ACADEMIA DE
LA MAGISTRATURA

REVISTA DE INVESTIGACIÓN
DE LA ACADEMIA DE LA MAGISTRATURA

Vol. 3, n.° 5, julio-diciembre, 2021
Publicación semestral. Lima, Perú.
ISSN: 2707-4056 (en línea)
DOI: 10.58581/rev.amag.2021.v3n5.09

Garantías procesales penales en la evidencia digital

Criminal procedural guarantees in digital evidence

Gladys Liliana Gonzáles Obando*
Distrito Fiscal de Lima Noroeste
(Lima, Perú)
ggonzalesdn@mpfn.gob.pe
https://orcid.org/0000-0003-1783-539X

Resumen: En este artículo, se presenta el estudio de las garantías procesales penales que deben de respetarse en el procedimiento de obtención de una evidencia digital en un hecho ilícito y su correspondiente incorporación a un proceso penal, de acuerdo con la Constitución política del Estado peruano. En principio, se enumeran brevemente las garantías procesales que deben considerarse en relación a la evidencia digital, a la par que se explica los requisitos exigibles para que dicha evidencia se incorpore a un proceso penal. En este trabajo de investigación, se utilizó el método descriptivo. Se halló que los operadores jurídicos del Ministerio Público se encuentran solicitando apoyo técnico para investigar estos nuevos delitos cibernéticos estando a que no existen fiscalías especializadas a nivel nacional. Ello, para no correr el riesgo de perderse la fuente de información del hecho ilícito

* Fiscal provincial titular penal en el Distrito Fiscal de Lima Noroeste y miembro titular de la Red de fiscales contra la Ciberdelincuencia del Ministerio Público.

cibernético, lo cual generaría impunidad. Por otro lado, se describirá si en el camino de obtener la evidencia digital se vulneran derechos fundamentales, ello impediría la valoración de dicha prueba digital. Por último, también se advirtió que, en el Código Procesal Penal, no existe un tratamiento jurídico especial de la evidencia digital, pues se considera como prueba documental. En consecuencia, habiendo firmado el Perú el Convenio de Budapest, urge crear un procedimiento especial para el tratamiento legal de la prueba digital, que vaya acorde con la evolución de los nuevos delitos cibernéticos.

Palabras clave: globalización, dispositivos electrónicos, cadena de custodia, delitos cibernéticos, operador jurídico, proceso penal

Abstract: In this article, the study of the criminal procedural guarantees that must be respected in the procedure of obtaining digital evidence in an illicit act and its corresponding incorporation into a criminal process is presented, in accordance with the Political Constitution of the Peruvian State. In principle, the procedural guarantees that must be considered in relation to digital evidence are briefly listed, as well as the requirements for such evidence to be incorporated into a criminal process. In this research work, the descriptive method was used. It was found that the legal operators of the Public Ministry are requesting technical support to investigate these new cyber crimes, since there are no specialized prosecutors at the national level. This, in order not to run the risk of losing the source of information about the cyber crime, which would generate impunity. On the other hand, it will be described if, in the way of obtaining digital evidence, fundamental rights are violated, this would prevent the evaluation of said digital evidence. Finally, it was also noted that, in the criminal procedure code, there is no special legal treatment of digital evidence, since it is considered as documentary evidence. Consequently, Peru having signed the Budapest Convention, it is urgent to create a special procedure for the legal treatment of digital evidence, which is consistent with the evolution of new cyber crimes.

Key words: globalization, electronic devices, chain of custody, cyber crimes, legal operator, criminal process

Recibido: 30/11/2021
Revisado: 20/12/2021
Aprobado: 27/12/2021
Financiamiento: Autofinanciado

1. Introducción

La inmersión en la era de la globalización mundial demanda el conocimiento de nuevas conductas ilícitas, como los delitos cibernéticos. Ello da lugar a la implementación de determinados tipos de procedimientos para la

obtención de la evidencia digital, diferente a la clásica evidencia material de un delito común.

En este marco, se cuestiona si se están respetando las garantías procesales en los procedimientos de recolección e incorporación a un proceso penal; de lo contrario, se estarían transgrediendo aquellas garantías consagradas en la carta magna peruana.

Ante ello, resulta importante hacer un recuento de todas aquellas garantías procesales que deben tenerse en cuenta y, por consiguiente, respetarse en la obtención de la evidencia digital.

La aproximación al conocimiento de los procedimientos mencionados y al panorama actual de los delitos cibernéticos en el Perú, permitirá determinar si se respetan las garantías procesales en la obtención de la evidencia digital y su posterior incorporación a un proceso penal, o, por el contrario, se estarían transgrediendo derechos fundamentales de los investigados.

Se finaliza con una reflexión sobre el avance de la lucha contra los delitos cibernéticos en el Perú, ¿o es que se ha dado lugar a la impunidad?

2. La evidencia digital como desafío de la globalización

Los avances científicos y tecnológicos han generado la adopción de nuevas formas de vida que demandan el uso de las tecnologías de información y comunicación (TIC). En este contexto, aparecen también nuevas formas de delinquir, las cuales constituyen un desafío para los operadores jurídicos en la lucha contra quienes, haciendo uso de medios tecnológicos, cometen delitos —en diversas modalidades.

Una investigación penal se inicia de distintas maneras, pero la más determinante se da cuando el operador jurídico se encuentra frente a la evidencia digital. Es «determinante» porque si se realiza inadecuadamente la recolección de dichas evidencias, no se logra el objetivo y se pierden esas evidencias. Al respecto, Mesa (2015) afirma que «estas personas carecen de nombre, rostros, pero se encuentran en relación a sus víctimas a un clic de distancia, operando en línea o por medio de herramientas tecnológicas de operación asincrónica» (p. 122).

De ahí que, en una investigación penal por un delito cibernético, la pesquisa debe saber que no se va a limitar a una evidencia física, sino que, además, tendrá que buscar en la nube y en dispositivos electrónicos. Pues, como indica Haro (2021), «los ciberdelincuentes con la facilidad de la tecnología desarrollan día a día técnicas para realizar los ataques y las herramientas utilizadas por ellos cada vez son más robustas» (p. 56). Adicionalmente, Santos y Flórez (2012) sostienen que:

> 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

es el juicio oral, pues es la oportunidad para presentar todas las evidencias digitales halladas, a las cuales se les podrá otorgar validez —con el respeto a los principios de inmediación, igualdad de condiciones, contradicción y publicidad— y se les incorporará en el proceso para, finalmente, ser valoradas.

Ante ello, los peritos informáticos tienen que mantener la autenticidad e inalterabilidad de las evidencias digitales, sin modificar las imágenes originales, las mismas que deben tener fecha y hora, y codificación. Es conveniente, contar con duplicados digitales originales de las imágenes reproducidas, a fin de preservar la autenticidad como una garantía de certeza respecto a la fidelidad de la evidencia ubicada en el lugar de los hechos. Una vez que se cumpla con el protocolo de obtención, su incorporación y valoración estarán asegurados, ya que se valorará su autenticidad y licitud en el debate del juicio oral.

De manera semejante, la actuación de los medios probatorios en el proceso penal está garantizado por la constitución. Es así que, existen tres estadios en los que se deben atenderse las reglas de exclusión probatoria, ya sea de prueba ilícita, ilegal o prueba irregular. En un primer momento, se puede invocar la nulidad, oposición u otro acto que permita la exclusión de los medios de prueba, se da precisamente en la audiencia de tutela de derechos. La segunda oportunidad es en la audiencia de control de acusación, en la cual se cuestiona la admisibilidad de las pruebas, su pertinencia, idoneidad, conducencia, utilidad y licitud. La tercera y última actuación es la valoración de la prueba ofrecida, pero previamente debe ser admitida e incorporada al juicio oral en la etapa de juzgamiento; lo esencial en esta oportunidad es la actuación probatoria, a través de un debate del principio contradictorio y oralización de los informes periciales. Al respecto, Gómez (2020) precisó que:

> Desde la óptica constitucional, el funcionario judicial debe realizar un análisis de cada prueba digital, para descartar que en su obtención se vulneraron derechos fundamentales, toda vez que en caso de que así ocurra, debe aplicar la cláusula de exclusión y evitar así la vulneración del principio del debido proceso. (p. 235)

Es importante subrayar que, la evidencia digital solo será admitida en el proceso judicial si cumple con tres requisitos indispensables: a) licitud, es decir, bajo el marco del respeto a los límites de los principios constitucionales y derechos fundamentales —derecho al secreto de las comunicaciones, a la intimidad personal, a la inviolabilidad de domicilio, a los secretos financieros, entre otros—; b) integridad, teniendo en cuenta que las evidencias digitales suelen ser volátiles y, por tanto, se tiene que garantizar su inmutabilidad del soporte digital; y c) autenticidad, se refiere a que sea la muestra original con la garantía de la preservación de su cadena de custodia.

Por otro lado, se ha advertido que, en el Código Procesal Penal, no existe un tratamiento jurídico especial de la evidencia digital, pues se considera como prueba documental. Ello, pese a que, en la actualidad, existen diversos tipos de evidencia digital que, en algunos casos, tienen una marcada diferencia con la clásica evidencia documental. Es por esto que se necesitaría crear un procedimiento especial para el tratamiento legal de la prueba digital.

Finalmente, otro aspecto destacable es la firma del Convenio sobre la Ciberdelincuencia en el Perú, denominado también de Budapest, el mismo que entró en vigencia el 1 de diciembre de 2019. El compromiso asumido comprende la aplicación de una política unificada entre todos los operadores jurídicos frente a la ciberdelincuencia. Ello, mediante el cambio de una legislación que responda al tratamiento procedimental de la evidencia digital. Si bien desde el año 2013 existe la Ley n.° 30096 —modificada por la Ley n.° 30170—, lo que necesitamos no es solo la tipificación de estos nuevos delitos, sino que es determinante el establecimiento del procedimiento penal para hechos ilícitos que solo cuentan con evidencia digital. Indudablemente, poco a poco se están implementando los nuevos métodos que utilizarán los operadores jurídicos para estos casos. En consecuencia, es vital también que se les capacite oportunamente para afrontar a estos nuevos delitos.

3. Materiales y métodos

Para el presente estudio, se utilizó la diversa documentación doctrinaria y legal en torno a los nuevos delitos cibernéticos, así como la casuística generada en el presente año de los delitos cibernéticos que se han denunciado ante el Ministerio Público (MP) a nivel nacional y que se encuentra en la estadística de dicha institución. También se realizaron entrevistas a representantes de la Fiscalía y se obtuvo una estadística general de la plataforma de ciberdelincuencia que tiene alcance a nivel nacional. Es importante precisar, que tras la creación de la Unidad Fiscal Especializada en Ciberdelincuencia del MP, se implementó dicha plataforma, a fin de que los fiscales soliciten acompañamiento técnico en la realización de las investigaciones de los ilícitos de la ley de delitos informáticos.

4. Resultados

En este estudio, se halló que la doctrina establece de manera uniforme que la evidencia digital solo se podrá incorporar al proceso penal si cumple con ser idónea, pertinente y útil; así como lícita, es decir, con respeto a los derechos fundamentales, hecho que en forma unánime fue señalada por los representantes del Ministerio Público que fueron entrevistados. Asimismo, se halló que los operadores jurídicos recientemente se encuentran capacitándose para afrontar las nuevas y diversas modalidades de delitos cibernéticos, cuya

clave es la búsqueda y protección de la evidencia digital. Esto se encuentra reflejado en la cantidad considerable de solicitudes de acompañamiento técnico presentadas a la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público a nivel nacional, las que son menores en comparación a los ingresos de denuncias por delitos cibernéticos, pese a que como se ha hallado, no existe un tratamiento diferenciado de la evidencia digital en el Código Procesal Penal, respecto de la prueba documental.

5. Discusión

Cuando en la obtención de la evidencia digital se vulnera derechos fundamentales —tales como del secreto de las comunicaciones, de la violación de domicilio, de la violación a la intimidad personal y familiar, y de la reserva financiera— o se incurre en irregularidades procesales, se obstaculiza la valoración de dicha prueba digital, es por ello que todo proceso penal se caracteriza por su legalidad. Sin embargo, vemos que el tratamiento e incorporación de la evidencia digital no se encuentra prevista en la norma jurídica —para el caso, el Código Procesal Penal—; y, por tanto, tiene el mismo tratamiento que la prueba documental. Entonces, es de suma importancia un cambio que promueva la atención adecuada de los nuevos delitos cibernéticos en dicha norma adjetiva.

Sabido es que no toda evidencia digital resulta ser idónea, pertinente y útil, ante ello, nuevamente se destaca la necesidad de una formación de los operadores jurídicos, con el objetivo de que puedan discriminar las evidencias digitales que podrían presentarse ante un juez para su respectiva valoración. Pero, sobre todo, para que conozcan el procedimiento de la cadena de custodia de la evidencia digital, y se cautele su autenticidad y garantice su contenido.

Todo esto asegurará que no queden impunes las nuevas modalidades de delitos cibernéticos, debiéndose iniciar una urgente y continua capacitación de todos los operadores jurídicos de la mano con el personal policial y peritos informáticos de las diversas instituciones. Así estarán preparados para respetar las garantías procesales en el proceso de obtención de la evidencia digital, evitando que se pierdan, y dando lugar a una incorporación válida en un proceso penal.

Finalmente, se advierte que existe un gran avance en la lucha contra los delitos cibernéticos en el Perú con la firma del Convenio de Budapest, el cual dio lugar a la creación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, que indudablemente reducirá la impunidad frente a la creciente variedad de formas de estos delitos cibernéticos, debido a que poco a poco todos los operadores jurídicos serán plenamente capacitados tanto jurídica como técnicamente.

6. Conclusiones

a) La obtención de la evidencia digital que no respeta las garantías constitucionales —tales como violación del secreto de las comunicaciones, violación de domicilio, violación a la intimidad personal y familiar, así como de la reserva financiera—, o que incurre en irregularidades procesales, impide la posterior valoración de dicha prueba.

b) A partir del estudio, se afirma que, actualmente, los operadores jurídicos no se encuentran capacitados para la obtención válida de una evidencia digital y, por tanto, tampoco se garantiza su incorporación al proceso penal. Esta problemática da lugar a la impunidad de diversos delitos cibernéticos.

c) En el Código Procesal Penal, no existe un tratamiento jurídico especial sobre la evidencia digital, pues se le considera como prueba documental. En consecuencia, se debe crear un procedimiento especial para el tratamiento legal de la prueba digital, que responda a la evolución de los nuevos delitos cibernéticos.

d) A la fecha, con la creación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, se ha dado un gran paso en la lucha contra los delitos cibernéticos, con lo que se espera reducir la impunidad.

Referencias

Arellano, L., y Castañeda, C. (2012). La cadena de custodia informático-forense. *Revista Activa,* 3(1), 67-81. https://bit.ly/3ztmqiH

Arévalo, P. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. *Revista Economía y Política*, (28), 35-46. https://bit.ly/3BhqMKk

Cano, J. (2002). *Evidencia digital: Reflexiones técnicas, administrativas y legales* [Diapositiva de PowerPoint]. Universidad de los Andes. https://bit.ly/2WB3znz

Cárdenas, B., y Fonseca, H. (2012). Rol del derecho penal y la informática forense en la protección de la información en la era digital. *Revista Academia y Virtualidad,* 5(1), 21-29. https://bit.ly/2XVv4IO

Convenio sobre la Ciberdelincuencia. (23 de noviembre de 2001). Serie de Tratados Europeos - n.° 185. https://bit.ly/2WxHeak

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