LA INFORMÁTICA FORENSE EN EL DERECHO PROCESAL ESPAÑOL

Una mirada introductoria a la luz del debido proceso

Descripción breve

La finalidad del presente documento es brindar una mirada introductoria a la informática forense a través de la investigación penal de los delitos informáticos y cibercrimenes con el propósito de sentar las bases de la investigación científica en esta materia, dándole pautas a los futuros investigadores de cómo manejar una escena del delito en donde se vean involucrados sistemas de información o redes y la posterior recuperación de la llamada evidencia digital, en el marco del debido proceso.

Santiago Acurio Del Pino, Juez Provincial, Sala Única Penal

sacurio@hotmail.com

La informática forense en ámbito del derecho procesal español.

TRABAJO DE INVESTIGACIÓN
6ª PROMOCIÓN DEL CURSO DE FORMACIÓN JUDICIAL ESPECIALIZADA PARA INTEGRANTES DE PODERES JUDICIALES DE IBEROAMÉRICA Y OTROS OPERADORES JURÍDICOS IBEROAMERICANOS

Contenido

1.- Introducción

Francisco Martínez Vásquez en el prólogo del libro de Investigación Criminal[1], señala que la investigación criminal debe ser entendida como un proceso de descubrimiento, recolección e identificación de evidencias para esclarecer el hecho delictivo, señala también que este tema ha obsesionado a muchas personas, no solamente al público experto, sino también a incontables personas ávidas de novelas detectivescas, novelas negras, series y películas de la temática, donde se muestran investigadores que en pocas horas usando técnicas novedosas, encuentran a los responsables de los delitos. A pesar de ello la investigación criminal menciona Francisco Martínez, demanda un trabajo arduo, lento, profesional y científico alejado de la simplicidad mostrada en la ficción. Por tanto, la dedicación que demanda la investigación criminal debe verse como un proceso de reconstrucción deductivo que debe arrojar luz sobre el hecho delictivo a través de evidencias que se constituyan en pruebas admisibles y rigurosas de la culpabilidad de una persona más allá de toda duda razonable. De no ser así ese error afectaría gravemente al debido proceso[2] como garantía de todos los ciudadanos.

Pero que es la investigación criminal o de delitos, de acuerdo a un documento generado por la Oficina de las Naciones Unidas contra la Droga y el Delito, *la investigación de delitos es el proceso por el cual se descubre al autor de un delito, cometido o planeado, mediante la reunión de hechos (o pruebas), si bien también puede suponer la determinación, ante todo, de si se ha cometido o no un delito. La investigación puede ser reactiva, es decir, aplicada a delitos que ya se han perpetrado, o proactiva, es decir, encaminada a evitar cierta actividad delictiva planeada para el futuro*[3].

De acuerdo al documento antes citado, *hay dos enfoques básicos de la gestión de la investigación de delitos. En algunos sistemas, caracterizados por jurisdicciones con tradición de derecho romano, el encargado de la investigación es un fiscal o un funcionario judicial, por ejemplo, un juez de instrucción. En estos casos, los investigadores trabajan bajo la dirección del fiscal o del juez de instrucción y, en realidad, puede incluso existir un organismo especial encargado del cumplimiento de la ley denominado "policía judicial". En el segundo en foque, que suele encontrarse en jurisdicciones de tradición de COMMON LAW, las investigaciones las lleva a cabo la policía de manera más o menos independiente de los fiscales hasta que el caso, y el sospechoso acusado, pasan a manos de la fiscalía ante los tribunales. Sin embargo, dentro de*

---

[1] GIMÉNEZ-SALINAS, Andrea y GONZÁLEZ, José Luis, Investigación Criminal, Primera Edición, Madrid, España, 2015, Editorial LID.

[2] El "DEBIDO PROCESO" es un derecho reconocido y garantizado por el Estado, el cual dicta las normas fundamentales básicas que deben cumplirse en la formación del proceso, el cual, perfeccionado cumpliendo con dichas garantías, adquiere el rango jurídico de "proceso debido". El debido proceso es una acabada y perfeccionada institución jurídica estructurada debidamente bajo el amparo de las normas garantizadoras de la Constitución. Tomado de Derecho Penal Informático, Acurio Del Pino Santiago, 2015, Corporación de Estudios y Publicaciones, Quito, Ecuador

[3] UNDOC, Oficina de las Naciones Unidas contra la droga y el delito, MANUAL DE INSTRUCCIONES PARA LA EVALUACIÓN DE LA JUSTICIA PENAL, Investigación de Delitos. Nueva York, 2010.

estos dos sistemas básicos hay muchas variaciones. Por ejemplo, en muchas jurisdicciones de COMMON LAW, los fiscales colaboran estrechamente con los investigadores policiales, por lo menos con respecto a ciertos tipos de delitos. Pero independientemente del sistema, los principios fundamentales siguen siendo los mismos: ***establecer quién cometió el acto ilícito y reunir suficientes pruebas para asegurar su condena***[4].

Increíblemente los delincuentes hoy están utilizando la tecnología para facilitar el cometimiento de infracciones y eludir a las autoridades. Este hecho ha creado la necesidad de que tanto la Policía Judicial, la Fiscalía y la Poder Judicial deba especializarse y capacitarse en estas nuevas áreas en donde las TICS[5] se convierten en herramientas necesarias en auxilio de la Justicia y la persecución de delito y el delincuente.

Los hábitos de las personas han cambiado con el uso de las TICS, también las formas en que los delincuentes actúan y comenten sus actos reprochables, es así que el acceso universal a las tecnologías de la información y la comunicación brinda nuevas oportunidades para que gente inescrupulosa, delincuentes, pornógrafos infantiles, artistas del engaño, quienes realizan toda clase de ataques contra la intimidad, fraudes informáticos, contra el tráfico jurídico probatorio, que atacan a la integridad de los sistemas computacionales y de red a nivel mundial, actúen de forma desmedida sin que los operadores de justicia puedan hacer algo, ya que estos han quedado relegados en sus actuaciones por la falta de recursos tecnológicos y capacitación a fin de lidiar con la evidencia digital presente en toda clase de infracciones y especialmente en los llamados Delitos Informáticos y Cibercrimenes

La comisión de infracciones informáticas es una de las causas de preocupación de los elementos de seguridad de muchos países en este momento dado que las mismas han causado ingentes pérdidas económicas especialmente en el sector comercial y bancario donde por ejemplo las manipulaciones informáticas fraudulentas ganan más terreno cada vez más, se estima que la pérdida ocasionada por este tipo de conductas delincuenciales supera fácilmente los doscientos millones de dólares, a lo que se suma la pérdida de credibilidad y debilitamiento institucional que sufren las entidades afectadas. Es por eso que en países como Estados Unidos, Alemania o Inglaterra se han creado y desarrollado técnicas y herramientas informáticas a fin de lograr tanto el descubrimiento de los autores de dichas infracciones, así como aseguran la prueba de estas.

La informática forense, es la ciencia criminalística que sumada al impulso y utilización masiva de las tecnologías de la información y de la comunicación en todos los ámbitos del quehacer del hombre, está adquiriendo una gran importancia, debido a la globalización de la Sociedad de la Información[6]. Pero a pesar de esto esta ciencia no tiene un método

---

[4] UNDOC, ver cita anterior.

[5] Tecnologías de la Información y la Comunicación

[6] Es una sociedad en la que la creación, distribución y manipulación de la información forman

estandarizado, razón por la cual su admisibilidad dentro de un proceso judicial podría ser cuestionada, pero esto no debe ser un obstáculo para dejar de lado esta importante clase de herramienta, la cual debe ser manejada en base a rígidos principios científicos, normas legales y de procedimiento.

De lo expuesto se colige que es necesario contar dentro de los operadores de justicia con el personal capacitado en estas áreas para lidiar con esta clase de problemas surgidos de la mal utilización de la informática y sus ramas afines.

La finalidad del presente documento es brindar una mirada introductoria a la informática forense a través de la investigación penal de los delitos informáticos y cibercrimenes con el propósito de sentar las bases de la investigación científica en esta materia, dándole pautas a los futuros investigadores de cómo manejar una escena del delito en donde se vean involucrados sistemas de información o redes y la posterior recuperación de la llamada evidencia digital, en el marco del debido proceso.

2.- Debido proceso

De conformidad al Art. 1 de la Constitución, España se constituye en un Estado social y democrático de Derecho, este enunciado nos dice que el sistema penal y procesal penal corresponde un sistema de mínima intervención, atendiendo al carácter subsidiario y fragmentario del derecho penal, que ya no mira al individuo como un objeto de persecución penal, devolviéndole a este su dignidad. En ese sentido ese individuo en goce de sus derechos humanos, es a quien, a través de la investigación penal objetiva, se le demostrará siguiendo un debido proceso, su responsabilidad frente a sus actos[7].

De acuerdo a Adolfo Somarrivas el debido proceso es una figura que proviene originalmente del derecho anglosajón, el cual con el transcurso del tiempo la ha venido desarrollando como determinando su contenido y delimitando sus elementos,[8] en fin a lo que podríamos considerar como la obligación de los operadores de justicia de respetar el "DUE PROCESS OF LAW". Cuyo contenido de acuerdo a Martín Agudelo Ramírez, es la suma de "*principios y garantías que son indispensables de observar en diversos procedimientos para que se obtenga una solución sustancialmente justa, requerida siempre dentro del marco del estado social, democrático y de*

---

parte importante de las actividades culturales y económicas, es decir es un estadio del desarrollo social caracterizado por la capacidad de los ciudadanos, el sector público y el empresarial para compartir, generar, adquirir y procesar cualquier clase de información por medio de las tecnologías de la información y la comunicación, a fin de incrementar la productividad y competitividad de sus miembros, y así reducir las diferencias sociales existentes contribuyendo a un mayor bienestar colectivo e individual. ACURIO DEL PINO, Santiago. Derecho Penal Informático, Segunda Edición 2017. https://www.academia.edu/33039698/Derecho_Penal_Inform%C3%A1tico_Segunda_Edici%C3%B3n_2017

[7] ACURIO DEL PINO, Santiago. Derecho Penal Informático, Segunda Edición 2017. https://www.academia.edu/33039698/Derecho_Penal_Inform%C3%A1tico_Segunda_Edici%C3%B3n_2017

Principios de Debido Proceso, Centro de información Jurídica en línea, https://cijulenlinea.ucr.ac.cr/portal/descargar.php?q=MzAx

derecho"[9].

En la Constitución española[10] encontramos el Art. 24.1 y 2 que señala:

1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión.
2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia.

Estos enunciados constitucionales son los que garantizan el derecho al debido proceso en España.

Ahora bien, parte del debido proceso es el derecho a la defensa, para lo cual el Art. 24.2 de la Constitución de España señala que las personas tienen el derecho a utilizar los medios de prueba relevantes para el ejercicio de su defensa. De lo dicho podemos afirmar que la Constitución española consagra la llamada libertad probatoria, considerada como el esfuerzo de todos los sujetos procesales tendiente a la producción, recepción y valoración de los elementos de prueba,[11] pero no cualquier medio de prueba sino solamente los pertinentes para su defensa.

La fase probatoria normalmente es la más relevante del proceso tanto civil como penal, es cuando los sujetos procesales tratan de demostrar al órgano judicial los argumentos favor de su pretensión. David Ortega Gutiérrez, señala que: "*el Juez o Tribunal tiene que velar por el buen desarrollo de esta fase de forma que las pruebas sean, como no puede ser de otra manera, obtenidas legalmente, deben ser pertinentes, esto es, relacionadas con el litigio, por un lado, y útiles al mismo, por otro. Por tanto, tienen que estar destinadas a esclarecer los hechos objeto del litigio. Nuevamente, el incumplimiento o vulneración de este derecho provocaría la indefensión de la parte afectada. Es por tanto preciso fundamentar la inadmisión de medios probatorios que puedan incidir en la sentencia*[12]."

Es así que la obtención y presentación de las pruebas dentro del proceso judicial debe estar guiado por reglas inspiradas en los principios de legalidad, de seguridad jurídica, derecho a la defensa y tutela judicial

---

[9] AGUDELO RAMÍREZ, Martín. El Debido Proceso, OPINIÓN JURÍDICA vol. 4, No. 7 pp. 89-105, https://dialnet.unirioja.es/descarga/articulo/5238000.pdf

[10] Constitución Española 1978, Edición conmemorativa del cuadragésimo aniversario. Cortes Generales, Dirección de Estudios, Análisis y Publicaciones, Floridablanca, 28071. Madrid.

[11] CAFFERATA NORES, José I. La prueba en el proceso penal. Con especial referencia a la ley 23.984. 3ra. Edición. De Palma Ediciones. Buenos Aires. 1998, p. 33

[12] ORTEGA GUTIÉRREZ, David. Sinopsis del Art. 24 de la Constitución Española. http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=24&tipo=2

efectiva. "*Estas reglas, entendidas como un sistema formal por cuanto otorgan los mínimos básicos para la regulación del tema probatorio en un sistema jurídico determinado, son las encargadas de proveer el método de contrastación que dará a la prueba el aspecto de validez*"[13].

En este contexto la función de la prueba en materia penal es la de llevar al Juez o Tribunal a la convicción o convencimiento más allá de toda duda razonable de dos situaciones en particular, la primera de la ocurrencia o no de unos hechos y en segundo lugar sobre la responsabilidad o no de la persona procesada.

3.- Fuentes y Medios Probatorios

A decir de Claudio Meneses Pacheco, la prueba en juicio, se sostiene que tanto fuentes como medios probatorios, se constituyen en datos empíricos que sirven de sustento a la actividad probatoria y al resultado de ésta. En este sentido, ambos son elementos (personas y cosas) el primero en el campo substancial, y el segundo como una actividad procesal concreta que suministran información fáctica. La diferencia entre uno y otro radica en el escenario donde se sitúan, pues mientras las fuentes de prueba se ubican en un plano previo y ajeno al proceso jurisdiccional (es decir son pre existentes e independientes al proceso), los medios de prueba se instalan en el contexto del juicio. La relación entre ambos surge, en definitiva, del modo como cada sistema de procesal determina la procedencia de los medios de prueba; en otras palabras, el asunto consiste en resolver cuáles fuentes de prueba pueden ser incorporadas a un juicio como medios de prueba relevantes y jurídicamente admisibles[14].

En delitos como el fraude informático o de falsificación electrónica, los medios de prueba[15] generalmente son de carácter documental, también pueden ser acompañados de dictámenes periciales, esto en razón de que esta clase de infracciones son del tipo ocupacional (característica común en la mayoría de delitos informáticos). Esto significa que la persona o personas que cometen esta variedad de actos delictivos en un noventa por ciento (90%) trabajan dentro de las instituciones afectadas; en consecuencia, la prueba de estas infracciones se encuentra generalmente en los equipos y programas informáticos, en los documentos electrónicos[16] y en los demás mensajes de datos que utilizan e intercambian estas personas en su red de trabajo. Situación la cual hace indispensable que el investigador, cuente con el conocimiento suficiente sobre la validez de la evidencia digital

---

[13] LÓPEZ CABELLO, Fernando Alday. La regla de exclusión de la prueba ilícita en España, estudio comparado con la actualidad mexicana. **http://hdl.handle.net/10803/659086**.

[14] MENESES PACHECO, Claudio. Revista IUS ET PRAXIS, ISSN 0717-2877, Vol. 14, No. 2, 2008, págs. 43-86. https://dialnet.unirioja.es/servlet/articulo?codigo=3054272

[15] Procedimiento que establece la Ley para ingresar un elemento de prueba en un proceso, por ejemplo, las formalidades para brindar testimonio, o el contenido de un acta de reconocimiento.

[16] Sobre documentos electrónicos hay que tomar en cuenta lo que señala la Ley 59/2003, de 19 de diciembre, relacionada con la firma electrónica, que señala en su artículo 3, cuando se refiere a los documentos electrónicos como: "(…) *la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado*". https://www.boe.es/buscar/act.php?id=BOE-A-2003-23399

en el proceso judicial y también acerca del funcionamiento de toda clase de sistemas informáticos, tanto como una sólida formación en cómputo forense y la capacidad para la administrar las evidencias e indicios de convicción aptos para lograr una condena en esta clase de delitos.

En la Ley de Enjuiciamiento Civil de España, encontramos que el Art. 4, señala que: "*En defecto de disposiciones en las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, serán de aplicación, a todos ellos, los preceptos de la presente Ley*".

Esta norma es importante ya que el la Ley de Enjuiciamiento Penal española no se encuentra alusión alguna a los medios probatorios que se pueden utilizar dentro del proceso penal. Por tanto, nos toca remitirnos específicamente a la disposición de la Ley de Enjuiciamiento Civil[17], donde se dice que los medios de que se podrá hacer uso en juicio son: el interrogatorio de las partes, los documentos públicos y privados, el dictamen de peritos, el reconocimiento judicial, el interrogatorio de testigos.

Además, en el numeral 2do del Art. 299 LEC se señala que: "*También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso*". Cabe mencionar también que en concordancia el Art. 382 LEC señala que estos medios probatorios deben ser valorados por el Tribunal de acuerdo a la sana crítica[18].

Finalmente, su numeral 3ro del mismo artículo dice: "*Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias*".

De lo expuesto podemos concluir que la evidencia digital en forma de mensajes de datos, es decir como cualquier dato o información, transmitida, generada, almacenada o enviada a través de un sistema informático o telemático puede ser estimada como medio probatorio relevante y jurídicamente admisible al amparo del Art. 299 de la Ley de Enjuiciamiento Civil, en concordancia con los artículos 382, 383 y 384 ibidem, adoptando para este caso la utilización de los principios, métodos y

---

[17] Los artículos pertinentes son el 299, 382, 383 y 384 de la Ley de Enjuiciamiento Civil. Estos permiten la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes. https://www.boe.es/buscar/act.php?id=BOE-A-2000-323.

[18] La sana crítica es el arte de juzgar, atendiendo a la bondad y verdad de los hechos, sin vicios ni error, mediante la lógica, la dialéctica, la experiencia, la equidad y las ciencias y artes afines y auxiliares y la moral, para alcanzar y establecer, con expresión motivada, la certeza sobre la prueba que se produce en el proceso. ARAZI, Roland. La Prueba en el Derecho Civil. Buenos Aires (Argentina): Ediciones La Roca, 1991, pp. 89 y s. Citado por Boris Barrios en Teoría de la Sana Crítica. Publicado en OPINIÓN JURÍDICA vol. 2, No. 3 pp. 99-132. http://www.academiadederecho.org/upload/biblio/contenidos/Teoria_de_la_sana_critica_Boris_Barrios.pdf

técnicas de la informática forense.

4.- Las Ciencias Forenses

Las Ciencias Forenses[19] son la utilización de procedimientos y conocimientos científicos para encontrar, adquirir, preservar y analizar las evidencias de un delito y presentarlas apropiadamente a una Corte de Justicia. Las ciencias forenses tienen que ver principalmente con la recuperación y análisis de la llamada evidencia latente, como por ejemplo las huellas digitales, la comparación de muestras de ADN, etc. Las ciencias forenses combinan el conocimiento científico y las diferentes técnicas que este proporciona con los presupuestos legales a fin de demostrar con la evidencia recuperada la existencia de la comisión de un acto considerado como delictivo y sus posibles responsables ante un Tribunal de Justicia.

Las ciencias forenses han sido desarrolladas desde hace mucho tiempo atrás. Uno de los primeros textos y estudios en este campo los podemos ubicar en el año de 1248 DC, cuando el médico chino HI DUAN YU, escribió el libro "**COMO CORREGIR LOS ERRORES**", en el cual se explicaban las diferencias entre una muerte por ahogamiento y otra por una herida de cuchillo al igual que la muerte por causas naturales.

Posteriormente con el avance de la ciencia y la tecnología, las ciencias forenses han alcanzado un desarrollo inconmensurable, pero ese desarrollo a veces no ha ido de la mano del avance de la legislación penal. Esto en razón del retraso en la incorporación de nuevos elementos de prueba y medios probatorios y sobre todo en la demora de la admisibilidad de nuevas evidencias o pruebas. Este es el caso por ejemplo de la prueba de ADN que fue admitida en un juicio recién en el año de 1996, pero su desarrollo y comprensión se logró desde la década de los ochentas.

Las ciencias forenses siempre están en constante cambio, siempre buscando nuevos métodos y procesos para encontrar y fijar las evidencias de cualquier tipo. Creando nuevos estándares y políticas. Son más de ochocientos años de experiencia como disciplina científica.

4.1.- La Informática Forense

Es una ciencia forense que se ocupa de la utilización de los métodos científicos aplicables a la investigación de los delitos, no solo Informáticos y donde se utiliza el análisis forense de las evidencias digitales, en fin, toda información o datos que se guardan en una computadora o sistema informático[20]. En conclusión, diremos que Informática Forense es "*la ciencia forense que se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital, para luego ésta ser presentada en una Corte de Justicia*"[21].

---

[19] Forense significa "Traer a la Corte"

[20] Sistema Informático: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

[21] ACURIO DEL PINO, Santiago. Derecho Penal Informático, Segunda Edición 2017.

La informática forense es el vehículo idóneo para localizar y presentar de forma adecuada los hechos jurídicos informáticos relevantes dentro de una investigación, ya sea de carácter civil o penal.

La ciencia forense es sistemática y se basa en hechos premeditados para recabar pruebas para luego analizarlas. La tecnología, en caso de la identificación, recolección y análisis forense[22] en sistemas informáticos, son aplicaciones que hacen un papel de suma importancia en recaudar la información y los elementos de convicción necesarios. La escena del crimen es el computador y la red a la cual éste está conectado.

Históricamente la ciencia forense siempre ha basado su experiencia y su accionar en estándares de práctica y entrenamiento, a fin de que las personas que participan o trabajan en este campo científico tengan la suficiente probidad profesional y solvencia de conocimientos para realizar un buen trabajo en su área de experiencia. Esta situación debe ser igual en el campo de la Informática forense, es por tanto necesario que las personas encargadas de este aspecto de la ciencia forense tengan parámetros básicos de actuación, no solo en la incautación y recolección de evidencias digitales, sino también en su procesamiento, cumpliendo siempre con los principios básicos del debido proceso.

El objetivo de la Informática forense es el de recobrar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal.

De otro lado, esta ciencia forense necesita de una estandarización de procedimientos y de acciones a tomar, esto en razón de las características específicas que las infracciones informáticas presentan. Son entonces estas propiedades que contribuyen a la existencia de una confusión terminológica y conceptual presente en todos los campos de la informática, especialmente en lo que dice relación con sus aspectos criminales.

Para finalizar hay que tomar en cuenta lo que dice Jeimy Cano en su libro "Computo Forense" al referirse a la informática forense: "*La informática forense es la manifestación natural del entorno digital y de la sociedad de la información para responder a la creciente ola de incidentes, fraudes y ofensas (en medios informáticos y a través de medios informáticos), con el fin de enviar un mensaje claro a los intrusos: estamos preparados para responder a sus acciones, y continuamos aprendiendo para*

https://www.academia.edu/33039698/Derecho_Penal_Inform%C3%A1tico_Segunda_Edici%C3%B3n_2017

[22] Se define como una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar la administración de justicia en su lucha contra los posibles delincuentes o como disciplina especializada que procura el esclarecimiento de los hecho, de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos, bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la (in) seguridad informática. CABALLERO, María Ángeles y CILLEROS SERRANO, Diego. El Libro del Hacker 2018. Ediciones ANAYA Multimedia, 2018, Madrid.

dar con la verdad de sus acciones"[23].

5.- Rol del Sistema Informático en el ITER CRIMINIS

De lo expuesto es importante clarificar los conceptos y describir la terminología adecuada que nos señale el rol que tiene un sistema informático dentro del *ITER CRIMINIS* o camino del delito. Esto a fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener nuestro caso. Es así que, por ejemplo, el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que, se utilice en un fraude informático, por tanto, el rol que cumpla el sistema informático determinara donde debe ser ubicada y como debe ser usada la evidencia.

Ahora bien, para este propósito se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (*evidencia electrónica*) y la información contenida en este (*evidencia digital*). Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital. En este contexto el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, mensajes de datos y programas almacenados y trasmitidos usando el sistema informático.

5.1.- Hardware o Elementos Físicos

SISTEMA INFORMÁTICO	
HARDWARE (Elementos Físicos)	**Evidencia Electrónica**
• El hardware es mercancía ilegal o fruto del delito.	• El hardware es una mercancía ilegal cuando su posesión no está autorizada por la ley. Ejemplo: en el caso de los *skimers* o dispositivos de duplicación (clonación) de tarjetas de crédito, su posesión es un delito. • El hardware es fruto del delito cuando este es obtenido mediante robo, hurto, fraude u otra clase de infracción.
• El hardware es un instrumento	• Es un instrumento cuando el hardware cumple un papel importante en el cometimiento del delito, podemos decir que es usada como un arma o herramienta, tal como una pistola o un cuchillo. Un ejemplo serían los snifers y otros aparatos

[23] CANO M. Jeimy en Computación Forense: Descubriendo los Rastros Informáticos, Editorial ALFAOMEGA, Primera Edición, México, 2009, Pág. 10

SISTEMA INFORMÁTICO	
HARDWARE (Elementos Físicos)	**Evidencia Electrónica**
	especialmente diseñados para capturar el tráfico en la red o interceptar comunicaciones.
• El hardware es evidencia	• En este caso el hardware no debe ni ser una mercancía ilegal, fruto del delito o un instrumento. Es un elemento físico que se constituye como prueba de la comisión de un delito. Por ejemplo, el scanner que se usó para digitalizar una imagen de pornografía infantil, cuyas características únicas son usadas como elementos de convicción

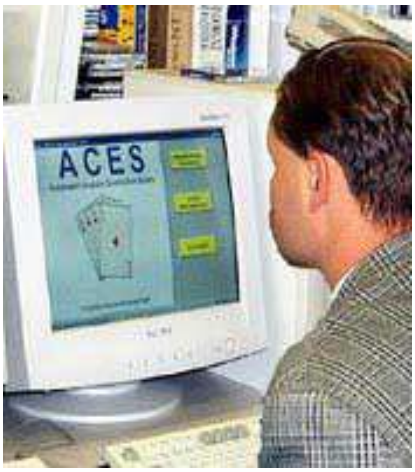
5.2.- Información

SISTEMA INFORMÁTICO	
INFORMACIÓN	**Evidencia Digital**
• La información es mercancía ilegal o el fruto del delito.	La información es considerada como mercancía ilegal cuando su posesión no está permitida por la ley, por ejemplo, en el caso de la pornografía infantil. De otro lado será fruto del delito cuando sea el resultado de la comisión de una infracción, como por ejemplo las copias pirateadas de programas de ordenador, secretos industriales robados.
• La información es un instrumento	La información es un instrumento o herramienta cuando es usada como medio para cometer una infracción penal. Son por ejemplo los programas de ordenador que se utilizan para romper las seguridades de un sistema informático, sirven para romper contraseñas o para brindar acceso no autorizado. En definitiva, juegan un importante papel en el cometimiento del delito.
• La información es evidencia	Esta es la categoría más grande y nutrida de las anteriores, muchas de nuestras acciones diarias dejan un rastro digital. Uno puede conseguir mucha información como evidencia, por ejemplo, la información de los proveedores de servicios de internet, de los bancos, y de las proveedoras

SISTEMA INFORMÁTICO	
INFORMACIÓN	**Evidencia Digital**
	de servicios las cuales pueden revelar actividades particulares de los sospechosos

En resumen, el propósito fundamental de las categorías antes mencionadas es el de enfatizar el papel que juegan los sistemas informáticos en la comisión de delitos, a fin de que el investigador criminal tenga un derrotero claro y preciso al buscar los elementos convicción que aseguren el éxito dentro de un proceso penal. En estas condiciones para efectos probatorios son objeto de examen, tanto el hardware como la información contenida en este.

6.- Evidencia Digital



En derecho procesal la evidencia es la certeza clara, manifiesta y tan perceptible que nadie puede dudar de ella. De otro lado la evidencia digital es cualquier mensaje de datos almacenado y trasmitido por medio de un sistema de información que tenga relación con el cometimiento de un acto que comprometa gravemente dicho sistema y que posteriormente guie a los investigadores al descubrimiento de los posibles infractores. En definitiva, son campos magnéticos y pulsos electrónicos que pueden ser recogidos y analizados usando técnicas y herramientas especiales[24], no es otra forma de EVIDENCIA LATENTE, necesita para su recolección y preservación principios científicos y un marco legal apropiado.

Para Miguel López Delgado la evidencia digital es el conjunto de datos en formato binario, esto es comprende los archivos, su contenido o referencias a éstos (metadatos[25]) que se encuentren en los soportes físicos o lógicos de un sistema comprometido por un incidente informático[26].

Otros autores como Anthony Reyes[27] se refieren a la evidencia digital como "**OBJETOS DE DATOS**" en relación a la información que es encontrada en los dispositivos de almacenamiento o en las piezas de almacenamiento multimedia, que no son más que cadenas de unos y ceros es decir de información binaria o digital grabada en un dispositivo magnético

[24] CASEY Eoghan, Handook of Computer Investigation, Elsevier Academia Press, 2005

[25] El término meta proviene del griego y significa *junto a, después, siguiente*. Los metadatos pueden ser definidos como datos sobre los datos. Son como las etiquetas de un producto, nos brinda información relativa a este como, el peso fecha de caducidad, etc. Tecnologías de la Información a la comunicación ALONSO, Juan A. y otros, Editorial ALFAOMEGA y RA-MA, 2005

[26] LOPEZ DELGADO, Miguel, Análisis Forense Digital, junio del 2007, CRIPORED.

[27] REYES, Anthony, Investigación del Cibercrimen, Syngress 2007.

(como discos duros o los disquetes), en uno de estado sólido[28] o memoria solida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD, BLUERAY).

Estos objetos de datos podemos encontrarlos en una gran cantidad de dispositivos tales como computadores personales, teléfonos celulares, los cuales tienen sistemas operativos y programas que combinan en un particular orden esas cadenas de unos y ceros para crear imágenes, documentos, música y muchas cosas más en formato digital. Pero también existen otros objetos de datos que no están organizados como archivos, son informaciones que están vinculadas a archivos como los metadatos antes mencionados, otros son fragmentos de archivos que quedan después de que se sobrescribe la información a causa del borrado de los archivos viejos y la creación de los archivos nuevos esto se llama SLACK SPACE, o espacio inactivo. También pueden quedarse almacenados temporalmente en los archivos de intercambio (SWAP FILE) o en la misma memoria RAM.

6.1.- Fuentes de la Evidencia Digital

Como ya se advirtió anteriormente algunas personas tienden a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo, es necesario distinguir entre aparatos electrónicos como los celulares y teléfonos inteligentes y la información digital que estos contengan. Esto es indispensable ya que el foco de nuestra investigación siempre será la evidencia digital, aunque en algunos casos también serán los aparatos electrónicos.

A fin de que los investigadores forenses tengan una idea de dónde buscar evidencia digital, éstos deben identificar las fuentes más comunes de evidencia. Situación que brindará al investigador el método más adecuando para su posterior recolección y preservación.

Las fuentes de evidencia digital pueden ser clasificadas en tres grandes grupos:

1. **SISTEMAS DE COMPUTACIÓN ABIERTOS**, son aquellos que están compuestos de las llamadas computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles, y los servidores. Actualmente estos computadores tienen la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital.
2. **SISTEMAS DE COMUNICACIÓN,** estos están compuestos por las redes de telecomunicaciones, la comunicación

[28] Más conocidos como SSD (Solid-State Drive) son dispositivos de almacenamientos de datos que usan una memoria sólida para almacenar la información de forma constante de forma similar que un disco duro usando lo que se conoce como SRAM (Memoria de Acceso Randómico Estático) o DRAM (Memoria de Acceso Randómico Dinámico). Estas memorias simulan la interfaz de un disco magnético convirtiéndose en dispositivos de almacenamiento masivo.

inalámbrica y el Internet. Son también una gran fuente de información y de evidencia digital.

3. **SISTEMAS CONVERGENTES DE COMPUTACIÓN,** son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital[29].

Por otro lado, y dada la ubicuidad de la evidencia digital es raro el delito que no esté asociado a un mensaje de datos guardado y trasmitido por medios informáticos. Un investigador entrenado puede usar el contenido de ese mensaje de datos para descubrir la conducta de un infractor, puede también hacer un perfil de su actuación, de sus actividades individuales y relacionarlas con sus víctimas.

A pesar de esto mucha evidencia digital es pasada por alto, o no es recuperada de forma correcta o no es analizada de forma que permita ser un indicio que compruebe o niegue nuestra teoría del caso. La idea es que el investigador pueda tener un criterio formado acerca de la evidencia digital y como esta puede ser usada en un proceso judicial (en materia penal o en materia no penal) o un problema dentro de una empresa, dada la masificación en el uso de las TICS, tanto en el sector privado como en el público.

6.1.1.- Incautación de Equipos Informáticos o Electrónicos

Si el investigador presume que existe algún tipo evidencia digital en algún aparato electrónico o en algún otro soporte material o dispositivo de almacenamiento relacionado con el cometimiento de una infracción. Este debe pedir la correspondiente autorización judicial para incautar dichos elementos, de igual forma debe tener la autorización judicial para acceder al contenido guardado, almacenado y generado por dichos aparatos, los cuales deben ser debidamente individualizados en la petición correspondiente[30].

Con la reforma de la Ley Orgánica 13/2015, de 5 de octubre, se modifica la Ley de Enjuiciamiento Criminal española y se introducen reformas para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. En este sentido hay nuevas reglas para el registro y secuestro de dispositivos de almacenamiento masivo de información que viene a regular más sólidamente todo acto de injerencia[31]

---

[29] Se trata de una característica que presenta el actual desarrollo de las infraestructuras de red y de los dispositivos terminales, que les permite, pese a su naturaleza diversa, transmitir y recibir, en esencia, la misma información, todo ello girando en torno a la digitalización de los contenidos que se transmiten y conduciendo ineludiblemente a una transformación de la actividad económica que desarrollaban en forma separada las empresas de telecomunicaciones, de informática y de contenidos audiovisuales. Ciberespacio, Sociedad y Derecho, HERRERA BRAVO Rodolfo, en el Libro Derecho a las Nuevas Tecnologías, Editorial La Rocca, 2007.

[30] En la Ley Orgánica 13/2015, de 5 de octubre se confiere sustantividad propia a otras formas de comunicación telemática que han carecido de tratamiento normativo en la ley procesal criminal.

[31] En la Exposición de motivos de la Ley Orgánica 13/2015, de 5 de octubre, se menciona que toda medida deberá responder al principio de especialidad. Ello exige que la actuación de que se trate tenga por objeto el esclarecimiento de un hecho punible concreto, prohibiéndose pues las medidas de investigación tecnológica de naturaleza prospectiva, de acuerdo con el concepto que informa la doctrina emanada del máximo intérprete de la Constitución, por todas las sentencias

en los derechos reconocidos en el Art. 18 de la Constitución española, por ello es necesario hacer algunas acotaciones:

- Antes de realizar una entrada y registro a un domicilio y la incautación de equipos informáticos o electrónicos se debe tomar en cuenta lo siguiente:

    1. ¿A qué horas debe realizarse?
        i. Para minimizar destrucción de equipos, datos
        ii. El sospechoso tal vez estará en línea, es necesaria la interceptación de datos.
        iii. Seguridad de investigadores.
    2. Entrar sin previo aviso
        i. Utilizar seguridad
        ii. Evitar destrucción y alteración de los equipos, o la evidencia contenida en esta.
    3. Materiales previamente preparados (Cadena de custodia)
        i. Embalajes de papel
        ii. Etiquetas
        iii. Discos duros vacíos
        iv. Herramienta
        v. Cámara fotográfica
    4. Realizar simultáneamente los allanamientos e incautación en diferentes sitios.
        i. Datos pueden estar en más de un lugar, sistemas de red, conexiones remotas.
    5. Examen de equipos
    6. Aparatos no especificados en la orden de allanamiento
    7. Creación de Respaldos en el lugar, creación de imágenes de datos.
        i. Autorización para duplicar, reproducir datos encontrados.
    8. Fijar/grabar la escena
        i. Cámaras, videos, etiquetas
    9. Códigos/claves de acceso/contraseñas
    10. Buscar documentos que contienen información de acceso, conexiones en redes, etc.
    11. Cualquier otro tipo de consideración especial (consideraciones de la persona involucrada: médicos, abogados, información privilegiada, etc.)

- En una investigación penal, hay que tomar en consideración que se puede limitar ciertos derechos (protección de datos personales, secreto a las comunicaciones, derecho a la intimidad) de las personas, es así que el investigador debe garantizar en todo momento el debido proceso

253/2006, de 11 de septiembre. Las medidas de investigación tecnológica deben además satisfacer los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad, cuya concurrencia debe encontrarse suficientemente justificada en la resolución judicial habilitadora, donde el juez determinará la naturaleza y extensión de la medida en relación con la investigación concreta y con los resultados esperados.

con la finalidad de que no se excluyan las evidencias obtenidas durante la etapa investigativa, en tal circunstancia siempre debe tener la orden judicial correspondiente debidamente motivada.

- Con el fin de asegurar la autenticidad de los dispositivos de almacenamiento y la integridad de la información que estos contienen, se impone la utilización de un sistema de sellado o firma electrónica (función Hash[32]) que garantice la información volcada desde el sistema informático registrado[33].

6.1.2.- Dispositivos de Almacenamiento

Los dispositivos de almacenamiento son usados para guardar mensajes de datos e información de los aparatos electrónicos. Existen dispositivos de almacenamiento de tres clases, a saber: dispositivo magnético (como discos duros o los disquetes), dispositivos de estado sólido[34] o memoria solida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD).

Existen gran cantidad de Memorias USB en el mercado y otros dispositivos de almacenamiento como tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.

6.1.3.- Buenas Prácticas en cuanto a dispositivos electrónicos o informáticos.

1. Si el aparato está encendido "ON", no lo apague “OFF".
   - Si lo apaga "OFF" puede iniciarse el bloqueo del aparato.
   - Transcriba toda la información de la pantalla del aparato y de ser posible tómele una fotografía.
   - Vigile la batería del aparato, el transporte del mismo puede hacer que se descargue. Tenga a mano un cargador
   - Selle todas las entradas y salidas.
   - Selle todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria
   - Selle los tornillos para evitar que se puedan retirar o reemplazar piezas internas.
   - Buscar y asegurar el conector eléctrico.
   - Colocar en una bolsa de FARADAY, los teléfonos celulares y SMARTFONES (especial para aislar de emisiones

---

[32] Es una función matemática que, a partir de un cierto volumen de datos, derivan una pequeña serie de datos, o huella digital como esta: 397B3732D63F53BF51FF5210551476F7. La función hash comprime los bits del mensaje a un valor hash de tamaño estable, de manera que distribuye los posibles mensajes uniformemente entre los posibles valores hash.

[33] Esta medida es para la plena validez de los documentos públicos o privados (Arts. 267 y 327 Ley de Enjuiciamiento Civil) aportados al proceso en formato electrónico y acoge una línea jurisprudencial de la Sala Segunda del Tribunal Supremo.

[34] Más conocidos como SSD (Solid-State Drive) son dispositivos de almacenamientos de datos que usan una memoria sólida para almacenar la información de forma constante de forma similar que un disco duro usando lo que se conoce como SRAM (Memoria de Acceso Randómico Estático) o DRAM (Memoria de Acceso Randómico Dinámico). Estas memorias simulan la interfaz de un disco magnético convirtiéndose en dispositivos de almacenamiento masivo.

electromagnéticas), si no hubiere disponible, en un recipiente vacío de pintura con su respectiva tapa.
- Revise los dispositivos de almacenamiento removibles. (Algunos aparatos contienen en su interior dispositivos de almacenamiento removibles tales como tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.)

2. Si el aparato está apagado "OFF", déjelo apagado "OFF".
   - Prenderlo puede alterar evidencia al igual que en las computadoras.
   - Antes del análisis del aparato consiga un técnico capacitado en el mismo.
   - Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

3. Recolecte las instrucciones de uso, los manuales y las notas de cada uno de los dispositivos encontrados.
4. Documente todos los pasos al revisar y recolectar los dispositivos de almacenamiento
5. Aleje a los dispositivos de almacenamiento de cualquier magneto, radio trasmisores y otros dispositivos potencialmente dañinos.

6.2.- Evidencia Digital Constante y Volátil

En un principio el tipo de evidencia digital que se buscaba en los equipos informáticos era del tipo CONSTANTE o PERSISTENTE es decir la que se encontraba almacenada en un disco duro o en otro medio informático y que se mantenía preservada después de que la computadora era apagada. Posteriormente y gracias a las redes de interconexión, el investigador forense se ve obligado a buscar también evidencia del tipo VOLÁTIL, es decir evidencia que se encuentra alojada temporalmente en la memoria RAM, o en el CACHE, son evidencias que por su naturaleza inestable se pierden cuando el computador es apagado. Este tipo de evidencias deben ser recuperadas casi de inmediato.

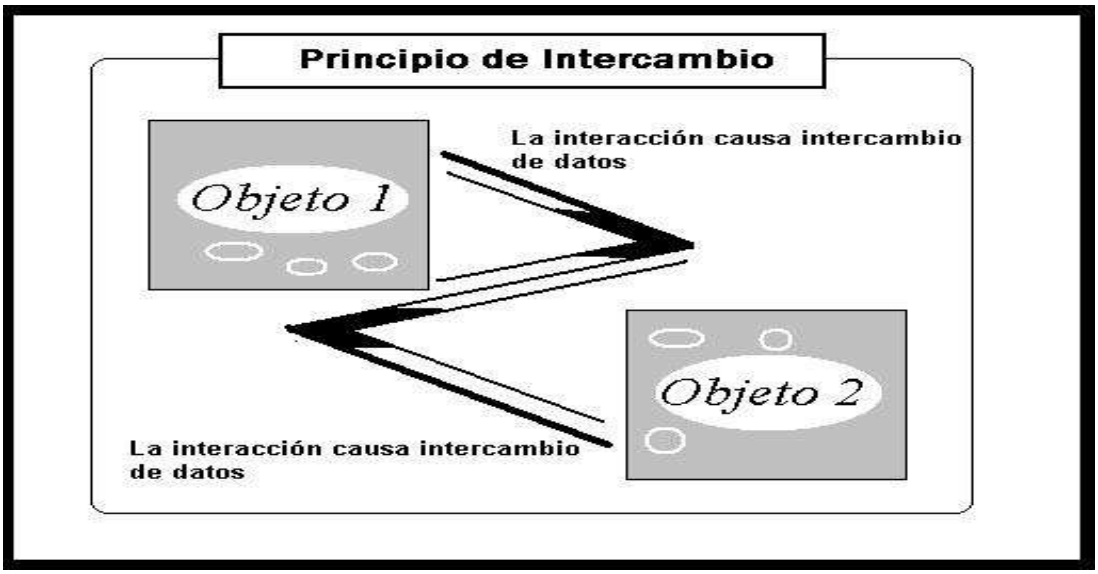
De lo dicho se desprende que cuando se comete un delito cualquiera, muchas veces la información que directa o indirectamente se relaciona con esta conducta criminal queda almacenada en forma digital dentro de un Sistema Informático. Este conjunto de datos ordenados sistemáticamente y convertidos en información se convierte en evidencia digital. He aquí entonces que encontramos la primera dificultad en lo que se refiere a la obtención de esta clase de evidencia como prueba de la infracción cometida, esto debido a que los sistemas informáticos en donde se almacena la misma presentan características técnicas propias, en tal razón la información ahí almacenada no puede ser recuperada, recolectada, preservada, procesada y posteriormente presentada como indicio de convicción utilizando los medios crimínalisticos comunes, se debe utilizar mecanismos diferentes a los tradicionales. Es aquí que se ve la necesidad de utilizar los procedimientos técnicos legales como el acceso remoto y la rigurosidad científica que pone a disposición de los investigadores la ciencia

forense informática a fin de descubrir a los autores y cómplices del delito cometido.

6.3.- Dinámica de la evidencia

La dinámica de la evidencia es la forma como se entienden y se describen los diferentes factores (humanos, de la naturaleza, de los equipos) que actúan sobre las evidencias, a fin de determinar los cambios que estos producen sobre ellas.

Podemos afirmar indudablemente que existen muchos agentes que intervienen o actúan sobre la evidencia digital, aquí se aplica el llamado principio de intercambio o de Locard[35]; el investigador forense se ve en la necesidad de reconocer la forma como estos factores pueden alterar la evidencia, y así tener la oportunidad de manejarla de una manera apropiada, evitando generalmente contaminarla, dañarla y hasta perderla por completo.



Los principios crimínalisticos, como el de Locard o de intercambio y el mismisidad[36] deben tenerse como instrumentos de la investigación en cualquier escena del crimen inclusive la informática. Esto se puede explicar por ejemplo en el caso de las bitácoras o LOGS del sistema operativo de un equipo informático utilizado por un Hacker o Cracker para romper las seguridades de un programa o vulnerar la integridad de un sistema informático remoto. En dicha bitácora el investigador podría encontrará registrada dicha actividad ilegal. Ese es un ejemplo del principio de intercambio en acción.

Cuando en una escena del crimen se tiene que trabajar en condiciones adversas, como en incendios, inundaciones, derrames de

[35] El principio de intercambio de Locard, menciona que cuando dos objetos entran en contacto siempre existe una transferencia de material entre el uno y el otro. Es decir que cuando una persona está en una escena del crimen esta deja algo de sí misma dentro de la escena, y a su vez cuando sale de ella esta se lleva algo consigo.

[36] Una cosa es igual a sí misma y diferente de las demás.

gasolina o químicos peligrosos, es indispensable que el investigador tome las medidas de seguridad necesarias para asegurar en primer lugar su integridad física, luego deberá implementar el procedimiento más adecuado para incrementar las posibilidades de recuperar las evidencias de la manera más completa. De lo dicho podemos manifestar que los examinadores forenses nunca tendrán la oportunidad de revisar una escena del crimen en su estado original, siempre habrá algún factor que haga que la escena del crimen presente algunas anomalías o discrepancias.

Con la finalidad de explicar cómo funciona la dinámica de las evidencias, a continuación, se expondrán algunas de las posibles situaciones en donde esta se ve afectada dentro de una escena del crimen:

1. **EQUIPOS DE EMERGENCIAS:** En el caso de un incendio, los sistemas informáticos pueden ser afectados por el fuego y el humo, posteriormente sometidos a una gran presión de agua al tratar de apagar este. Esto provoca que los técnicos forenses no puedan determinar a ciencia cierta si los sistemas informáticos encontrados en la escena estuvieron comprometidos, fueron atacados o usados indebidamente. En otras ocasiones los equipos de emergencia manipulan la escena cuando es necesario para salvar la vida de una persona.
2. **PERSONAL DE CRIMINALÍSITICA Y FUERZAS DE SEGURIDAD**[37]**:** En algunas ocasiones el personal de criminalística o de las fuerzas de seguridad por accidente cambia, reubica, o altera la evidencia. Por ejemplo, en el caso de que se quiera sacar una muestra de sangre de una gota precipitada sobre un disquete o disco compacto mediante el uso de un escarpelo, esto puede accidentalmente comprometer los datos e información almacenada en dichos soportes.
3. **EL SOSPECHOSO O EL IMPUTADO TRATANDO DE CUBRIR SUS RASTROS**: Cuando el Sospechoso o el imputado deliberadamente borra o altera los datos, registros u otros mensajes de datos considerados como evidencia dentro de un disco duro.
4. **ACCIONES DE LA VÍCTIMA**: La víctima de un delito, puede borrar correos electrónicos que le causen aflicción o le provoquen alguna situación embarazosa.
5. **TRANSFERENCIA SECUNDARIA**: En algunas ocasiones, los sistemas informáticos usados en el cometimiento de un delito, son usados posteriormente por alguna persona de forma inocente, causando con ello la destrucción y alteración de evidencia.

[37] Se tiene que minimizar todo rastro del investigador en la escena del delito. Una historia clásica en estos casos es la del investigador forense que encontró una huella digital dentro de un caso de homicidio, al recuperar y preservar dicha huella creyó tener la pista necesaria para resolver el caso. Pues hizo comparar dicha huella digital con la base de datos de la Policía Judicial, al no encontrar un resultado, amplió la búsqueda a nivel nacional encontrándose que la huella encontrada en la escena era suya.

6. **TESTIGOS**: Un administrador del sistema puede borrar cuentas de usuarios sospechosas, las mismas que fueron creadas por un intruso, a fin de prevenir su acceso y utilización futura.
7. **EL CLIMA Y LA NATURALEZA**: Los campos electromagnéticos pueden corromper la información guardada en discos magnéticos.
8. **DESCOMPOSICIÓN:** En algunos casos la información almacenada en discos magnéticos, o en otros soportes puede perderse o tornarse ilegible para los sistemas de información, a causa del tiempo y de las malas condiciones de almacenamiento.

En resumen el investigador forense debe entender como los factores humanos, de la naturaleza y de los propios equipos informáticos pueden alterar, borrar o destruir evidencia, debe comprender como dichas variables actúan sobre la escena misma del delito, debe por tanto encaminar la investigación desde su etapa más temprana tomando en cuenta esos cambios, a fin de adecuar el mejor método para adquirir, preservar y luego analizar las pistas obtenidas, y así reducir de manera considerable los posibles efectos de la dinámica de la evidencia.

6.4.- Entendimiento y relevancia de la Evidencia Digital

Los problemas tradicionales al manejar investigaciones relacionadas con equipos informáticos, es la forma como se recupera la información digital o electrónica de esta clase de equipos, en otras palabras, el problema radica en cómo instrumentalizar un procedimiento o un método adecuado para realizar esta tarea, cumpliendo con la premisa de que estas prácticas deben ser aceptadas y puestas en acción de forma universal, esto en relación a las capacidades que muestran los operadores de justicia en el uso de la informática forense dentro de sus áreas de influencia. Esto debido a la CIBERFOBIA o miedo a la nueva tecnología que experimentan algunos jueces, fiscales e incluso los cuerpos de seguridad del estado, situación que hace que el uso de técnicas forenses con el fin de recuperar y preservar la evidencia digital sea considerado una práctica poco ortodoxa en el mundo analógico en el que todavía viven algunos operadores de justicia.

La Ley de Enjuiciamiento Criminal no ha podido sustraerse al paso del tiempo, como se señala en la exposición de motivos de la reforma del 2015, ya que las nuevas y renovadas formas de delincuencia ligadas al uso de las nuevas tecnologías han puesto de manifiesto la insuficiencia de un cuadro normativo concebido para tiempos bien distintos.

La evidencia es la materia que usamos para persuadir al tribunal o al juez de la verdad o la falsedad de un hecho que está siendo controvertido en un juicio. Los flujos de información generados por los sistemas de comunicación telemática actuales advierten de las posibilidades que se hallan al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos. Surge así la necesidad

de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que el sistema constitucional español garantiza a cada ciudadano frente a terceros. Son entonces las normas procesales y las reglas del debido proceso las que informarán al juez o al tribunal que evidencias son relevantes y admisibles dentro de un proceso judicial y cuáles no lo son.

Por muy estimable que haya sido el esfuerzo de jueces y tribunales españoles para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática del sistema procesal español antes de la reforma del 2015, situación ya criticada tanto por el entorno académico como por los otros países pertenecientes a la Unión Europea. Ultimadamente, el Tribunal Constitucional español ha apuntado el carácter ineludible de una regulación que aborde las intromisiones en la privacidad del investigado en un proceso penal que puede llevar a la exclusión[38] de los medios de prueba obtenidos de forma ilegal o ilegítima.

En la investigación de algunos hechos delictivos, la incorporación al proceso de los datos electrónicos de tráfico[39] o asociados puede resultar de una importancia decisiva. La reforma del 2015 acoge el criterio fijado por la Ley 25/2007[40], de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, e impone la exigencia de autorización judicial para su cesión a los agentes facultados, siempre que se trate de datos vinculados a procesos de comunicación. Su incorporación al proceso solo se autoriza cuando se trate de la investigación de delitos informáticos que en base al principio de proporcionalidad justifican el sacrificio de la inviolabilidad de las comunicaciones. Se da un tratamiento jurídico individualizado al acceso por los investigadores al IMSI[41], IMEI[42], dirección IP[43] y otros elementos de identificación de una determinada tarjeta SIM o terminal informático, en

---

[38] La regla de exclusión probatoria consiste en que cualquier elemento de prueba que se haya obtenido o incorporado al proceso en violación de una garantía constitucional, o de las formas procesales dispuestas para su producción, queda descartado dentro del proceso judicial. CARRIÓ, Alejandro, Justicia Criminal, Citado por JAUCHEN, Eduardo, Tratado de la Prueba Material, Rubinzal-Culzoni Editores, 2000, pág. 614.

[39] Se entenderán por datos de tráfico todos los datos relativos a una comunicación realizada por medio de un sistema informático o de información, generados por este último en tanto sea parte de la cadena de comunicación y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente. Definición dada por el Convenio de Cibercriminalidad de la Unión Europea, en concordancia con lo dispuesto en el Art. 588 ter b de la Ley de Enjuiciamiento Criminal.

[40] https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243

[41] IMSI es el acrónimo de International Identidad Internacional del Abonado Móvil. Es un código de identificación único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS

[42] IMEI- Identificador internacional del equipo móvil (por sus siglas en inglés) o sus equivalentes en el futuro, código variable pregrabado en los equipos terminales móviles que los identifican de manera específica

[43] **Internet Protocol (IP) Numbers o IP adresses (Protocolo de Internet, números)**: Un identificador numérico único usado para especificar anfitriones y redes. Los números IP son parte de un plan global y estandarizado para identificar computadores que estén conectados a Internet. Se expresa como cuatro números del 0 al 255, separado por puntos: 188.41.20.11.

consonancia con una jurisprudencia del Tribunal Supremo ya consolidada sobre esta materia.

En conclusión, se debe entender a la evidencia digital[44] como una muy poderosa herramienta, es la perfecta memoria de lo que ha sucedido en una escena del delito, no existe razón para que esta mienta, por tanto, debe ser considerada como un medio de probatorio eficaz para acreditar la existencia de un hecho jurídico relevante, así como quien, y dónde y cómo esta se ha generado.

En el sistema mixto español la evidencia admisible, es la evidencia relevante o conducente como lo señala el Art. 299 de LEC. Es evidencia relevante aquella que tiene *valor probatorio, esto es, si posee alguna tendencia a hacer más o menos probable algún hecho de importancia para la resolución sobre el caso.*

La evidencia además de relevante también debe ser:

- **Autentica:** debe ser verídica y no haber sufrido manipulación alguna. Para ello se debe garantizar mediante el uso de la cadena de custodia en la evidencia física (Ej.: dispositivos de almacenamiento) y la aplicación de códigos de integridad (Función Hash) en la evidencia digital.
- **Completa:** debe representar la prueba desde un punto de vista objetivo y técnico, sin valoraciones personales, ni prejuicios.
- **Creíble:** debe ser comprensible.
- **Confiable:** las técnicas utilizadas para la obtención de la evidencia no deben generar ninguna duda sobre su veracidad[45].

7.- Procedimiento de Operaciones Estándar

Cuando se va revisar una escena del crimen del tipo informático es necesario tener en cuenta un procedimiento de operaciones estándar (POE), el mismo que es el conjunto de pasos o etapas que deben realizarse de forma ordenada al momento de recolectar o examinar la evidencia digital. Esta serie de procedimientos se utilizan para asegurar que toda la evidencia recogida, preservada, analizada y filtrada se la haga de una manera transparente e integra. La transparencia y la integridad metodológica (estabilidad en el tiempo de los métodos científicos utilizados) se requieren para evitar errores, a fin de certificar que los mejores métodos son usados, incrementado cada vez la posibilidad de que dos examinadores forenses lleguen al mismo

[44] Evidencia digital es cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático. Guía para el manejo de Evidencia Digital HB: 171 2003, citada por Cano M. Jeimy en Computación Forense: Descubriendo los Rastros Informáticos, Editorial ALFAOMEGA, Primera Edición, México, 2009, Pág. 3.

[45] La valoración de la prueba, debe realizarse de acuerdo al grado actual de aceptación científica y técnica de los principios en que se fundamenten, por ello la aplicación de estándares de obtención, recolección y presentación de evidencia digital como lo es la RFC 3227 (http://www.ietf.org/rfc/rfc3227.txt) es importante para el trabajo del investigador forense.

dictamen o conclusión cuando ellos analicen la misma evidencia por separado. A esto se lo conoce como reexaminación.

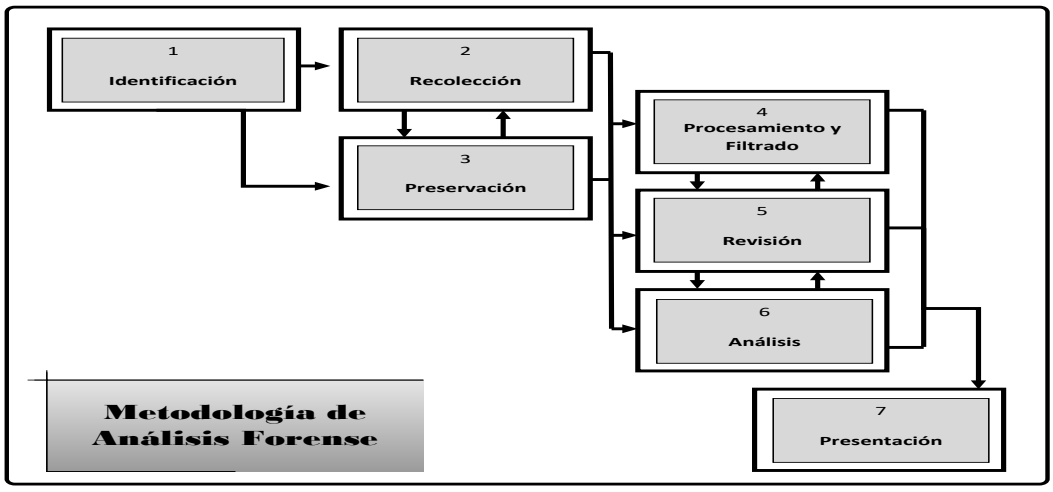
Realizar un análisis forense necesita metodologías y guías.

- Electronic Crime Scene Investigation
- UNE 71506:2013
- ISO/IEC 27037:2012
- Forensic Examination of Digital Evidence

El procedimiento de operaciones estándar forense debe tener las siguientes características[46]:

- **Verificable:** se debe comprobar la veracidad de las conclusiones extraídas a partir de la realización del análisis.
- **Reproducible:** se deben poder reproducir en todo momento las pruebas realizadas durante el proceso.
- **Documentado:** todo el proceso de estar correctamente documentado y debe realizarse de manera comprensible y detallada.
- **Independiente:** las conclusiones obtenidas deben ser las mismas, independientemente de la persona que realice el proceso y de la metodología analizada.

A nivel jurídico el investigador deberá utilizar una metodología forense que describe los pasos para obtener y presentar las evidencias encontradas en el proceso de reconocimiento y preservación de la evidencia, luego se seguirá con su procesamiento, filtrado, revisión y análisis, que finalmente nos llevaran a su presentación, que se encuentra esquematizada en el cuadro que a continuación se describe:



Cuadro 1: Metodología de Análisis Forense

[46] MARTÍNEZ RETENAGA, Asier. Guía de toma de evidencias en entornos Windows, con la colaboración de Daniel Fírvida Pereira y Jesús Díaz Vico, Madrid, 2014. http://www.incibe.es

En estos casos el orden es fundamental, ya que el desorden es enemigo de la claridad, por tanto el seguir los pasos en el orden correcto nos garantizara que la evidencia digital obtenida no sea, dañada o alterada en el proceso investigativo, además que también garantizaremos la cadena de custodia de los elementos físicos y los dispositivos de almacenamiento, a fin de que no haya duda de la procedencia de estos artefactos en la escena del delito, y que estos se han mantenido íntegros más allá de cualquier duda.

Cuando la evidencia es obtenida en violación de las garantías constitucionales y el no respeto a las reglas procesales que ordenan su producción, el órgano judicial no podrá basar ninguna de sus decisiones en una prueba viciada, es por tanto que este tipo de evidencia debe ser excluida y será ineficaz en cualquier proceso judicial[47].

Cabe mencionar que la reforma del 2015 a la ley procesal penal española pretende acabar con otro vacío normativo. Se trata del registro de dispositivos informáticos de almacenamiento masivo y el registro remoto de equipos informáticos. Respecto del primero de ellos, la reforma descarta cualquier duda acerca de que esos instrumentos de comunicación como teléfonos inteligentes y, en su caso, dispositivos almacenamiento de información son algo más que simples piezas de convicción. De ahí la exigente regulación respecto del acceso a su contenido. En lo que tiene que ver con registro remoto –diligencia ya presente en buena parte de las legislaciones europeas por vía del convenio de Budapest–, el intenso grado de intromisión que implica su adopción justifica que incluso se refuerce el ámbito objetivo de la medida, para lo que se han delimitado con un listado riguroso de los delitos que la pueden habilitar como son los de tipo informático, además de la utilización de herramientas para el rastreo informático de equipos y personas.

Durante la recolección de evidencia digital, el investigador deberá tener en cuenta las siguientes reglas básicas según la ciencia informática forense y los estándares normativos actuales[48].

[47] JAUCHEN, Eduardo, Tratado de la Prueba Material, Rubinzal-Culzoni Editores, 2000, pág. 615.

[48] MARTÍNEZ RETENAGA, ASIER. Guía de toma de evidencias en entornos Windows, con la colaboración de Daniel Fírvida Pereira y Jesús Díaz Vico, Madrid, 2014. http://www.incibe.es

8.- Conclusiones

Finalmente hay que considerar que las actuaciones que el Juez Instructor, el Ministerio Público Fiscal, y los Cuerpos de Seguridad deben estar enmarcadas en la obtención legítima de la prueba dentro de la investigación, para lo cual se debe tomar en consideración aspectos como:

EFECTIVIDAD DE LA PRUEBA	UTILIDAD DE LA PRUEBA
• Respeto por la protección de datos personales • Respeto por la intimidad personal • Respeto por el secreto de las comunicaciones • Respeto por la libertad de expresión	• Finalidad lícita • Necesidad de recolección • Transparencia en la recolección • Proporcionalidad en la recolección

9.- Bibliografía

GIMÉNEZ-SALINAS, Andrea y GONZÁLEZ, José Luis, Investigación Criminal, Primera Edición, Madrid, España, 2015, Editorial LID.

UNDOC, Oficina de las Naciones Unidas contra la droga y el delito, MANUAL DE INSTRUCCIONES PARA LA EVALUACIÓN DE LA JUSTICIA PENAL, Investigación de Delitos. Nueva York, 2010.

ACURIO DEL PINO, Santiago. Derecho Penal Informático, Segunda Edición 2017. https://www.academia.edu/33039698/Derecho_Penal_Inform%C3%A1tico_Segunda_Edici%C3%B3n_2017

PRINCIPIOS DE DEBIDO PROCESO, Centro de información Jurídica en línea, https://cijulenlinea.ucr.ac.cr/portal/descargar.php?q=MzAx

AGUDELO RAMÍREZ, Martín. El Debido Proceso, OPINIÓN JURÍDICA vol. 4, No. 7 pp. 89-105, https://dialnet.unirioja.es/descarga/articulo/5238000.pdf

CAFFERATA NORES, José I. La prueba en el proceso penal. Con especial referencia a la ley 23.984. 3ra. Edición. De Palma Ediciones. Buenos Aires. 1998, p. 33

ORTEGA GUTIÉRREZ, David. Sinopsis del Art. 24 de la Constitución Española. http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=24&tipo=2

LÓPEZ CABELLO, Fernando Alday. La regla de exclusión de la prueba ilícita en España, estudio comparado con la actualidad mexicana. http://hdl.handle.net/10803/659086.

MENESES PACHECO, Claudio. Revista Ius et Praxis, ISSN 0717-2877, Vol. 14, No. 2, 2008, págs. 43-86. https://dialnet.unirioja.es/servlet/articulo?codigo=3054272

CABALLERO, María Ángeles y CILLEROS SERRANO, Diego. El Libro del Hacker 2018. Ediciones ANAYA Multimedia, 2018, Madrid.

CANO M. Jeimy en Computación Forense: Descubriendo los Rastros Informáticos, Editorial ALFAOMEGA, Primera Edición, México, 2009, Pág. 10.

CASEY Eoghan, Handook of Computer Investigation, Elsevier Academia Press, 2005.

LOPEZ DELGADO, Miguel, Análisis Forense Digital, junio del 2007, CRIPORED.

REYES, Anthony, Investigación del Cibercrimen, Syngress 2007

CARRIÓ, Alejandro, Justicia Criminal, Citado por JAUCHEN, Eduardo, Tratado de la Prueba Material, Rubinzal-Culzoni Editores, 2000, pág. 614.

JAUCHEN, Eduardo, Tratado de la Prueba Material, Rubinzal-Culzoni Editores, 2000, pág. 615.

MARTÍNEZ RETENAGA, ASIER. Guía de toma de evidencias en entornos Windows, con la colaboración de Daniel Fírvida Pereira y Jesús Díaz Vico, Madrid, 2014. http://www.incibe.es

ARAZI, Roland. La Prueba en el Derecho Civil. Buenos Aires (Argentina): Ediciones La Roca, 1991, pp. 89 y s. Citado por Boris Barrios en Teoría de la Sana Crítica. Publicado en OPINIÓN JURÍDICA vol. 2, No. 3 pp. 99-132. http://www.academiadederecho.org/upload/biblio/contenidos/Teoria_de_la_sana_critica_Boris_Barrios.pdf

10.- Normas Legales

Constitución Española 1978, Edición conmemorativa del cuadragésimo aniversario. Cortes Generales, Dirección de Estudios, Análisis y Publicaciones, Floridablanca, 28071. Madrid

Ley de Enjuiciamiento Criminal, Legislación Consolidada BOE.

Ley de Enjuiciamiento Civil. https://www.boe.es/buscar/act.php?id=BOE-A-2000-323

Ley 59/2003, de 19 de diciembre, relacionada con la firma electrónica. https://www.boe.es/buscar/act.php?id=BOE-A-2003-23399