REVISTA CIENTÍFICA INTERDISCIPLINARIA
Adventus
ilamecpos.com
ISSN - 3008-9174

CADENA DE CUSTODIA DE LA EVIDENCIA DIGITAL

Por ***Marcelo Antonio Torok***[1]

I. INTRODUCCION

La evidencia digital, emerge en el mundo del análisis forense en los últimos años, desde que la tecnología informática pasó a ser parte de nuestra vida diaria, a fin de comprender los hechos acontecidos, sus autores, las motivaciones que les llevaron a actuar de determinada forma y las consecuencias para las víctimas y el resto de la sociedad, se requiere recomponer las circunstancias y acciones, tal como si fueran un rompecabezas multidisciplinario, con diversas dimensiones y sucesiones temporales, por lo que se debe generar esa imagen vívida de los hechos mediante el estudio de los testimonios y la evidencia probatoria obrante.

La Justicia en su estado más puro, busca encontrar la luz de la verdad a través de los indicios que se le presentan al magistrado. Como todo ser humano, el juez se encuentra limitado en sus condiciones para cumplir con tamaña obligación por diversos factores, entre los que destacaremos el comprensible desconocimiento de la mayoría las ciencias y artes, como asimismo del real acontecer de los hechos, sobre los que pretende impartir justicia.

Entre otras aptitudes, el magistrado cuenta con una que le distingue en el ejercicio de su labor: "*La Sana Crítica*", esa libertad discrecional, que el juez ejerce, a la hora de dar contenido a su decisión para la resolución de casos, sin vulnerar el espíritu del Derecho.

Por tanto, cuando afirmamos que tal discrecionalidad existe en algún grado, queremos decir que el propio Derecho le deja al juez márgenes, para que pueda elegir entre distintas opciones o entre diferentes alcances de una misma solución del Caso, ya que el magistrado no tiene conclusiones predeterminadas por el sistema jurídico, sino que, en mayor o menor medida, cuenta con espacios para escoger entre alternativas diversas, pero compatibles todas ellas con la ley.

Pero decíamos que el juez tiene limitaciones en el conocimiento de las diversas

Ingeniero en Informática – UCEMA. Magister en Ciencias Criminológico Forenses. Docente del Instituto Universitario de la Policía Federal Argentina (IUPFA)

ciencias y que, para solucionar esta eventualidad, el magistrado, cuenta con los peritos, los cuales, gracias a sus conocimientos, actúan como fuente de consulta para la resolución de controversias. De esta forma el Juez dispone del necesario asesoramiento y respaldo de idoneidad en cada disciplina.

Para llegar al conocimiento de los hechos, sus motivos y alcances, se requiere recomponer las circunstancias, motivaciones y las consecuencias, tal como si fuera un rompecabezas multidisciplinario, con diversas dimensiones y sucesiones temporales, por lo que se debe generar esa imagen vívida de los hechos mediante el estudio de los testimonios y la evidencia probatoria obrante.

El debido respeto a la *Cadena de Custodia de la Evidencia Digital* - CCED antes referido, implica el cumplimiento cuidadoso de todos los pasos necesarios, desde la detección de los posibles recursos probatorios, hasta su disposición para el análisis forense, garantizando que las huellas probatorias recolectadas, son realmente las mismas que se procesan y de las que surgen las conclusiones presentadas ante el tribunal. Todo ello sin viciar el manejo que se haga de los elementos preservados, a fin de evitar la alteración, sustitución, contaminación o destrucción de los mismos, lo que desembocaría en inevitables nulidades, de las cuales no se podría volver atrás.

El cuadro de situación actual, fruto de la evolución de la informática, se vio potenciado por las circunstancias de aislamiento que hemos atravesado durante la pasada pandemia, que impulsó una inusitada dependencia generalizada, de la tecnología que empleamos día a día, no solo en las organizaciones, sino también todos los individuos, sin importar su edad, actividad o condición social.

Nuestra vida, nuestro trabajo, nuestros proyectos y nuestros afectos pasan en un alto grado, por los dispositivos digitales (particularmente computadoras y teléfonos celulares), que empleamos día a día.

Como afirma un antiguo adagio: “*Por donde pasa la Vida, pasa el Derecho*”, por consiguiente, la necesidad de Justicia, por lo que se requiere una clara comprensión de donde buscar la prueba digital y como conservarla adecuadamente, dado que la dinámica que impone la actividad digital a nuestra vida diaria, nos obliga, a quienes formamos parte del mundo del derecho y la investigación forense, a poner el foco en comprender la importancia de la debida valoración y tratamiento de los indicios digitales, reflexionando respecto a la CCED, aplicando los distintos pasos que la componen y procurar promover un *modus operandi* que conduzca a los peritos informáticos a cumplir sus labores forenses de acuerdo con “*Buenas Prácticas*” debidamente corroboradas, a

fin de garantizar la calidad de la prueba.

Cumpliendo con todo lo expresado, aplicando el "*Método Científico*", que implica la investigación ajustada a procesos claros y repetibles, con métricas ciertas, que normalicen la presentación de sus observaciones, clarificando las conclusiones logradas durante las diligencias periciales, de manera estructurada y bien fundada, que conduzcan al esclarecimiento de la verdad objetiva.

II. METODOLOGÍA

La "*Escena del Hecho*" es única e irrepetible, es un espacio rico, que nos cuenta de eventos y manifestaciones. Rastros diversos, (entre ellos digitales), respecto a lo realmente sucedido y huellas, algunas reales, otras deterioradas y hasta algunas fraguadas, que pueden eventualmente incluir, lo que pretende comunicar o hacer creer al público y las autoridades, el autor del acto criminal. Resguardar cuidadosamente la CCED, es la garantía del manejo idóneo de la prueba desde el punto de vista profesional tecnológico.

Mediante la tipificación clara y a tiempo de la evidencia, se pueden aplicar conjuntos de buenas prácticas, específicas para cada tipo de elemento probatorio. Es decir que, utilizando técnicas adecuadas, se resguarda la integridad probatoria de cada elemento, de acuerdo a las particularidades que encierran los diversos tipos de tecnología encontrada.

Debe tenerse en cuenta, que la labor forense, inicia con el funcionario que colecta la evidencia, aunque sea en forma accidental o desconociendo la gravedad del hecho (*Primer Interventor*), pasa por el *Personal Logístico* que la cataloga, asegura, traslada y almacena, continúa con la participación de los *Peritos Informáticos Forenses*, que la procesan rescatando múltiples indicios probatorios y concluye con los *Analistas Digitales*, que correlacionando datos y eventos, aportan al juez de la causa sus observaciones precisas que le permitan aplicar al magistrado la sana crítica, a fin de interpretar debidamente la prueba y resolver en base a ella.

La CdC, no implica solamente establecer adecuados protocolos de actuación, respecto a cómo actuar frente a la evidencia, contempla la capacitación y el adiestramiento de todo agente interviniente, que colecte, reciba o analice evidencias y/o rastros digitales en cualquier etapa del proceso, e incluye la disposición justo a tiempo, de las herramientas informáticas forenses específicas necesarias para llevar adelante la tarea encomendada, los recursos necesarios para el resguardo de la información

obtenida y los lugares físicos seguros de almacenamiento (*depósitos o almacenes*), aprobados y controlados por la Justicia, como componentes ineludibles del proceso de preservación de la evidencia.

Se deben contemplar técnicas de trazabilidad para garantizar el seguimiento de la evidencia a resguardar, en función de la línea de tiempo del devenir de los hechos, contenedores de la evidencia (tanto físicos como lógicos) y recursos validadores de integridad tales como "*Cálculos de Hash*"- CdH, y el empleo de Blockchain, para garantizar la autenticidad y adecuado manejo técnico, en el tratamiento de la evidencia.

La CdC no puede aplicarse de manera arbitraria, a una parte de los indicios recopilados, debe incorporarse de manera uniforme al conjunto de toda la evidencia recopilada. El tratamiento de los efectos probatorios, debe realizarse de idéntica forma y con iguales herramientas, métodos y parámetros de evaluación para la totalidad de la evidencia obrante. A fin de evitar distorsiones y errores de medición, deben separarse en forma estricta, los efectos probatorios certificados (debidamente adquiridos), de los no certificados (de dudosa procedencia).

Tan importante como el análisis y conservación segura y trazable de la evidencia, es hacer lo propio con los reportes, informes y dictámenes, resulta sumamente aconsejable emplear recursos tales como bloqueo de archivos contra escritura, firma digital, hashes y reservorios seguros de la documentación, que permitan que todos los involucrados, (y solo los involucrados) puedan acceder a la documental que da sustento a las tareas forenses.

La CCED, requiere aplicar una serie de buenas prácticas para lograr los objetivos planteados. Podemos definir una serie de pasos y labores, a contemplar en un Protocolo especialmente pensado a tal fin, para la implementación eficiente de la CdC, los cuales no necesariamente deben cumplirse en la misma secuencia presentada, tal como queda planteado a continuación. Incluso en la práctica podrá observarse que, hay ciclos de tareas, que se reiteran en función de las demandas de las diversas diligencias procesales. Podemos plantear los pasos a seguir, de la siguiente forma:

<u>Primera Intervención</u>

- Toma de Contacto con la Escena del Hecho
- Establecimiento y control del perímetro de seguridad
- Inspección de la escena y composición de lugar
- Registro visual
- Elaboración de un croquis del espacio físico

ISSN - 3008-9174

Labor Forense en el Terreno

- Detección y registro escrito, fílmico y fotográfico, de eventuales indicios probatorios, tanto físicos, como lógicos y etéreos (inalámbricos).
- Evaluación e inventario de la evidencia digital obrante
- Determinación de evidencia activa, pasiva y desactivada
- Recopilación registrada
- Determinación y desarrollo de los procedimientos de preservación de los indicios obrantes, consignado:
  - Aquellos que serán analizados *In Situ*
  - Los que serán trasladados al *Laboratorio Forense*, para su procesamiento
  - Aquellos que, al menos en la instancia presente y bajo las actuales circunstancias, no serán considerados para su preservación y análisis
- Resguardo, embalaje y fajado seguro de los elementos a remitir al Almacén Judicial o protegidos para su análisis en el terreno, todo de acuerdo con las eventuales necesidades forenses futuras.
- Traslado al Depósito de los elementos previamente seleccionados, incluyendo el *Formulario de Cadena de Custodia* y una *Nota de Traslado*.

Actividades de Laboratorio

- Organización de las actividades a desarrollar
- Establecimiento de una agenda de trabajo, convocando a los peritos designados por las *Partes* y comunicando todo al *Responsable de la Instrucción* (Tribunal o Fiscalía)
- Concreción de las diligencias periciales
- En caso de ser requerido un eventual encendido y conexión de los dispositivos bajo prueba, se hará de manera protegida, respecto a escritura y radiaciones
- De corresponder, la realización de copias forenses de las unidades de almacenamiento, se efectuará en un formato bit a bit
- Extracción de indicios, (incluyendo información borrada), de acuerdo con las instrucciones recibidas del magistrado o fiscal, (quien lleve adelante la instrucción)

Análisis Forense

- Tratamiento a brindar a la evidencia recopilada

- Búsqueda de coincidencia de palabras claves
- Entrecruzamiento de datos procedentes de diversas fuentes
- Incorporación de los indicios recopilados, en el cuadro de la línea de tiempo de la investigación

- Elevación de reportes, informes y dictámenes, tal lo requerido

Cierre de las Diligencias

- Se regresan los recursos ya procesados al depósito judicial y allí se conservan mientras duran las impugnaciones y pedidos de aclaraciones
- Finalmente, según disponga el magistrado, los dispositivos preservados, pueden:
  - Volver a sus legítimos propietarios
  - Borrado seguro de la información obrante para donar luego el dispositivo
  - Destrucción (para el caso que el dispositivo no admita la eliminación de la información ilícita contenida en el mismo)
- Borrado seguro de las copias de trabajo y de las extracciones obrantes en los *Servidores* del laboratorio forense

La presente enumeración de pasos, incluyendo un esquema en cascada, busca plantear los puntos a desarrollar en un Protocolo de Actuación. El desarrollo de cada uno de los pasos, depende de los requisitos que disponga el Código Procesal de Rito y toda otra normativa particular de aplicación.

Las disposiciones públicas no deberían ser un limitante, para el desarrollo de un sistema eficiente de garantía para CCED, tampoco debería serlo el "*costumbrismo*" (*aquí lo hacemos así*), ni tampoco la urgencia en obtener resultados, debería ser un motivo para saltear pasos que garantizan el aseguramiento de la prueba.

III. RESULTADOS

Regular los procedimientos generales y específicos de la cadena de custodia de la evidencia digital, a los fines de que sea demostrada la validez de la evidencia, desde la etapa de su detección y recopilación en la escena del hecho, hasta la culminación del proceso de análisis y elevación de informes y aclaraciones al magistrado, teniendo como destinatarios del presente trabajo, la Justicia en sus distintos estamentos, los Consejos / Colegios Profesionales de la especialidad, las Universidades e Instituciones de

Formación Profesional destinadas a integrantes de las Fuerzas Armadas y/o de Seguridad y el personal de los laboratorios informático forenses y peritos independientes, que practican el resguardo, fijación, colección, embalaje, rotulado, etiquetaje, traslado, preservación, análisis, almacenaje y custodia de las evidencias digitales, con la finalidad de mantener un criterio unificado de patrones forenses.

La CdC, es la garantía de Integridad en el proceso forense. No se trata simplemente de resguardar, sino de hacerlo de tal forma, que los indicios probatorios recopilados mantengan su esencia característica que, para el caso de la evidencia digital, se encuentra obrante en los parámetros definidos como “metadatos”. Estos valores son fundamentales, a la hora de ponderar jurídicamente un indicio, debido a que, una vez probada su validez e integridad, (y contando con la garantía de continuidad de haberse acatado el procedimiento de la Cadena de Custodia), podrán los investigadores abocarse a su interpretación y correlación probatoria, enfocándose en sus correctas interpretaciones, despejada toda duda de la validez de la evidencia obrante.

IV.CONCLUSIONES

La toma de conciencia, respecto a la correcta aplicación de la CCED y su continuo perfeccionamiento, constituye una importante necesidad de nuestro sistema judicial, con el objetivo de una adecuado resguardo y continuidad, en estado de integridad, confidencialidad y continuidad en la disponibilidad, de los indicios probatorios recopilados, a los fines de favorecer la búsqueda de la verdad.

La prueba digital, no por efímera es menos valiosa que otras, por el contrario, es una de las más ricas y bien cuidada, nos puede brindar muchas certezas, la CCED procura mantenerla en condiciones de ser analizada, con criterios científicos de certeza y repetitividad, libre de contaminación, disponible donde y cuando sea requerida, en forma precisa, clara y contundente y cuantas veces sea necesario repetir los procesos.

Recolectar evidencia no es simplemente un acto de acumulación, al preservar indicios probatorios, lo importante es rescatar su significado, comprender el valor que van a tener en el proceso de investigación y cuidar su integridad, respecto a toda forma de contaminación, robo o sabotaje. Obtener mediante el método científico y la aplicación de buenas prácticas forenses, conclusiones que aporten luz en una causa judicial, nos alejara de la frustración de la nulidad del proceso, que implica una negación

de la Justicia y el triunfo de las trasgresiones del mundo delincuencial.

La Escena del Hecho, es como un libro que se abre ante los ojos del experto, que para ser abordada requiere de una pausa inicial, una solemnidad ritual que relaciona al evento investigado con el inquisidor que está procurando leer el mensaje disponible en cada uno de los indicios que nos deja traslucir y eventualmente preservar. La Cadena de Custodia, es la garantía que la historia recopilada se corresponde con la verdad.

V. REFERENCIAS BIBLIOGRÁFICAS

Argentina. Ley 26388 – 2008 – Contra el delito informático

_____*Ley 25506 – 2001 – Firma Digital*

IRAM-ISO-IEC 27042 – Guías para el análisis y la interpretación de la evidencia digital

IRAM-ISO-IEC 27037 – Guías para la identificación, la recolección, la adquisición y la preservación de la evidencia digital

IRAM 36100 – Aplicación de la cadena de custodia. Vocabulario y requisitos

Convenio sobre Ciberdelincuencia – *Budapest y Protocolos Adicionales*