verification.

Cited as: Torres, M. (2020). Informática forense y el camino de la Evidencia digital. Ciencia y Técnica Administrativa.

REVISTA

DE INVESTIGACIÓN DE LA ACADEMIA DE LA MAGISTRATURA

5

Vol. 3 - N.° 5
julio- diciembre 2021
Lima, Perú

FONDO EDITORIAL
Academia de la Magistratura

ISSN: 2707-4056
(en línea)

> Cuando se manejan las evidencias hay que tener en cuenta que muchas de ellas pueden ser virus, o el daño pudo haber sido causado por una falla del hardware o software o una falla eléctrica, además se tiene que tener en cuenta que el intruso pudo haber dejado trampas para eliminar o modificar información al momento de hacer el análisis o utilizar herramientas antiforense para evitar ser encontrado o rastreado. (p. 93)

Según Arellano y Castañeda (2012), «en la recolección física de prueba indiciaria tradicional, se secuestra el indicio y se lo traslada», mientras que «en la recolección de documentación informática esta acción puede realizarse o no, ya que es suficiente con copias bit a bit la prueba y luego trasladar dicha copia» (p. 70).

Así nace un reto para los operadores policiales y fiscales, pues la obtención de la evidencia digital tiene que atender los cánones del estricto respeto de las garantías procesales, de modo que se cumpla con los requisitos de admisibilidad en un proceso penal. A esto se suma, además, que muchos operadores jurídicos se mantienen aún reacios a las innovaciones tecnológicas. En relación a esto, Del Pino (s.f.) estableció que posiblemente se debe a «la Ciberfobia o miedo a la nueva tecnología que experimentan algunos jueces, fiscales e incluso los cuerpos de seguridad del estado» (p. 20).

Asimismo, Peñaloza (2019) destaca que, actualmente, los fiscales deben investigar delitos con pruebas digitales utilizando un código procesal implementado para investigaciones de delitos analógicos. Por lo tanto, es primordial que se adapten los códigos como corresponde.

Por su parte, en el 2012, Cárdenas y Fonseca señalaron que el ciudadano debe mantener una actitud activa, pues:

> «el avance, crecimiento y expansión de las tecnologías de la información y las comunicaciones (TIC), en el nivel científico, académico, empresarial y técnico, implica para la sociedad, para los entes del Estado y para las organizaciones en general, un compromiso grande, un estar alerta, un estar atento frente a los riesgos y amenazas que este desarrollo conlleva» (p. 23).

Entonces, como se mencionó antes, no solo es importante el procedimiento de obtención de la evidencia digital para la eficacia de la prueba, sino que, además, se debe respetar las garantías procesales en la investigación penal. Pero, ¿cuáles son esas garantías? Antes de enumerarlas, se desarrollarán definiciones de evidencia digital.

Para Casey (citado por Cano, 2002), una evidencia digital es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. Por consiguiente, toda información extraída de un medio o dispositivo electrónico y/o informático creado para almacenar datos o

transferirla, cuyo contenido se trate de un hecho o conducta humana que sirva para probar un delito, se denomina evidencia digital; es decir, es el registro de la información guardada o difundida a través de un sistema informático. De manera similar, Torres (2020) señaló que es «cualquier información probatoria almacenada o transmitida en forma digital que una parte de un caso judicial puede usar en el juicio».

Esta evidencia —para su seguridad, preservación y custodia, y con el propósito de que genere un valor probatorio a futuro— debe ser recabada con el procedimiento debido a través de la cadena de custodia. Por ello, Arévalo (2018) afirma que «es de vital importancia mantener un procedimiento para el tratamiento de evidencia digital, el cual debe considerar las mejores prácticas existentes» (p. 42). Acorde con ello, Marqués y Serra (2014) precisaron que:

> Esto significa que, para garantizar la admisibilidad de las pruebas, es necesario prestar especial atención a los métodos y procedimientos utilizados para la obtención de las mismas, respetando no sólo los procedimientos técnicos sino también la legislación judicial y la legislación aplicable al caso. (p. 168)

En el año 2017, se publicó el Manual de Evidencia Digital en el Perú, el cual comprende un tratamiento de este tipo de evidencias, e invita a los operadores jurídicos a ceñirse a su metodología. Además de leerlo, es imprescindible ponerlo en práctica, pues propone un manejo de la evidencia digital basado únicamente en las buenas prácticas:

> El correcto tratamiento de la evidencia digital es fundamental para que sea admisible: haber sido obtenida respetando las garantías y procedimientos legales, basada en una previa autorización judicial o del director de investigación, justificando su tratamiento en los procedimientos de obtención, preservación, análisis y presentación ante el tribunal, respetando la cadena de custodia, cuyos pasos deberá desprenderse de un manual de buenas prácticas. (Martín, 2017, p. 15)

Un proceso penal debe atender las garantías que le otorgan validez, tales como: a) derecho a la tutela jurisdiccional, para acceder a la justicia; b) presunción de inocencia, es una de las garantías que tiene el investigado desde el inicio y como tal se le debe tratar durante todo el proceso penal, hasta que judicialmente sea condenado; c) derecho a la defensa, con el que el investigado puede contradecir los cargos que se le imputan; y d) derecho al debido proceso, se refiere al respeto de todas estas garantías durante la investigación.

Por otro lado, es necesario tener en cuenta que las evidencias digitales que se incorporan a un proceso penal como prueba tienen que ser idóneas, pertinentes, conducentes y útiles; ninguna debe relacionarse a causales de ilicitud. Solo, así, el juez podrá incorporarlas al proceso penal y valorarlas en su sentencia, de modo que su decisión comprenda la superación de toda duda razonable. No obstante, el momento crucial de toda investigación penal

Del Pino, S. (s.f.). *La Informática Forense en el Derecho Procesal Español: Una mirada introductoria a la luz del debido proceso* [trabajo de investigación]. Escuela Judicial, Consejo General del Poder Judicial. https://bit.ly/2USmWro

Gómez, D. (2020). Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano. *Revista Ratio Juris, 15*(30), 220-240. https://bit.ly/2Y8jpGP

Haro, P. (2021). *Técnicas de seguridad en redes de comunicaciones aplicadas a la custodia de evidencia digital* [Tesis de maestría]. Repositorio de la Pontificia Universidad Católica del Ecuador. https://bit.ly/3jnXwLT

Marqués, T., y Serra, J. (2014). Cadena de custodia en el análisis forense. Implementación de un marco de gestión de la evidencia digital. En *RECSI XIII: Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información. Alicante*, 2-5 de septiembre de 2014 (pp. 167-172). Servicio de Publicaciones. https://bit.ly/3mDRCbk

Martín, A. (2017). *Manual de Evidencia Digital*. American Bar Association. https://bit.ly/2XZxq9D

Mesa, A. (2015). La evidencia digital eximente de violación a la protección del dato personal a partir de la autorregulación. *Academia & Derecho*, 6(10), 119-156. https://bit.ly/38mYd1v

Peñaloza, B. (2019). Mendoza: hacia un Código Procesal Penal adecuado para la investigación de ciberdelitos. XIX *Simposio Argentino de Informática y Derecho* (SID 2019)-JAIIO 48 (Salta), 39-42. https://bit.ly/3yrsGpT

Santos, L., y Flórez, A. (2012). Metodología para el análisis forense en Linux. *Revista Colombiana de Tecnologías de Avanzada* (RCTA), 2(20), 90-96. https://bit.ly/3yj91Za

Torres, M. (2020). Informática forense y el camino de la Evidencia digital. *Ciencia y Técnica Administrativa.* https://bit.ly/3mHaBls