COLEGIO MEXICANO DE ESTUDIOS DE POSGRADO JURIDICOS Y ECONOMICOS A.C.

PROTOCOLO DE INVESTIGACION

ESPECIALIDAD EN CRIMINOLOGÍA

´´Estudio Comparativo de la Pérdida de Control de Datos Biométricos y Huellas Digitales en Redes Sociales en el Estado de Morelos´´

LIC. LYNDA CRYSTEL FLORES FLORES

INDICE

Introducción General

En la actualidad se asegura que las tecnologías de la información son útiles y beneficiosas en diversas áreas, ya que permite mejorar la organización profesional y personal, así como también encontrar un sin fin de literatura, de igual manera nos permite realizar programas para el fácil acotamiento de datos importantes, sin dejar atrás el uso de las redes sociales.

Es por ello que el mal uso de la tecnología atraído consigo la pérdida de control sobre nuestros datos biométricos, como son huellas dactilares, el iris de los ojos, las facciones del rostro, el tono de voz, las firmas y el ADN, de manera involuntaria, ya que se desconoce los filtros de seguridad con esos datos.

Mediante esto se abordara el planteamiento de una política pública como propuesta para asegurar el resguardo, el respeto y la protección de los derechos digitales contemplando de esta manera evitar ser víctima de delitos como la suplantación de identidad.

Con base a lo anterior, la suplantación de identidad puede tomar muchas formas y los términos legales difieren de un país a otro. En el estado de Morelos, el delito de suplantación de identidad se define dentro del Código Penal en su artículo 189-BIS, como: “Al que por cualquier medio suplante la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la suplantación de identidad causando con ello un daño o perjuicio u obteniendo un lucro indebido”, una vez teniendo en cuenta esto, se deduce que la suplantación de identidad sucede cuando usurpan medios electrónicos o informáticos manipulando la información sustraída, de tal manera que también suele darse mediante el uso sin autorización de datos identificativos.

Planteamiento del Problema

En la época de la digitalización, se requiere que la ley se adapte para amparar y proteger derechos fundamentales. Los derechos digitales, muy ligados a la libertad de expresión y la privacidad, son aquellos que permiten a las personas acceder, usar, crear y publicar medios digitales, así como acceder y utilizar ordenadores, otros dispositivos electrónicos y redes de comunicaciones. Las tecnologías digitales se están innovando y transformando la forma en que se ejercen, se protegen y se vulneran derechos básicos como la libertad de expresión y el acceso a la información

Derivado de lo anterior, resulta de gran importancia que se hagan valer los derechos digitales dentro de las tecnologías de la información, ya que actualmente hay una gran problemática al emplear o entregar nuestros datos personales, específicamente hablando de nuestros datos biométricos, esto porque se ha generado un punto de riesgo incrementado en lo que respecta a la accesibilidad y facilidad para obtener y recrear las huellas digitales de las personas.

Por lo que, al momento de denunciar todo tipo de delitos relacionados con la tecnología, nuestras autoridades muestran una pésima atención y orientación al momento de hacer una denuncia. En otras palabras, lo que se busca en esta investigación es proporcionar un taller o programa que capacite a las autoridades y ciudadanos para lograr un adecuado uso de la tecnología y datos biométricos para el respeto de los derechos digitales. Aunado a lo anterior es de vital importancia crear y aplicar políticas de prevención de este tipo de delitos.

Objetivos Generales:

Conocer e implementar el adecuado uso de datos biométricos en las tecnologías de la información para garantizar la protección de la identidad y de las huellas digitales a través de la implementación de un protocolo dentro de la tecnología de información para la enseñanza de un manejo responsable de datos biométricos en redes sociales.

Objetivos específicos

- Crear una propuesta que asegure el derecho a un sano control de datos biométricos de la identidad y huellas digitales en redes sociales.
- Promoción del adecuado uso de los datos biométricos para evitar ser víctima de suplantación de identidad.
- Lograr promover el conocimiento sobre el actuar de los derechos digitales.

Justificación de la Investigación

Desde hace poco hemos venido enfrentando una problemática grave con el uso inadecuado de las tecnologías de la información y facilidad para acceder a los medios masivos de información y las redes sociales y por lógica el fácil acceso a todo tipo de informaciones que van desde lo personal hasta lo institucional.

Es por ello que cuando un individuo sube alguna foto mostrando sus particularidades físicas como lunares, cicatrices, tatuajes, etc., son pieza clave para realizar una suplantación de identidad, pero cabe mencionar que también se puede falsificar las huellas dactilares por medio de hacer alguna seña particular en alguna foto.

Es necesario resaltar, que los denominados hackers son especialistas en realizar este tipo de falsificaciones, mediante el empleo de técnicas, estrategias y diversos métodos de estudio y análisis para coadyuvar mediante la informática y dactiloscopia sobre los casos en los que se traten de delitos como fraude, robo, suplantación de identidad y mediante ello realizar una pronta administración de justicia.

Delimitación de la Investigación

La presente investigación está dirigida para el estado de Morelos con la finalidad de establecer una óptica y análisis crítico para erradicar el riesgo, la pérdida de control y divulgación de datos biométricos y huellas digitales en redes sociales.

Hipótesis

La política pública de control con responsabilidad de datos biométricos y huellas digitales deberá, prever, conocer y garantizar que los encargados de las redes sociales respeten los derechos digitales a través de la correcta aplicación y métodos para la capacitación de los usuarios en las redes sociales.

El promover estos derechos servirá de apoyo en esta política que dará como resultado el respeto y protección de datos biométricos y huellas digitales dentro de las redes sociales, a fin de dar lugar a la correcta atención y orientación por parte de las autoridades al denunciar delitos relacionados con la tecnología y evitar ser víctima de dichos delitos. Esto implica a coadyuvar con diversas ciencias que forman parte de la Criminalística: dactiloscopia, informática forense, identificación humana y derecho penal.

Metodología de Investigación

En el primer capítulo la investigación a realizar será teórica e inductiva interpretando los hechos sucedidos. En el segundo capítulo se investigaran las generalidades que conforman los datos biométricos y redes sociales entorno a la informática forense.

En el tercer capítulo se pretende realizar un estudio experimental con el fin de establecer principios científicos mediante la comprobación de los cambios que han surgido con el uso de la tecnología. Finalmente en el cuarto capítulo analizaremos las legislaciones que protegen los derechos digitales.

Marco Teórico

Los derechos digitales son aquellos que permiten a las personas acceder, usar, crear y publicar medios digitales, así como acceder y utilizar ordenadores, otros dispositivos electrónicos y redes de comunicaciones.

Puesto que la defensa de los datos biométricos y huellas digitales, son considerados derechos de intimidad y privacidad, se llegó a la conclusión de que estos derechos implican la protección de los derechos fundamentales, ya que en tal sentido son esenciales, originarios, innatos, imprescriptibles e intransferibles. Sin embargo el cumplimiento de los datos biométricos y huellas digitales está ligado a la medida de que se respeten y cumplan los derechos de intimidad y privacidad.

Los derechos de intimidad y privacidad están previstos en los derechos fundamentales que ya están reconocidos internacionalmente.

En nuestro país las siguientes legislaciones protegen los derechos de la intimidad y privacidad:

- Constitución Política de los Estados Unidos mexicanos.
- Comisión Nacional de Derechos Humanos.
- Ley Federal de Protección de Datos Personales.
- Código Penal Federal
- Código Penal del Estado de Morelos.

CAPITULO PRIMERO

MARCO TEORICO DE LA DACTILOSCOPIA

¨Todo lo que nace proviene
Necesariamente de una causa,
Pues sin causa, nada
Puedes tener origen¨
Platón

SUMARIO.1.1.Introducción.1.2.Antecedentes de la Dactiloscopia.1.3.Precursores de la Dactiloscopia.1.4.Definiciones.1.5.Principios de la Dactiloscopia.1.6.Tipos de Huellas Dactilares.1.7.Elementos de estudio para Identificar una Huella Dactilar.1.8.Función del perito en Dactiloscopia.1.9.Conclusión.

1.1. Introducción

El presente capitulo tiene como finalidad recorrer los sucesos históricos que han sido de vital importancia para la creación del estudio de las impresiones de los dibujos de las crestas papilares de las yemas de los dedos de las manos, denominado Dactiloscopia, así como atraer y desglosar los conceptos principales que encaminaran la problemática que se está viviendo con la pérdida de control involuntaria de nuestros datos biométricos y huellas dactilares. Por lo que se pretende dar seguimiento que los derechos digitales se cumpla.

1.2. Antecedentes de la Dactiloscopia.

Con respecto a lo antes expuesto, se tiene que el primer antecedente de la Dactiloscopia surge con los chinos, ya que a su cultura se le conoce por haber utilizado impresiones de crestas de fricción como medio de identificación. El primer ejemplo proviene de un documento chino que se titula ¨The Volumen of Crime Scene Investigation- Burglary¨, de la dinastía Qin, que surge en el año 221-206 a.C. El documento contiene una descripción de cómo se utilizaron las huellas de las manos como un tipo de evidencia[1]. La dinastía Qin fue una de las primeras en establecer el uso de impresiones de crestas de fricción en piel como medio de identificación.

Durante los Qin a través de las dinastías Han del este, en el año 221 a.C. a 220 d.C. el ejemplo más frecuente de la individualización mediante crestas de fricción fue el sello de la arcilla[2], estos documentos consisten en trozos o páginas de bambú que se enrollaron con fijaciones de cuerda, y las cuerdas fueron selladas con arcilla. Aun lado de la junta estaría impresionado el nombre del autor, por lo general en la forma de sello, y por otro lado la impresión de la huella dactilar del autor. El sello se utilizó para mostrar la autoría y evitar la manipulación previa a que el documento llegara al lector destinado. Es por ello que generalmente se reconocía que era tanto la huella dactilar como el nombre lo que le dio autenticidad al documento. Mediante este documento, la impresión de la huella dactilar en el sello de la arcilla, se convirtió en un ejemplo definitivo de la reproducción intencional de crestas de fricción en piel antes de la era cristiana.

Es importante mencionar, que con la invención china del papel en el año 105 d.C. se hizo común firmar los documentos utilizando las crestas de fricción dactilares, ya que esto se había vuelto una práctica habitual en China para colocar una impresión, ya sea las marcas de las palmas o falanges o bien las huellas dactilares en todos los documentos de tipos contrato.

---

[1] Laud H, John. Libro de Referencia de las Huellas Dactilares. Departamento de Justicia de los Estados Unidos. https://www.ojp.gov/pdffiles1/nij/249575.pdf. Washington, DC. p.4.
[2] Ibid.p.4.

En el año 650 d.C. el historiador chino Kia Kung Yen[3] describe un medio de identificación o escritura utilizado previamente, como son las tablas de madera que eran inscritas con los términos del contrato y las muescas se cortaban por lados en los mismo lugares, de tal forma que las tabletas podían emparejarse después demostrando su genuinidad, con ello la importancia de las muescas era la misma que la de las huellas dactilares actualmente.

Mediante esta explicación, es importante mencionar que la cultura china utilizaba las huellas dactilares para individualizar. Ahora bien el uso de las impresiones de piel con crestas de fricción en China continúo en la dinastía Tang, en el año 617 a 907 d.C[4]. como se podía apreciar en los contratos inmobiliarios, testamentos y listados del ejército. Se puede postular que con los chinos usando las crestas de fricción de la piel para la individualización y el comercio con otras naciones de Asia, estos otros países pudieron haber adoptado la práctica. Por otro lado, en Japón se promulgo una ley interna, la cual surgió en el año 702 d.C. según la cual expresaba lo siguiente; ¨En caso de que un esposo no pudiera escribir, le permitían contratar a otro hombre para que escribiera el documento y después del nombre del esposo, firmara con su propio dedo índice¨[5]. Con lo ya expuesto, esto hace pensar que los japoneses tenían cierta comprensión del valor de las crestas de fricción en la piel para la individualización. Es así que en la India hay referencias en cuanto a la nobleza utilizando las crestas de fricción de la piel como firmas, un ejemplo de ello esta;

En el año 1637 d.C. las fuerzas conjuntas de Shah Jahan y Adil Khan, bajo el mando de Khan Zaman Bahadur, invadieron el campamento de Shahuji Bhosle, gobernante de Pona (Maharashtra en la actualidad) el ejercito conjunto derroto a Shahuji, quien fue obligado a aceptar los términos de la paz; ya que la guarnición de Shahuji se había reducido a medidas extremas, Shahuji escribía con frecuencia para Khan Bahadur en el más humilde esfuerzo, jurando lealtad a la corona; y al mismo tiempo solicito un tratado por escrito estampado con la impresión de la mano.

---

[3] Laud H, John. Op. Cit.p.4
[4] Ibid.p.5.
[5] Idem.

Sin embargo el párrafo anterior es un ejemplo del uso de impresiones de la palma de la mano por parte de la nobleza en la India para demostrar la autenticidad de la autoría al escribir un documento importante, es decir que se cree que el uso de las impresiones en documentos importantes fue adoptado por los chinos, donde se utilizaba normalmente mientras que en la India, el uso de estas impresiones era principalmente reservado para la realeza.

En particular el uso de crestas de fricción de piel como firma en China, Japón, India y posiblemente otras naciones antes de descubrimiento europeo está bien documentado.

1.3. Precursores de la Dactiloscopia.

A finales del siglo XVII, los científicos europeos empezaron a publicar sus observaciones a cerca de la piel humana. Por otro lado las crestas de fricción de la piel fueron descritas por primera vez en detalle por el Dr. Nehemiah Grew en el año 1684 con el documento ¨ Phylosophical Transactions of the Royal Society of London¨[6], cuya descripción marco el inicio en el Hemisferio Occidental en las observaciones y caracterizaciones de crestas de fricción en piel. En el año de 1685, el anatomista holandés Govard Bidloo, publico el documento ¨ Anatomy of the Human Body¨, el cual expresaba los detalles de la piel y las crestas papilares del pulgar, pero de igual manera este documento no abordaba la individualización o permanencia de las mismas.

El estudio científico de las huellas dactilares despego después de la edad Moderna, cuando en el año de 1687, el filósofo italiano Marcello Malpighi publico el escrito ¨Concerning the External Tactile Organs¨, donde abordada temas como la función, forma y estructura de las crestas de fricción en piel.

Por lo contrario a Malpighi se le atribuye ser el primero en utilizar el microscopio recién inventado para estudios médicos, esto con el fin de señalar en su tratado que la piel surcada aumenta la fricción entre un objeto y la superficie de la piel, así la cresta de fricción de la piel mejora la tracción para caminar y sujetar.

---

[6] Laud H, John. Op. Cit.p. 1-5.

En reconocimiento al trabajo de Malpighi, una capa de piel fue nombrada como él y fue considerado como el abuelo de la dactiloscopia[7].

En cuanto al año 1788 el médico y anatomista alemán Johann Cristoph Andreas Mayer, escribió el libro titulado ¨Anatomical Copper- plates with Appropiate Explaniations¨, el cual contenía los planos detallados de los patrones de las crestas de fricción en piel, en donde Mayer escribió que ¨Aunque la disposición de las crestas de la piel nunca se duplica en dos personas, las similitudes son más cercanas entre algunos individuos. Entre otros, las diferencias están marcadas, pero a pesar de las peculiaridades de la disposición, todos tienen una cierta semejanza¨. A lo cual a Mayer se le atribuye como el primero en escribir que las crestas de fricción de la piel son únicas[8].

A principios del siglo XIX, Thomas Bewick quien fue un grabador en madera y ornitólogo inglés, publico muchos libros con grabados en madera de aves y otros animales, de los cuales tres grabados realizados en los años 1809, 1818 y 1826 incluían una huella dactilar, y los dos últimos tenían la leyenda siguiente; ¨ Thomas Bewick, su marca¨. Es importante mencionar que los grabados en madera eran muy detallados, pero se desconoce si Bewick entendía el valor de las crestas de fricción en piel para la individualización. Por otra parte, en el año de 1823 el Dr. Johannes Purkinje, quien fue Profesor en la universidad de Breslau en Alemania, clasifico dentro de su tesis titulada ¨Commentary on the Physiological Examination of the Organs of Vision and the Cutaneous System¨, los patrones de huellas dactilares en nueve categorías y dio a cada uno un nombre, sin embargo aunque el Dr. Purkinje no fue más allá de nombrar a los patrones, su contribución es importante porque sus nueve tipos de patrones fueron pioneros del sistema de clasificación de Henry.

Es por ello que Purkinje es considerado como el padre de la dactiloscopia[9] y es mediante este primer sistema dactiloscópico que pasó sin pena ni gloria entre sus contemporáneos, y no fue hasta unas décadas más tarde cuando se empezó a aplicar en el campo de la criminalística.

---

[7] Caballero Delgado, Samuel Alfonso. Dactiloscopia Certeza o Incertidumbre. Editorial Ltda. Colombia. 2009. p.32.
[8] Laud H, John. Op. Cit.p.6.
[9] Caballero Delgado, Samuel Alfonso. Op.Cit. p.33.

Ahora bien, el antropólogo alemán Herman Welcker, marco el camino para el estudio de la permanencia de crestas de fricción en la piel, es decir, que comenzó imprimiendo su mano derecha en el año de 1856 y nuevamente en el año de 1897, por lo tanto obtuvo el crédito como la primera persona en iniciar un estudio de permanencia, sin embargo dicho antropólogo solo buscaba ofrecer asistencias a las reclamaciones previas en relación con la permanencia de las crestas de fricción, debido a esto Welcker no excitado a menudo por realizar dichas impresiones ya que él no buscaba crédito alguno, en general el crédito por ser la primera persona en estudiar la persistencia de las crestas de fricción de la piel se le otorga a Sir William James Herschel[10].

Es necesario mencionar que, Sir William James Herschel fue Jefe de distrito del servicio civil del distrito de Hooghly, Bengala, India, y en el año de 1858 apoyándose de la clasificación de los tipos dactiloscópicos realizados por el Dr. Purkinje, fue el primero en utilizar las huellas dactilares con fines de identificación, implementando la toma de impresiones dactilares en documentos contractuales y en servicios de pensiones, fue gracias a este procedimiento que se evitaron cuantiosas pérdidas al estado, descubriendo así a las personas que pretendían cobrar dos o más veces su propia pensión habiendo de igual manera casos de suplantación. Asimismo Herschel comenzó a emplear las impresiones dactilares registro de identificación de indígenas analfabetos y es en el año de 1877 que propone la toma en los registros carcelarios, a lo cual Herschel concluyo que las huellas dactilares eran distintas en todos los individuos, demostrando así con sus propias huellas con una diferencia de 28 años que no cambian, descubriendo de esta manera su inmutabilidad y la perennidad de las mismas[11]. En cambio dentro del mismo año Thomas Taylor quien fue un microscopista del departamento de agricultura de los Estados Unidos, dio una conferencia en relación con la delincuencia, en donde se exponía la idea de utilizar huellas de sangre encontradas en escenas del crimen como un medio para identificar a los sospechosos, dicha conferencia fue publicada en la edición de julio de 1877, titulada ¨ The American Journal of Microscopy and Popular Science¨.

[10] Laud H, John. Op. Cit. p. 7.
[11] Caballero Delgado, Samuel Alfonso. Op. Cit.p. 34.

No obstante, el medico escoses Henry Faulds abrió un hospital de Tsukiji, Japón y trabajo allí de 1873 a 1885, durante su estadía en Tokio, Japón descubrió que las huellas dactilares permiten dejar huellas invisibles o latentes, gracias a la transferencia del sudor emanado por las glándulas sudoríparas y por la contaminación de grasa de las glándulas sebáceas, por el simple contacto directo en cualquier superficie, diseñando técnicas para su revelado y recolección que permanecen vigentes. Es por ello que fue el primero en aplicar y promover la toma de las diez impresiones dactilares, en una ficha que denomino tarjeta decadactilar, cabe mencionar que Faulds recopilo abundante material dactiloscópico, estudiando la diversidad de formas, con fines genéticos de la herencia y etnológico, pero que destino para el estudio de la identificación humana, publicando a su vez en la prestigiosa revista científica Nature el 28 de Octubre de 1880 en el ¨ que se destaca la importancia de recoger huellas dactilares en el lugar de los hechos, para identificar al delincuente¨, gracias a este articulo Juan Vucetich en el año de 1892, logro resolver el homicidio de los hijos Francisca Rojas. Por lo tanto, Faulds logro que Scotland Yard implementara la toma de impresiones dactilares en sus investigaciones forenses, es importante destacar que entre Herschel y Faulds siempre existió una rivalidad por atribuirse el descubrimiento de las huellas dactilares como medio de identificación[12].

Con respecto a Sir Francis Galton, fue un célebre antropólogo inglés, sobrino del naturalista Darwin, quien continuo con los estudios preliminares sobre las huellas dactilares, reconfirmando los principios descubiertos por Herschel y Faulds sobre la inmutabilidad y perennidad, demostrando de manera científica la unicidad de las huellas dactilares no regida por factores hereditarios, sanguíneos, ni familiares, sino más bien identificando las peculiaridades macroscópicas de las crestas papilares, con su respectivo nombre, por ello se le llaman puntos Galton.

[12] Laud H, John. Op.Cit. p. 7-8.

Cabe mencionar que Galton clasifica las impresiones dactilares por los deltas y núcleos en tres tipos así[13];

- Sin núcleos, ni deltas (arcos).
- Con núcleo y un delta (lazos).
- De dos o más deltas, con uno o más núcleos (verticilos).

Posterior a esto, en el año 1892 Galton publico el best seller ¨ The Fingersprints¨, en el cual plasmo todo su conocimiento, siendo este la base de los métodos de clasificación que surgieron años más tarde, su libro se considera un best seller de las ciencias forenses con el primer glosario técnico de las huellas dactilares, después de publicar su libro Galton, inicio con la creación de una campaña en su país, para que se le atribuyera a las huellas dactilares el reconocimiento como método fehaciente para la identificación humana con valor probatorio en el proceso penal y civil. Mediante esto soporto grandes debates y oposiciones que no creían en el carácter único y universal de las huellas dactilares, luego de años de lucha, Galton consiguió que las huellas dactilares fueran reconocidas como un método de identificación plena de los seres humanos, es así que a Galton se le atribuye el más alto nivel de importancia como gestor y promotor de las huellas dactilares.

En el año de 1879, Alphonse Bertillon siendo un empleado de la prefectura de policía de Paris, Francia comenzó a estudiar las medidas corporales de varios individuos y trazo la antropometría, la cual se empezó a utilizar en el año de 1882. Es decir, que la antropometría es el estudio de las medidas del cuerpo con fines de identificación, a lo cual el método antropométrico de Bertillon media la altura, alcance, tronco, longitud de la cabeza, ancho de la cabeza, longitud de la oreja derecha, ancho de la oreja derecha, longitud del pie izquierdo, longitud del dedo medio izquierdo, longitud del meñique izquierdo y la longitud del ante brazo izquierdo.

[13] Caballero Delgado, Samuel Alfonso. Op.Cit.p.36-37.

Debido al éxito de la antropometría, Bertillon fue promovido a Jefe del departamento de identidad judicial en 1888. Por el contrario la antropometría es una manera científica y biométrica de individualizar, y fue utilizada en los delincuentes en casi todo el mundo desde su introducción en 1882 y hasta 1914. Mientras tanto la identificación con crestas de fricción dactilares se hizo más prevalente tras la experimentación que mostraba su utilidad, se añadieron las huellas dactilares a los registros antropométricos. Por lo tanto, un registro antropométrico completo incluiría 11 medidas del cuerpo, 2 fotografías (cara de frente y lateral derecho), y un conjunto de las 10 huellas dactilares. A pesar de que no se había adoptado oficialmente como único medio de identificación en Francia o en otros lugares de Europa, el concepto de utilizar las crestas de fricción en piel para la individualización fue ganando fuerza[14].

Conforme a lo ya expuesto con algunos de los precursores, es importante mencionar que muchos de ellos siguen haciendo referencia al estudio de las crestas de fricción en la piel, por lo que uno de ellos es el Dr. Arthur Kollmann quien realizó el estudio del desarrollo embriológico de las crestas de fricción en la piel, proponiendo a su vez en el año de 1883 que las crestas se forman por la presión lateral entre crestas nacientes y que las crestas son discernibles en el cuarto mes de vida fetal y están completamente formadas en el sexto mes. Es por ello que Kollman fue el primero en identificar la presencia y ubicación de las almohadillas palmares de las manos y los pies[15].

Por otro lado en el año de 1886, Isaiah West Taber, un fotógrafo de San Francisco propuso la utilización de huellas dactilares para identificar a inmigrantes chinos, luego de ello en el año de 1889, el Director General de las Oficinas de Correos en India coleccionaba huellas dactilares de los empleados para evitar que las personas que habían sido despedidas fueran recontratadas, mediante esto el uso de huellas dactilares para la identidad funcionó bien para evitar prácticas fraudulentas, así mismo el científico médico legal francés René Forgeot publicó una tesis en 1891 en la que propuso el uso de polvos y productos químicos para desarrollar huellas ocultas en escenas de crimen con el fin de individualizar a la persona que había tocado un objeto.

[14] Ibid.p. 38.
[15] Laud H, John. Op.Cit.p.9.

Tomando como guía las investigaciones de Galton, Juan Vucetich empezó a experimentar con huellas dactilares en el año de 1891, comenzó a registrar las huellas dactilares de delincuentes y diseño su propio sistema de clasificación, se actualizaba constantemente leyendo revistas científicas, así como también el artículo de Henry Faulds, implementando de tal manera la toma de las diez impresiones dactilares al registro antropométrico de delincuentes, reduciendo al mínimo el sistema antropométrico dejando solo lo básico de información que contienen las actuales reseñas judiciales.

Posteriormente lee los estudios de Francis Galton publicados en el año de 1892 e inicia una amplia investigación para resolver los inconvenientes que tenía el sistema de Galton, de tal manera que logro simplificarlo y mejorarlo en un sistema decadactilar que permitía archivar y ubicar rápidamente las tarjetas decadactilares, sin tener en cuenta los nombres y apellidos, solo basado en la formula Dactiloscópica, donde pudo clasificar los dibujos dactilares en cuatro tipos fundamentales que llamo; Arco, Presilla Interna, Presilla externa y Verticilo[16].

Luego de haber pasado ocho años de logros y verificaciones, se le otorgo el merecido reconocimiento, publicando su método en el año de 1900. En el año de 1894, colaboro con Galton en un método de clasificación de las huellas dactilares, es decir que con la ayuda de los agentes de policía de la India Khan Bahadur Azizul Haque y Rai Bahaden Hem Chandra Bose, se desarrolló el sistema de clasificación Henry.

Una vez que el sistema de clasificación fue desarrollado y mostró ser eficaz, Henry escribió al gobierno de India pidiendo una revisión comparativa de la antropometría y las huellas dactilares. Charles Strahan, Topógrafo General de la India, y el químico Alexander Pedler fueron enviados a Bengala para reunirse con Henry e investigar los dos métodos de identificación.

[16] Caballero Delgado, Samuel Alfonso. Op.Cit.p. 43.

Hacia finales de marzo de 1897, enviaron un informe al Gobierno de India que declaraba: En conclusión, somos de la opinión de que el método de identificación mediante huellas dactilares, como funcionó en el sistema de grabación de impresiones y de clasificación utilizados en Bengala, puede ser adoptado de manera segura como superior al método de antropometría en la sencillez del trabajo, en el costo del aparato, en el hecho de que todo el trabajo calificado se desplaza a una oficina central o de clasificación, en la rapidez con que el proceso puede ser trabajado y en la certeza de los resultados.

Aunque en 1897, el gobierno de India sancionó el uso exclusivo de huellas dactilares como medio de identificación para internos.

Finalmente es importante hacer mención de un precursor que fue médico francés y a su vez fue considerado como el padre de la criminalística moderna Edmund Locard, quien realizo investigaciones, tratados y bases científicas de diversas áreas como balística, dactiloscopia, medicina, grafología, y documentoscopia.

En el año de 1912, fue nombrado como padre de la Poroscopia y en el año de 1914 da a conocer que el número ideal de minucias o puntos localizados en una impresión dactilar debe de ser doce y como mínimo ocho características, al igual que en las huellas dactilares, Locard considero un número mínimo de poros para la identificación, estableciendo que cuarenta es el numero legal para establecer la individualidad. Por lo tanto si el número de puntos característicos seria ocho, por consiguiente por cada punto como mínimo serían cinco poros arrojando el total anteriormente considerado de cuarenta poros. Locard fue el primero en aplicar el análisis microscópico al estudio de las huellas dactilares y en demostrar que las huellas e impresiones dactilares falsas, se diferencian de las plasmadas comprendiendo los beneficios del uso del microscopio en el campo forense[17].

[17] Ibid.p. 44-45.

En definitiva es importante conocer cada una de las aportaciones de los precursores de la dactiloscopia, para poder así dar continuidad al estudio de las huellas dactilares y particularidades, es decir, que cada elemento que compone nuestra huella dactilar es importante para su estudio e individualización de la misma, para saber diferenciar a una persona de otra.

1.4. Definiciones

Como ya se mencionó en el capítulo anterior, el precursor Juan Vucetich también padre de la Dactiloscopia, designo con un solo nombre dicha ciencia el cual era ¨Icnofalangometrial¨ qué significa estudio de las impresiones digitales, pero el doctor Francisco Latzinia, proclamo que con una palabra más corta y también de origen griego se podía nombrar a esta ciencia con el uso de la palabra Dactiloscopia, que se compone de dos vocablos griegos Daktilos que significa dedos y Skopein que significa examen o estudio[18]. Mediante esto puede definirse a la Dactiloscopia como el procedimiento técnico que tiene por objeto el estudio y clasificación de los dibujos digitales con el fin de identificar a las personas distinguiéndolas unas de otras.[19]

Por ende a estos dibujos dactilares o bien digitales se les denomina dactilogramas, que quiere decir escritura de los dedos, nombre que procede de dos vocablos griegos Daktilos (dedos) y grammas (escrito). A su vez, los dactilogramas se dividen en naturales y artificiales, es decir, que son naturales aquellos que se observan en las yemas de los dedos, y son artificiales los que se obtienen al imprimirlos previo al entintado, sobre papel o cualquier otra superficie, quedan reproducidos como si fueran producto de la reproducción de un sello.

Cabe mencionar que los dactilogramas artificiales toman el nombre genérico de impresiones papilares, porque son las rugosidades de la epidermis, quienes las originan y se particularizan con el nombre de la región que las produce, estas a su vez se denominan dactilares si proceden de los dedos de la mano, plantares si pertenecen a la planta del pie, y palmares cuando provienen de la palma de la mano.

---

[18] Criminalística y más. http://criminalisticaymasifil2.blogspot.com/p/escribir-el-nombre-del-autor.html. 08/03/2021. 4:32 pm.

[19] Trujillo Arriaga, Salvador. El Estudio Cientifico de la Dactiloscopia. LIMUSA. México. 2000. p.21.

Sin embargo, cuando dejamos impresiones o huellas dactilares dejadas por las sustancias excreción de los poros en cualquier superficie que se toque, se le denomina dactilograma latente, en cambio cuando una huella o imagen se encuentra en una superficie de consistencia blanda, como son la plastilina, barro, jabón, yeso, se le denomina dactilograma moldeado.

Cuando se emplean términos como Presilla interna y Presilla externa, se definen de tal manera que; la Presilla interna es aquella cuyo núcleo está formado por crestas que forman gazas y que en su recorrido dichas crestas salen a la izquierda del observador, en el caso de la Presilla externa, el recorrido de sus crestas es a la derecha del que observa. Es importante mencionar que el diccionario de la lengua española define la palabra verticilo como un conjunto de ramos, hojas o flores situados alrededor de un punto del tallo, pese a lo anterior en cuanto a la variedad de dibujos que presentan estas figuras en nuestros dedos es lo que dio como resultado el designarlas con este nombre.

En cambio existen otros términos, que son relevantes de igual manera para el estudio de las huellas dactilares, como son la formula y subformula decadactilares, los cuales se representan por medio de un conjunto de letras y números, es decir, que los números se representan en forma de quebrados en los cuales el numerador indica los tipos fundamentales y el denominador el número de crestas delto- centrales.

Sin embargo, la subfórmula de los verticilos se manifiesta con la palabra de introdelto que indica interior, mesodelto que significa medio y extrodelto que quiere decir exterior[20].

Tomando como referencia los términos empleados en dactiloscopia, a cerca del estudio de las huellas dactilares y crestas papilares, es importante destacar que la dactiloscopia es una ciencia de aplicación que esta cimentada en una verdad absoluta, una base filosófica y esta a su vez conforma un fin jurídico y social.

[20] Ibid.p.22.

Así mismo el doctor Luis Reyna Almandos se expresa con respecto a la dactiloscopia de la siguiente manera;¨Es la única rama del derecho que descansa en un fundamento matemático y la teoría de la Perennidad, inmutabilidad y diversidad de las líneas dactilares ha llegado a ser después de largos estudios, una verdad indestructible a la hora de su aplicación¨[21].

Conforme ha pasado el tiempo, hemos entendido que el fenómeno de la dactiloscopia, ha sido de vital importancia para individualizar a un individuo de otro, pero lejos de individualizar, se ha estudiado y comprobado que cada huella y crestas son únicas, por lo tanto es difícil llegar a alterar o falsificar una huella, por ende es importante realizar una investigación minuciosa en el lugar de intervención, ya que nos podemos encontrar con las huellas dactilares impresas en alguna superficie de un delincuente o víctima, es por ello que la dactiloscopia, es una ciencia trascendental en la administración de justicia de nuestro país.

Además podemos decir que de la dactiloscopia se han ido desglosando diversas ciencias como la Palametoscopia, la cual se encarga del estudio de las palmas de las manos, y se aplica en delincuentes reincidentes, de tal manera que se usa también para la identificación de recién nacidos, por otro lado la Pelmatoscopia, se encarga del estudio de las impresiones plantares, finalizan así con la Poroscopia, que se encarga del estudio de los orificios o poros de las glándulas sudoríparas, los cuales podemos identificarlos como puntos blancos en las crestas[22].

1.5. Principios de la Dactiloscopia.

Toda vez que las huellas dactilares son totalmente individualizadas, únicas en cada persona, ningún ser humano hasta nuestros días ha coincidido con las huellas dactilares de otra persona, ante tales evidencias es indudable que un método aprovechable de fácil acceso, económico y con alguien que haya aplicado adecuadamente el método o técnica para la obtención de huellas dactilares, podrá tener la certeza de la identificación plena de un individuo vivo o muerto.

---

[21] Criminalística y más. Op.Cit.

[2222] Vargas Alvarado, Eduardo. Medicina Legal. Trillas. México.2017.p.90.

Derivado de dichas bases surge el estudio de lo que comúnmente se denomina huella dactilar, pero dogmáticamente es importante referir que la piel humana está compuesta por dos capas, en una de ellas, la dermis (capa interna), específicamente en las zonas de fricción (palmas de dedos, manos y planta de pies), se forman estructuras cónicas llamadas papilas, que se caracterizan por líneas (crestas) y espacios (surcos); al dibujo que arroja la suma de crestas y surcos papilares se le denomina lofogramas. Existen lofogramas de los dedos de las manos (dactilogramas), de las palmas de las manos (quirogramas) y de las plantas de los pies (pelmatogramas).

Los principios en que se sustenta la dactiloscopia se resumen en[23]:

- Perennidad; Se basa en el indudable hecho de que las huellas dactilares se forman en el sexto mes de la vida intrauterina, siendo perennes desde ese momento y hasta la descomposición del cadáver en que viene la desintegración. Los dibujos formados por las crestas papilares persisten miles de años en estado de momificación, quienes demostraron esto fueron los precursores Forgeot y Vucetich al examinar momias egipcias y americanas respectivamente.

- Inmutabilidad; Se apoya en el innegable hecho de que las crestas papilares no pueden modificarse voluntaria ni patológicamente, pues hasta las lesiones, quemaduras, y desgastes profesionales o intencionales que sufra una persona, se reproducen completamente siempre que no haya sido destruida profundamente la dermis.

- Diversidad; Por la diversidad de formas que tienes estos dibujos papilares, cada dibujo tiene características únicas e irrepetibles, no existen dos dibujos exactamente iguales, es decir, hablamos de la individualidad de la huella, luego, la identidad personal.

---

[23] Camacho Vaca, Arturo. Certeza de la Dactiloscopia. https://revista.cleu.edu.mx/new/descargas/1904/Articulo08_certeza-de-la-dactiloscopia.pdf. 08/03/2021. 5:27 pm.

1.6. Características de las Huellas Dactilares.

Para hacer mejor comprensión de los términos ya mencionados en los anteriores apartados, es necesario analizar que cada huella dactilar se conforma de diversas características básicas para un adecuado estudio de las mismas, las cuales son[24];

- Zona del Dibujo; Es la única parte de la impresión dactilar que nos interesa con respecto a la interpretación y clasificación. Lógicamente, va estar presente en todos los dibujos, pero en muchos arcos y a su vez arcos en tienda resulta imposible de definir, pero esto no es realmente importante, dado que los únicos dibujos que precisamos para la clasificación son las presillas y los verticilos. En estos dos casos la zona del dibujo puede ser definida así: La Zona del Dibujo, es aquella parte de la presilla o de un verticilo en la que aparecen los núcleos, deltas, y crestas que nos interesan para la clasificación. La zona del dibujo de las presillas y verticilos cerradas o limitadas por las líneas directrices.

- Las líneas directrices; Pueden ser definidas como las dos crestas más exteriores que comienzan paralelas, se desvían y rodean o tienden a rodear la zona del dibujo. Las líneas directrices, no son siempre dos crestas continuas, en realidad con mucha frecuencia se ve que están cortadas o interrumpidas, cuando en una línea directriz hay una interrupción o corte definitivo, se considera la cresta exterior inmediata como su continuación. Al ubicar las líneas directrices necesario tener presente la distinción entre una divergencia y una bifurcación.

- Bifurcación; Son en realidad una sola cresta que se separa formando dos.

- Divergentes: Son crestas que corren paralelas y súbitamente se separan.

- Convergentes: Es la que saliendo de un punto de la cresta se detiene y abruptamente regresa al punto de partida.

---

[24] Dactiloscopia. http://dactiloscopia-quijada.blogspot.com/p/introduccion.html. 08/03/2021. 05:40 pm.

- Delta: Es considerado como tal debido a que es la primera cresta o parte de cresta que está más cercana del punto de divergencia de las dos líneas directrices.
- Núcleo: Tal como indica su nombre, es el centro aproximado del dactilograma.
- Cuenta de crestas: Es lo que se hace del delta al núcleo en una presilla.
- Trazo o recorrido: Es el punto de partida del delta a uno que se encuentra al lado izquierdo de cada huella, para llegar al delta dos.

1.7 Tipos de Huellas Dactilares

A lo largo de este capítulo hemos estado haciendo mención de que las huellas dactilares, se toman desde el nacimiento, para identificarnos por el resto de nuestra vida. Afortunadamente, no hay dos huellas dactilares iguales, ya que cada una de las yemas de los dedos tiene un patrón único que nunca cambiara, un ejemplo de esto son las personas o individuos que son gemelos idénticos con el ADN compartido, las huellas de ellos serán siempre diferentes.

Es por ello que tres patrones de huellas dactilares son la multitud de combinaciones presentes en todos los seres humanos, lo que hace que sea más notable que todo el mundo tenga un patrón diferente, lo que esto con lleva a que aprender de estos patrones nos ayudara a entender y analizar las técnicas básicas de identificación. Sin embargo, como ya anteriormente mencionamos, cada huella dactilar consta de crestas, líneas o deltas.

Estos identificadores se unen para crear patrones específicos, para distinguir un patrón debemos primero entender los identificadores; una cresta es una serie de líneas que atraviesa la impresión horizontal y la cima se observa en los bordes de la huella digital, mediante esto, los expertos llaman a una línea continua que forma una cresta a una línea divergente, mientras que la línea después de un descanso se llama una continuación.

Un delta es una línea que gira hacia arriba o hacia adentro. Muchos deltas se encuentran en el punto exterior de las crestas y comprenden el punto donde una cresta triangular irradia a cabo en tres direcciones.

De la siguiente manera, podremos identificar los patrones[25];

- Patrón de Arco; Los patrones de arco tienen líneas que empiezan en un lado de la huella, van hacia el centro y salen del otro lado de la huella. Existen dos tipos de arcos, como son; Arcos simples, en donde en este tipo de configuración, las crestas entran por un lado y corren hacia el lado opuesto, formando una pequeña o el levantamiento en el centro, esta configuración debe llenar no más de uno de los cuatro requisitos de las presillas; sin crestas recurvantes, sin formación angular y sin levantamiento abrupto. Por otro lado, están los arcos pirámides, los cuales son una variación de los arcos simples, pero las configuraciones formadas por sus crestas no son tan sencillas como las de los arcos simples.

  La semejan zaque a veces existe entre un arco pirámide y una presilla es tanta, que hay que tener gran cuidado al examinarlos a fin de no confundirlos.
- Patrones de Lazo; Los patrones de recodo tienen líneas que empiezan en un lado de la huella, van aumentando hacia el centro, se regresan y salen del mismo lado en que empezaron.
- Patrón Compuesto; Consiste en dos formaciones distintas del lazo con dos separaciones y los hombros distintos y dos deltas.
- Patrón espiral: Los patrones en forma de espiral tienen muchos círculos que no se salen de cualquier lado de la huella.

[25] Hope Davis, Spencer. Tipos de Patrones en la Identificación por Huellas Dactilares. https://www.geniolandia.com/13176324/tipos-de-patrones-en-la-identificacion-por-huellas-dactilares. 08/03/2021. 05:50 pm.

1.8. Función del Perito en Dactiloscopia

El perito en dactiloscopia se dedica al estudio del dibujo papilar de la yema de los dedos con fines de verificar la identificación humana, estos estudios se realizan en personas vivas como en cadáveres. Así mismo esta especialidad está relacionada a la criminalística, es por ello que los peritos en dactiloscopia se dedican a la búsqueda y revelado de huellas dactilares en un lugar de intervención. En la actualidad el campo de trabajo del experto en dactiloscopia es amplio, ya que en el país existe una institución dedicada al registro civil de personas donde se requiere especialistas para las codificaciones de las impresiones dactilares en las cedulas de identidad.

Por otro lado en el campo de la criminalística, el que comete un delito utiliza las manos y puede dejar huellas dactilares en el lugar de intervención o escena del crimen, por tanto, se requiere de expertos en la materia para el revelado de huellas dactilares, es decir, que el perito en dactiloscopia es fundamental para el proceso de identificación de cadáveres[26].

1.9. Conclusión.

En definitiva es importante resaltar que nuestras huellas dactilares son únicas e intransferibles, a lo cual esto hace que sea más fácil nuestra identificación por cualquier medio tecnológico y a través de una base de datos. Es por ello que es importante cuidar nuestras huellas dactilares, ya que son nuestro medio de identificación y que por tanto somos susceptibles a ser víctimas de robo o suplantación de identidad por medio de la sustracción de nuestras huellas dactilares y datos biométricos.

[26] Gómez Bernal, Eduardo. Tópicos Médicos Forense. SISTA. México. 2017.p. 473.

CAPITULO SEGUNDO

LA INFORMATICA FORENSE Y SUS ELEMENTOS

SUMARIO 2.1.Introducción 2.2.Antecedentes y Precursor de la Informatica Forense 2.3.Concepto, Objetivo y usos de la Informática Forense 2.4.Analisis Forense 2.5.Caracteristicas de las Tecnologías de la Información 2.6.Definición de Hackers 2.7. Técnicas de Hacking 2.8.Falsificación de la Información conforme redes sociales 2.9.Clasificación de Huellas Digitales 2.10.Conclusión.

2.1. Introducción

El presente Capitulo como lo indica el titulo tiene como finalidad averiguar sobre la procedencia de la informática forense, así como también dilucidar sobre los conceptos y elementos que conforman a dicha ciencia. Con base a esto se pretende confrontar la problemática que se vive con respecto a la pérdida de control de datos biométricos y huellas digitales en redes sociales, conociendo de tal manera las causas y efectos que ha traído la falsificación de la información conforme a las tecnologías de la información, al mismo tiempo que se dará seguimiento a la resolución a través de un mecanismo adecuado.

2.2. Antecedentes y Precursor de la Informática Forense

Con respecto a la Informática Forense es preciso conocer las causas que dieron origen a la creación de dicha ciencia, la cual forma parte de la criminalística. Por lo que el campo de la Informática forense se inició en la década de 1978, mediante la creación que se hizo en Florida, sobre los crímenes de sistemas informáticos en el ¨ Computer Crimes Act¨, la cual es una acta que permite reconocer delitos informáticos ante la ley, como contra la propiedad privada, contra equipos informáticos y contra usuarios de

computadoras, un ejemplo claro de los delitos cometidos; son el sabotaje, el copyright, modificaciones, borrados y sustracción de datos[27].

No obstante, tres años después nace un programa denominado ¨ Copy II PC Sotfware¨ conocido también como ¨Copy 2 PC¨, en 1981 la cual consistía en una herramienta de copia exacta de los disquetes[28] de la época, que protegía a estos de la piratería. Posteriormente un año después, Peter Norton haría una herramienta para recuperar archivos borrados por accidente y más aplicaciones que serían pioneras en la informática forense[29]. Así mismo en el año de 1982, Peter Norton publico una aplicación denominada Un ¨ ERASE: NORTON UTILITIES 1.0¨, la primera versión del conjunto de herramientas ¨ NORTON UTILITIES¨, que permite recuperar archivos accidentalmente, cabe mencionar que otras aplicaciones como File Fix o Time Mark también eran útiles para su aplicación forense. Luego de su éxito con la suite de aplicaciones ¨ Copy 2 PC¨, Peter publico varios libros técnicos, como son el Inside the I.B.M.[30]

En cambio, en el año de 1984 fue creado un programa del FBI, conocido por un tiempo como el programa de medios magnéticos (Magnetic Media Program), que ahora se conoce como CART o análisis de informática y equipo de respuesta. Ahora bien, tiempo después de haberse publicado dicho programa, al hombre que se le atribuyo como el ¨Padre de la Informática Forense¨, comenzó a trabajar en este campo. Su nombre era Michael Anderson y era agente especial de la división de investigación criminal del IRS. En el año de 1985, Clifford Stoll un astrónomo de Estados Unidos, colaboro en la detección del Hacker Markus Hess, y en 1988 publico el documento ¨ Stalky de Willy Hacker¨ el cual relataba lo ocurrido en su detección.

---

[27] Navarro, Carlos. *Historia de la Informática Forense*. https://www.timetoast.com/timelines/historia-de-la-informatica-forense. 11/03/2021. 3:51 pm.

[28] Disquete; Es un elemento que permite almacenar datos digitales, que consta de un disco magnético protegido por una cubierta rectangular o cuadrada de plástico.

29 Marín, Miguel. Historia de la Informática Forense y su aplicación. http://tuertoperoveotodo.blogspot.com/2019/10/historia-de-la-informatica-forense-y-su.html. 11/03/2021. 4:04 pm.

[30] Navarro, Carlos. Op.Cit.

Este documento es transformado en 1989, en el libro ¨ El huevo del Cucu¨, anticipando de tal manera la metodología forense.

En el año de 1987, se crea la High Tech Crime Investigation Association (HTCIA), asociación de santa clara que agrupa profesionales tanto de agencias gubernamentales como compañías privadas para centralizar el conocimiento e impartir cursos. Así mismo en dicho año nace la compañía Access Data, pionera en el desarrollo de productos orientados a la recuperación de contraseñas y el análisis forense con herramientas como la actual Forense Tolkit (FTK). En 1988, se creó el programa ¨International Association of Computer Investigative Specialists¨ (IACIS), que certificará a profesionales de agencias gubernamentales en el Certified Forensic Computer Examiner (CFCE), una de las certificaciones más prestigiosas en el ámbito forense. En este mismo año se desarrolla el programa Seized Computer Evidence Recovery Specialists o SCERS, con el objetivo de formar a profesionales en computer forensics.[31]

La disciplina continuó creciendo en la década de 1992, con el libro "A forensic methodology for countering computer crime", de P. A. Collier y B. J. Spaul quienes acuñan el término "computer forensics". Otros libros posteriores continuaron desarrollando el termino y la metodología, como: "High-Technology Crime: Investigating Cases Involving Computers" de Kenneth S. Rosenblatt. En el año de 1995, se funda el International Organization on Computer Evidence (IOCE), con el objetivo de ser punto de encuentro entre especialistas en la evidencia electrónica y el intercambio de información. A partir de 1996 la INTERPOL organiza los International Forensic Science Symposium, como foro para debatir los avances forenses, uniendo fuerzas y conocimientos. En 1997, se reconoció ampliamente que los funcionarios encargados de hacer cumplir la ley en todo el mundo tenían que ser bien versados en la forma de adquirir la evidencia de las computadoras, un hecho puesto de manifiesto en un comunicado del G8 en 1997.

[31] Navarro, Carlos. Op.Cit.

La INTERPOL celebró un simposio sobre informática forense al año siguiente, y en 1999, el programa CART del FBI abordó 2000 casos individuales.[32]

Finalmente La carga de casos del CART del FBI continuó creciendo, mientras que en 1999, el equipo analizó 17 terabytes de datos, para el año 2003 el grupo examinó 782 terabytes de datos en sólo un año. Con los avances en la informática y la proliferación del acceso a Internet en todo el mundo, la informática forense comenzó a desempeñar un papel más importante para los agentes del orden.

Con el advenimiento de los teléfonos inteligentes y PDA, las formas en que la informática forense puede operar se ha vuelto aún más importante a medida que los delincuentes tienen muchas opciones para romper la ley mediante el uso de dispositivos de computación.[33]

2.3. Concepto, Objetivos y usos de la Informática Forense.

Según el FBI, la Informática o Computación Forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. La Informática Forense hace entonces su aparición como disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.[34]

Dicho de otra manera la Informática Forense posibilita la detección y recuperación de la información digital que sirve de evidencia a la hora de reconstruir un hecho o sucesión de ellos. La actuación forense en Informática permite recuperar y enhebrar esos rastros digitales de nuestro paso por la vida, garantizando su valor probatorio.[35]

En el apartado anterior, se hizo mención de los antecedentes de la informática forense, destacándose de esta manera que en el año de 1984, el laboratorio del FBI con el

---

[32] Yisus. Historia Informática Forense. http://informaticaforense1.blogspot.com/2013/11/historia-informatica-forense.html. 11/03/2021. 7:19 pm.
[33] Ibid.
[34] Gutierrez David, Juan. *Informatica Forense*. 2006. p.3.
[35] Ruiz de Angeli, Gonzalo M. El Rastro Digital Del Delito Aspectos Técnicos, Legales y Estratégicos de la Informática Forense. Universidad FASTA. Mar del Plata.2017.p.16.

apoyo de otras agencias que persiguen el cumplimiento de la ley, empezaron a desarrollar programas para examinar evidencia computacional. De este modo, dentro de lo denominado forense encontramos las siguientes definiciones;[36]

- Computación Forense (Computer Forensics): Es una disciplina de las ciencias forenses que considera las tareas propias asociadas con la evidencia, para procurar, descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.
- Forensia en Redes (Network Forensics): Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción.
- Forensia Digital (Digital Forensics): Es una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (utilizando preguntas como; ¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿por qué?) 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 inseguridad informática.[37]

[36] Gutiérrez David, Juan. Op.Cit.
[37] Idem.

Objetivos de la Informática Forense:

La Informática Forense tiene 3 objetivos:

1) La compensación de los daños causados por los criminales o intrusos.
2) La persecución y procesamiento judicial de los criminales.
3) La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de la evidencia.[38]

Usos de la Informática Forense

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense:[39]

- Prosecución Criminal: Evidencia incriminatoria que puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
- Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
- Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
- Temas Corporativos: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
- Mantenimiento de la ley: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

[38] Gutierrez David, Juan. Op.Cit.
[39] Ibid. p.4.

2.4. Análisis Forense.

El análisis forense es un área perteneciente al ámbito de la seguridad informática surgida a raíz del incremento de los diferentes incidentes de seguridad. En el análisis forense se realiza un análisis posterior de los incidentes de seguridad, mediante el cual se trata de reconstruir como se ha penetrado o vulnerado en el sistema.

Por tanto, cuando se está realizando un análisis forense se intenta responder las siguientes preguntas:[40]

- ¿Quién ha realizado el ataque?
- ¿Cómo se realizó?
- ¿Qué vulnerabilidades se han explotado?
- ¿Que hizo el intruso una vez que accedió al sistema?

En otras palabras, el análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis puede determinar quien, desde donde, como, cuando y que acciones ha llevado a cabo un intruso en los sistemas más afectados por un incidente de seguridad. El procedimiento utilizado para un análisis forense es el siguiente:

- Estudio Preliminar: En esta fase se realiza un estudio mediante entrevista y documentación entregada por el cliente con el objetivo de tener una idea inicial del problema que nos vamos a encontrar.
- Adquisición de Datos: Se realiza una obtención de los datos e informaciones esenciales para la investigación. Se duplican o clonan los dispositivos implicados para un posterior análisis. En esta fase habrá que tener mucho cuidado en la adquisición de los datos puesto que cabe la posibilidad de incumplir los derechos fundamentales del atacante.

[40] Rivas López, José Luis. Análisis Forense de Sistemas Informáticos. Eureca Media, SL.Barcelona.2009.p. 9.

- Análisis e Investigación: Se realiza un estudio con los datos adquiridos en la fase anterior. En esta fase también habrá que tener mucho cuidado puesto que cabe la posibilidad incumplir los derechos fundamentales del atacante.
- Realización del Informe: En esta fase se elabora el informe que será remitido a la dirección de la organización o empresa. Posteriormente, se podrá usar para acompañar la denuncia que realicemos a la autoridad competente. [41]

Las fuentes de información que se utilizan para realizar análisis forense son diversas, como correos electrónicos, IDS/IPS, archivo de logs de los cortafuegos, archivo de logs de los sistemas, etc.

2.5 Características de las tecnologías de la Información.

La tecnología de la información es un proceso que utiliza una combinación de medios y métodos de recopilación, procesamiento y transmisión de datos para obtener nueva información de calidad sobre el estado de un objeto, proceso o fenómeno. El propósito de la tecnología de la información es la producción de información para su análisis por las personas y la toma de decisiones sobre la base de la misma para realizar una acción. La introducción de una computadora personal en el ámbito de la información y la aplicación de los medios de comunicación de telecomunicaciones han determinado una nueva etapa en el desarrollo de la tecnología de la información. La TEcnologia de la información (TI) moderna es una tecnología de la información con una interfaz de usuario "amigable" que utiliza computadoras personales e instalaciones de telecomunicaciones. La nueva tecnología de la información se basa en los siguientes principios básicos;[42]

- Modo interactivo (diálogo) de trabajar con una computadora.
- Integración con otros productos de software.
- Flexibilidad en el proceso de cambio de datos y definiciones de tareas.

[41] Ibid. p. 6.
[42] Las Tecnologías de la Información. https://www.ceupe.com/blog/que-son-las-tecnologias-de-la-informacion.html. 12/03/2021 .2:21 pm.

Características de las Tecnologías de la Información.

- Operación del usuario en el modo de manipulación de datos (sin programación): El usuario no debe saber y recordar, sino que debe ver (dispositivos de salida) y actuar (dispositivos de entrada).
- Soporte de información transversal: En todas las etapas de la transmisión de información sobre el apoyo de una base de datos integrada, que proporciona una forma única de introducir, buscar, mostrar, actualizar y proteger la información.
- Procesamiento de documentos sin papel: Durante el cual sólo se registra la versión final del documento en papel, las versiones intermedias y los datos necesarios registrados en los medios se entregan al usuario a través de la pantalla de visualización del PC.
- Modo de solución de tareas interactivo (de diálogo) con una amplia gama de posibilidades para el usuario.
- Producción colectiva de un documento sobre la base de un grupo de ordenadores unidos por medios de comunicación.
- Procesamiento adaptativo de la forma y los modos de presentación de la información en el proceso de resolución de problemas.

Tipos de tecnologías de la información[43]

- La tecnología de la información para el procesamiento de datos: Está diseñada para resolver problemas bien estructurados, cuyos algoritmos de solución son bien conocidos y para los cuales existen todos los datos de entrada necesarios. Esta tecnología se aplica al nivel de rendimiento del personal de baja calificación con el fin de automatizar algunas operaciones rutinarias y constantemente repetidas del trabajo administrativo.

[43] Las Tecnologías de la Información. Op.Cit.

- La tecnología de información de gestión: Está destinada al servicio de información de todos los empleados de las empresas, relacionado con la aceptación de las decisiones administrativas. En este caso, la información suele presentarse en forma de informes de gestión ordinarios o especiales y contiene información sobre el pasado, el presente y el posible futuro de la empresa.
- La tecnología de la información de la oficina automatizada: Está diseñada para complementar el sistema de comunicación existente del personal de la empresa. La automatización de la oficina asume la organización y el apoyo de los procesos de comunicación tanto dentro de la empresa, como con el entorno externo sobre la base de redes informáticas y otros medios modernos de transferencia y trabajo con la información.
- La tecnología de la información para el soporte de decisiones: Está diseñada para desarrollar una decisión de gestión que se produce como resultado de un proceso iterativo en el que participan un sistema de soporte de decisiones (un enlace informático y el objeto de la gestión) y una persona (el enlace de gestión, que establece datos de entrada y evalúa el resultado).
- La tecnología de la información de los sistemas expertos: se basa en el uso de inteligencia artificial. Los sistemas expertos permiten a los gerentes recibir asesoramiento experto sobre cualquier problema sobre el cual se haya acumulado conocimiento en estos sistemas.

2.6. Definición de Hacker

Los hacker y la cultura asociada a ellos, inicio en la década de 1960 y 1970, en universidades como el instituto tecnológico de Massachusetts (MIC), Carnegie Mellon, Berkeley, CalTech o Standford, que tenían la capacidad de mantener equipos de cómputo y una gran cantidad de alumnos sedientos de conocerlos, programarlos y experimentar con ellos, hasta llegar a las entrañas mismas de su arquitectura.

Sin embargo, a lo largo de los años, este término se ha enrarecido y hasta mitificado dentro del ámbito de lo ilegal, lo maligno y lo destructivo[44].

Si nos detenemos a revisar la definición de hacker, encontraremos autores como Sweigart quien lo detalla como un individuo que estudia un sistema (informático) para comprenderlo tan profundamente, que pueda ser capaz de modificarlo de distintas formas, en su mayoría creativas. Por su parte, Erickson señala que el hacker resuelve problemas en formas inimaginables comparado con aquellos que se circunscriben en resolverlos pensando en metodologías convencionales.

Incluso Palmer describe el término hacker como aquella persona que programa de manera entusiasta y aprende a detalle los sistemas de cómputo. En efecto, un hacker es una persona que tiene profundos conocimientos en informática, es decir, incursiona a detalle los sistemas operativos, la programación, arquitectura de computadoras, sistemas de comunicación de datos, entre otros. Su objetivo principal es conocer y demostrar que conoce.

Tipos de Hackers

- Black Hat Hackers: Hackers de Sombrero Negro son los individuos malos, los que comúnmente se les refiere como simples Hackers. El término se usa mucho específicamente para los Hackers que rompen la seguridad de una Computadora, un Network o crean Virus de Computadora.
- White Hat Hackers: Hackers de Sombrero Blanco son los individuos buenos, los éticos. Regularmente son los que penetran la seguridad de sistemas para encontrar vulnerabilidades, se centra en asegurar y proteger los sistemas de Tecnologías de información y comunicación. Algunos son consultores de seguridad, trabajan para alguna compañía en el área de seguridad informática protegiendo los sistemas de los Black Hat Hackers, donde se puede definir a los White hat hackers como escudos o que protegen un sitio u otro medio.

[44] Vélez Martínez, Cuauhtémoc. Hackers. http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/hackers.aspx. 13/03/2021. 5:09pm.

- Gray Hat Hackers: También llamados Hackers de Sombrero Gris son los que juegan a ser los buenos y los malos, en otras palabras, tienen ética ambigua. Por lo general no hackean para beneficio personal ni tienen intenciones maliciosas, pero pueden estar dispuestos a comprometerse técnicamente crímenes durante el curso de sus hazañas tecnológicas con el fin de lograr una mayor seguridad donde un hacker puede usar su conocimiento para incrementar la seguridad en la cual también se le puede tomar como uno que viola a seguridad.
- Crakers: Estos comúnmente entran en sistemas vulnerables y hacen daño ya sea robando información, dejando algún virus, malware, trojan en el sistema y crean puertas traseras para poder entrar nuevamente cuando les plazca.
  Viola la seguridad de un sistema informático.
- Script Kiddies: Se le conoce a los Hackers que utilizan programas escritos de otros para penetrar algún sistema, red de computadora, página web, etc. ya que tiene poco conocimiento sobre lo que está pasando internamente en la programación. Es habitual asumir que los script kiddies son personas sin habilidad para programar sus propios medios, y que su objetivo es intentar impresionar a sus amigos o ganar reputación.
- Phreaker: Es aquella persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello. En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos.
- Newbie: Este es el Novato es el que se tropieza con una página web sobre Hacking y baja todas las utilidades y programas a su PC, comienza a leer y ejecutar los programas para ver que hacen. Se refiere a un recién iniciado en la informática. Y hace referencia a las personas realmente interesadas en aprender, y que no buscan que los demás integrantes de la comunidad o foro a la que pertenecen solucionen sus problemas.

- Lammer: En este caso se trata de un individuo que se cree Hacker y no tiene los conocimientos necesarios ni la lógica para comprender que es lo que realmente está sucediendo cuando utiliza algun programa ya hecho para hackear y romper alguna seguridad. Es el que ha bajado cientos de libros y videos de sitios donde se propaga la piratería de diversos temas de hacking, te lo dice y no ha leído ni visto ninguno de los videos, solamente los almacena. Se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender.[45]

2.7 Técnicas de Hacking

En relación con el apartado anterior, que explica la definición de Hacker y sus derivados, es importante saber las técnicas que emplean mediante hacking, esto quiere decir que las técnicas son una materialización de una mente que va más allá del manual, mediante esto podemos visualizar dos modelos de técnicas para ser llamado Hacker. Uno conceptual y otro operacional. Los dos son mutuamente complementarios y no excluyentes.

En el conceptual detallamos que se busca alcanzar, y en el operacional el cómo se desarrolla. Estas dos visiones les darán a los analistas más elementos de actuación y revisión antes de profundizar en los detalles técnicos de los ataques realizados.[46]

El modelo conceptual presenta tres etapas o fases claramente identificadas: reconocimiento, vulneración u ataque, eliminación y salto. Cada una de ellas es parte del sello de la investigación y perseverancia del Hacker para lograr su cometido: una nueva distinción para la seguridad de la información. Este modelo de Hacking desarrolla la mente de un analista de riesgos y vulnerabilidades que se concentra en las posibilidades y actúan conforme a ellas, alejándose del perfil tradicional del analista de riesgos que se concentra en la protección de los activos y los controles requeridos.

---

[45] Flores Quispe, Carlos Alberto. Tipos de Hackers. http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a08.pdf. 14/03/2021. 5:54 pm.

[46] Cano Martínez, Jeimy J. Computación Forense Descubriendo los Rastros Informáticos. México. 2009.p.35.

En el modelo Operacional de Hacking se complementa lo expuesto en la propuesta conceptual previamente revisada. Operacionalmente, para lograr sus propósitos, el hacker adelanta los siguientes pasos: Reconocimiento pasivo, reconocimiento activo-scanning, explotación o vulneración del sistema e intrusión. Finalmente y consistente con lo planteado en el modelo conceptual, se requiere evadir posibles investigaciones o acciones para identificar, y evidenciar el posible ataque o intrusión. [47]

Lograr este cometido está directamente relacionado con el nivel de experiencia y conocimiento técnico del atacante, es decir, entre más especializado sea el atacante en el sistema operacional, aplicación o dispositivo de hardware, menos espacio para rastros habrá para el investigador forense, pues este sabrá adelantar las acciones requeridas para que lo que se encuentre sea inconsistente, no coincida con lo que ha pasado, o se confunda con una falla normal del sistema objetivo.

2.8 Falsificación de la Información conforme las Redes Sociales.

Actualmente con nuestras actividades diarias exponemos nuestra identidad y nuestros datos personales en diversas ocasiones, por ejemplo cuando realizamos compras y utilizamos nuestra tarjeta de crédito, esta puede ser clonada para posteriormente hacer uso de nuestros recursos económicos de manera fraudulenta; al realizar un trámite bancario nos identificamos con algún documento oficial en donde dejamos expuesto no solo nuestro nombre y nuestra firma sino nuestra dirección, nuestra edad y hasta nuestro distrito electoral; también al realizar trámites escolares, por ejemplo; proporcionamos datos como son nuestra dirección, nuestro número de teléfono de oficina o personal; al sacar una copia de nuestra identificación oficial esta puede ser escaneada para posteriormente hacer uso de todos los datos que en ella se ostentan; y así, existen distintas acciones que ponen a los individuos en riesgo de usurpación, robo o suplantación de nuestra identidad.[48]

---

[47] Ibid.p.39

[48] Barrera Aguilar, Efrain. Suplantacion de la Identidad Digital con Fines de Trata de Personas en Facebook.https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/363/1/INFOTEC_MDTIC_EAB_26092019.pdf. 14/03/2021. 7:00pm.

Actualmente nuestros teléfonos celulares se han convertido en dispositivos que almacenan ya sea en su memoria interna o haciendo uso del almacenamiento en la nube, una cantidad enorme de información personal. Los distintos desarrolladores de programas solicitan nuestros datos para poder utilizar ciertas aplicaciones como son las bancarias, las de juegos y las de entretenimiento. Estas aplicaciones al instalarlas nos solicitan que aceptamos, e incluso, compartamos con terceros la información solicitada.

Los usuarios de estos dispositivos constantemente somos requeridos para actualizar ciertos programas; en ocasiones estas “actualizaciones”, son programadas y ya ni siquiera estamos conscientes de ellas, pero que sin estas, no podríamos continuar utilizando los programas lo que haría imposible seguir recibiendo pagos, mensajes, acceder a los juegos, hacer uso de aplicaciones como las bancarias, etcétera; y es muy riesgoso no hacerlas inmediatamente puesto que esto ocasiona el aumento de la inseguridad en los dispositivos móviles y es más fácil que la información sea robada e incluso se nos intente extorsionar, por ejemplo al hacer uso de nuestras fotos privadas que fueron almacenadas y sustraídas sin nuestra autorización.

Por otro lado, cuando se crean los perfiles falsos en las redes sociales pueden afectar a la imagen de una empresa. Estos perfiles suelen ser utilizados para dejar comentarios negativos, opiniones negativas y publicarlas en tu página de la red social. Las redes sociales son herramientas maravillosas de comunicación y de auto-promoción para una empresa. Los profesionales utilizan las redes sociales sobre todo para comunicarse con sus clientes o futuros clientes, vender y retener a los clientes. Pero cuidado, una presencia en las redes sociales no está exenta de riesgos y se requiere vigilancia. Un perfil falso también se llama fake. Un fake es un perfil falso, una falsificación, una imitación. Un fake puede suplantar el perfil o identidad de una persona real utilizando su nombre, la dirección, y la imagen. Un perfil falso también puede ser una identidad creada desde cero.

Los perfiles falsos son creados por personas o robots normalmente con malas intenciones. Más allá de los timos clásicos, una de las nuevas misiones de estos perfiles falsos es dañar la imagen de una empresa o una persona con opiniones y comentarios negativos.

Estos perfiles falsos son cada vez mayores, las redes sociales como Twitter y Facebook ponen en marcha acciones para proteger a sus usuarios. En caso de identidades hechas con robots o bots, Facebook las puede detectar gracias a una herramienta desarrollada que puede detectar una cuenta con un nombre o una imagen similar a otro usuario, enviando una notificación de alertar al usuario de que puede haber sido víctima de una suplantación de identidad.

Se está obligando a confirmar dicho mensaje. Si el perfil es falso Facebook lleva a cabo una comprobación manual. Según estudios realizados, se ha detectado un aumento de perfiles falsos que muchas empresas están utilizando para aumentar artificialmente su comunidad.[49]

2.9. Clasificación de Huellas Digitales

La huella digital es un concepto que incorpora todos los registros y rastros que dejamos cuando utilizamos internet. En la mayoría de los casos son beneficiosos para el usuario, pero en otras pueden ser realmente perjudiciales ya que nunca son irrelevantes. Estos registros representan información sobre nosotros que pueden servir a terceros para ganar dinero o bien conocer nuestras preferencias y poder vender mejor sus productos.[50]

Para entender mejor este término, vamos a establecer primeramente que hay dos clasificaciones principales de huellas digitales (*digital footprint):* las pasivas, a las que llamamos sombra digital, y las activas, también conocidas como identidad digital. Se crean huellas digitales pasivas cuando los datos se recolectan o se generan sin conocimiento o consentimiento del individuo.

Se crean huellas digitales activas cuando los datos personales son lanzados deliberadamente por el individuo con el propósito de compartir información acerca de sí mismo en los sitios web, las redes sociales o los sistemas en línea.

---

[49] Flox, Antonio. Los Perfiles Falsos en las Redes Sociales. https://www.indedmedia.com/blog/los-perfiles-falsos-las-redes-sociales/. 14/03/2021. 7:30 pm.
[50] ¿Que es la Huella Digital y Cuál es su Importancia?. https://www.ambit-bst.com/blog/huella-digital-importancia. 15/03/2021. 8:00 pm.

De tal manera que la Sombra digital, la cual forma parte de la huella digital pasiva puede almacenarse de muchas maneras dependiendo de la situación. Dicho de otra manera cuando en un entorno en línea, la sombra digital es almacenada en una base de datos como un *hit.*

Esta huella puede rastrear la IP del usuario, cuándo fue creada y de dónde venían los datos. Un ejemplo de ello es cuando subimos la fotografía de un evento, de un conocido o de un familiar a una red social.

En un entorno fuera de línea, la sombra digital puede almacenarse en archivos, los cuales son gestionados por administradores de la información para conocer las acciones ejecutadas en la máquina, sin la posibilidad de determinar quién lo realiza. Por ejemplo, los datos registrados en un sistema para conocer elementos de interés del sujeto de cara a alguna actividad particular. Como las bases de datos de talento humano, para citar un caso, o las bases de datos consultadas en el caso de Keylor Navas. Ahora bien, cuando hablamos de la identidad digital, nos referimos de igual manera a la huella digital activa, es decir, que podemos explicar que la identidad digital se ensambla siempre en entornos en línea, es decir, un usuario la almacena porque se registra en un sitio, una red social, un sistema de reclutamiento o selección, o cuando crea y gestiona un correo; también al hacer un *post* en una red social, un blog, etc.

Con fines más intrusivos, la identidad digital puede ser almacenada en archivos (*cookies),* o bien cuando el dueño de la computadora captura secuencias de los registros de acontecimientos de su sistema para que estos puedan mostrar las acciones del individuo en esa terminal.[51]

[51] Todos Dejamos Huella Digital. https://www.nacion.com/opinion/foros/todos-dejamos-huella-digital/WS4IE7MYV5HSTMTUXDHQS2RQHE/story/. 15/03/2021. 8:30 pm

2.10 Conclusión

Para concluir este apartado, es importante mencionar que la informática forense es una ciencia en constante evolución que coadyuva con procedimientos estrictos y rigurosos, por lo que esto ayudara a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

Propuesta

En relación con lo ya expuesto anteriormente se debe de formular e implementar una política pública en donde se adapten no solo los derechos digitales si no también los derechos humanos relacionados con el derecho de intimidad, derecho de privacidad y derecho a la libre expresión, ya que de esta manera no se garantizan correctamente la realización de dichos derechos, sino más bien es darle un enfoque conforme los mecanismos de prevención para lograr una difusión de los datos biométricos que se deben de proteger y respetar en redes sociales en Morelos, esto para evitar ser víctima de delitos cibernéticos, lo cual ayudara a erradicar dichos delitos en redes sociales y atribuirles su respectiva sanción conforme la ley.

A continuación se mostraran los derechos digitales [52] y los derechos humanos[53] existentes que nos ayudaran para la implementación de la política pública de control de datos biométricos y huellas digitales que se deberá usar con responsabilidad para prever, conocer y garantizar para que los encargados de las redes sociales respeten los derechos digitales en el estado de Morelos.

Derechos Digitales:

1. Derecho a la intimidad en el ámbito laboral

[52] Los 10 derechos digitales que debes conocer. https://www.eude.es/blog/derechos-digitales-eude/. 25/03/2021

[53]LA DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS DE LAS NACIONES UNIDAS. https://www.jovenesporlosderechoshumanos.mx/what-are-human-rights/universal-declaration-of-human-rights/articles-1-15.html. 25/03/2021.

Permite a los trabajadores tener derecho a la protección de su intimidad frente a los dispositivos digitales, de video vigilancia y de grabación de sonidos en el lugar de trabajo, y sistemas de geolocalización.

2. Derecho a la neutralidad de Internet

Los proveedores de servicios de Internet deberán ser transparentes en su oferta de servicios, evitando discriminar a los ciudadanos por motivos técnicos y económicos.

3. Derecho a la seguridad digital

Derecho de los usuarios a la seguridad en las comunicaciones que realicen a través de Internet

4. Derecho al olvido en búsquedas en Internet, servicios de redes sociales y equivalente

Los motores de búsqueda en Internet deben eliminar los resultados que surgen a partir del nombre de una persona, cuando haya datos inexactos, no pertinentes o no actualizados.

5. Derecho a la libertad de expresión

Es nuestro derecho a emitir y recibir opiniones y toda clase de información en todo formato digital, sin controles previos por parte del Estado o de las empresas prestadoras de servicios.

6. Derecho a la portabilidad

Los usuarios pueden recibir y transmitir los contenidos que han facilitado a los prestadores de servicios de internet.

7. Derecho de la negociación colectiva

Los convenios colectivos pueden establecer garantías adiciones de los derechos y libertades, relacionados con los datos personales de los trabajadores y los derechos digitales en el ámbito laboral.

8. Derecho a la protección de datos de los menores en Internet

La ley establece que los centros educativos y cualquier persona que desarrolle actividades con menores de 14 años de edad, deberá contar con el consentimiento del meno o de sus representantes legales.

9. Derecho de rectificación en Internet

Posibilita la opción de que cuando los usuarios difundan contenidos contra el honor y la intimidad, puedan rectificar ateniendo a los requisitos de una ley específica que regula el derecho a la rectificación.

10. Derecho a la actualización de informes en medios digitales

Los usuarios podrán solicitar a los medios de comunicación digitales un aviso de actualización visible junto a las noticias, si estas no reflejan su situación actual por circunstancias posteriores a la publicación.

Derechos Humanos

1. Todos Hemos Nacido Libres e Iguales. Todos hemos nacido libres. Todos tenemos nuestras propias ideas y pensamientos. Todos deberíamos ser tratados de la misma manera.

2. No Discrimines. Estos derechos pertenecen a todos, sin importar nuestras diferencias.

3. El Derecho a la Vida. Todos tenemos el derecho a la vida y a vivir en libertad y con seguridad.

4. Ninguna Esclavitud. Nadie tiene derecho a convertirnos en esclavos. No podemos hacer a nadie nuestro esclavo.

5. Ninguna Tortura. Nadie tiene ningún derecho a dañarnos o torturarnos.

6. Tienes Derechos Sin Importar a Donde Vayas.

7. Todos Somos Iguales Ante la Ley. La ley es la misma para todos. Nos debe tratar a todos con equidad.

8. La Ley Protege tus Derechos Humanos. Todos tenemos el derecho de pedir a la ley que nos ayude cuando hemos sido tratados injustamente.

9. Ninguna Detención Injusta. Nadie tiene el derecho de meternos en la cárcel sin una buena razón y de mantenernos encarcelados o de echarnos de nuestro país.

10. El Derecho a un Juicio. Si se nos lleva a juicio tiene que ser en público. Las personas que nos juzgan no deben permitir que alguien más les diga qué hacer.

11. Somos Siempre Inocentes hasta que se Pruebe lo Contrario. No se debería culpar a nadie de haber hecho algo hasta que se haya demostrado. Cuando alguien nos acusa de haber hecho algo incorrecto, tenemos el derecho de demostrar que eso no es verdad.

12. El Derecho a la Intimidad. Nadie debería tratar de dañar nuestra reputación. Nadie tiene el derecho de entrar en nuestra casa, abrir nuestras cartas o molestarnos o a nuestra familia sin una buena razón.

13. Libertad de Movimiento. Todos tenemos el derecho de ir a donde queramos en nuestro propio país, y de viajar a donde nos plazca.

14. Derecho de Buscar un Lugar Seguro en Donde Vivir. Si tenemos temor de ser tratados mal en nuestro propio país, tenemos el derecho de irnos a otro país para estar seguros.

15. El Derecho a una Nacionalidad. Todos tenemos el derecho de pertenecer a un país.

Ahora bien de esta manera se planteara la política pública antes mencionada para el adecuado control y responsabilidad de los datos biométricos y huellas digitales en redes sociales en el estado de Morelos.

1. Mecanismos de Difusión de Datos Biométricos.	Mediante el uso de las tecnologías de la información se conformara el debido conocimiento de los datos biométricos dirigido a los usuarios de las redes sociales con el fin de brindar un adecuado con control y responsabilidad del manejo de información personal en redes sociales.
2. Prevención de Delitos Cibernéticos en Redes Sociales	Establecer estrategias que ayuden a proteger la identidad de cada usuario en redes sociales así como también su información personal. Esclarecer no usar cualquier medio tecnológico de otro individuo, ya que de esta manera puedes ser víctima de suplantación de identidad. Evitar en lugares públicos abrir nuestras redes sociales, un ejemplo un cibercafé.
3. Capacitación dirigida a los Encargados de las Redes Sociales para contrarrestar Delitos Cibernéticos	Brindar un programa para capacitar e instruir a los encargados de las redes sociales sobre cómo actuar cuando se está en una situación de delitos cibernéticos y así mismo brindar el apoyo necesario a las víctimas.
4. Promoción de los Derechos Digitales.	Promover y garantizar a los encargados y usuarios el conocimiento de los derechos

	digitales en redes sociales. Promover las sanciones que traerán el indebido uso de los derechos digitales conforme la ley.
5. Crear un grupo de ayuda para víctimas de Delitos Cibernéticos.	Capacitar al personal encargado de los delitos cibernéticos para promover y garantizar ayuda a las víctimas de los delitos cibernéticos así como también garantizar sus debidos derechos digitales y humanos hacia su identidad.

Bibliografía

Barrera Aguilar, Efraín. Suplantación de la Identidad Digital con Fines de Trata de Personas enFacebook.https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/363/1/INFOTEC_MDTIC_EAB_26092019.pdf. 14/03/2021. 7:00pm.

Cano Martínez, Jeimy J. Computación Forense Descubriendo los Rastros Informáticos. México. 2009.p.35.

Caballero Delgado, Samuel Alfonso. Dactiloscopia Certeza o Incertidumbre. Editorial Ltda. Colombia. 2009. p.32.

Criminalística y más. http://criminalisticaymasifil2.blogspot.com/p/escribir-el-nombre-del-autor.html. 08/03/2021. 4:32 pm.

Camacho Vaca, Arturo. Certeza de la Dactiloscopia. https://revista.cleu.edu.mx/new/descargas/1904/Articulo08_certeza-de-la-dactiloscopia.pdf. 08/03/2021. 5:27 pm.

¿Qué es la Huella Digital y Cuál es su Importancia? https://www.ambit-bst.com/blog/huella-digital-importancia. 15/03/2021. 8:00 pm.

Dactiloscopia. http://dactiloscopia-quijada.blogspot.com/p/introduccion.html. 08/03/2021. 05:40 pm.

Flores Quispe, Carlos Alberto. Tipos de Hackers. http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a08.pdf. 14/03/2021. 5:54 pm.

Flox, Antonio. Los Perfiles Falsos en las Redes Sociales. https://www.indedmedia.com/blog/los-perfiles-falsos-las-redes-sociales/. 14/03/2021. 7:30 pm.

Gómez Bernal, Eduardo. Tópicos Médicos Forense. SISTA. México. 2017.p. 473.

Gutiérrez David, Juan. Informática Forense. 2006. p.3.

Hope Davis, Spencer. Tipos de Patrones en la Identificación por Huellas Dactilares. https://www.geniolandia.com/13176324/tipos-de-patrones-en-la-identificacion-por-huellas-dactilares. 08/03/2021. 05:50 pm.

Laúd H, John. Libro de Referencia de las Huellas Dactilares. Departamento de Justicia de los Estados Unidos. https://www.ojp.gov/pdffiles1/nij/249575.pdf. Washington, DC. p.4.

Las Tecnologías de la Información. https://www.ceupe.com/blog/que-son-las-tecnologias-de-la-informacion.html. 12/03/2021 .2:21 pm.

Los 10 derechos digitales que debes conocer. https://www.eude.es/blog/derechos-digitales-eude/. 25/03/2021

LA DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS DE LAS NACIONES UNIDAS. https://www.jovenesporlosderechoshumanos.mx/what-are-human-rights/universal-declaration-of-human-rights/articles-1-15.html. 25/03/2021.

Marín, Miguel. Historia de la Informática Forense y su aplicación. http://tuertoperoveotodo.blogspot.com/2019/10/historia-de-la-informatica-forense-y-su.html. 11/03/2021. 4:04 pm.

Navarro, Carlos. Historia de la Informática Forense. https://www.timetoast.com/timelines/historia-de-la-informatica-forense. 11/03/2021. 3:51 pm.

Ruiz de Angeli, Gonzalo M. El Rastro Digital Del Delito Aspectos Técnicos, Legales y Estratégicos de la Informática Forense. Universidad FASTA. Mar del Plata.2017.p.16.

Rivas López, José Luis. Análisis Forense de Sistemas Informáticos. Eureca Media, SL.Barcelona.2009.p. 9.

Trujillo Arriaga, Salvador. El Estudio Científico de la Dactiloscopia. LIMUSA. México. 2000. p.21.

Todos Dejamos Huella Digital. https://www.nacion.com/opinion/foros/todos-dejamos-huella-digital/WS4IE7MYV5HSTMTUXDHQS2RQHE/story/. 15/03/2021. 8:30 pm

Vargas Alvarado, Eduardo. Medicina Legal. Trillas. México.2017.p.90.

Vélez Martínez, Cuauhtémoc. Hackers. http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/hackers.aspx. 13/03/2021. 5:09pm.

Yisus. Historia Informática Forense. http://informaticaforense1.blogspot.com/2013/11/historia-informatica-forense.html. 11/03/2021. 7:19 pm.