2023

LEGISLACIÓN

UNIDAD 4:

DERECHO INFORMÁTICO

UNIVERSIDAD TECNOLÓGICA NACIONAL - FACULTAD REGIONAL GENERAL PACHECO

TECNICATURA UNIVERSITARIA EN PROGRAMACIÓN

DOCENTE: LUPANI MARÍA CECILIA. AYUDANTE: CARBONARI VERÓNICA

Contenido

EL DERECHO Y LA INFORMÁTICA

Definimos al Derecho Informático como "*el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación de sujetos en el ámbito de la informática y sus derivaciones, especialmente en el área denominada tecnología de la información. Así, las Ciencias Jurídicas analizan los impactos de la informática en todos los ámbitos de la sociedad y estudia los cambios y transformaciones que produce para poder regularlas adecuadamente".*

Como principio general, el Derecho debe evolucionar con las nuevas necesidades y costumbres de los seres humanos para así poder regular adecuadamente las nuevas relaciones que surgen. Así, se considera que el Derecho Informático es un punto de inflexión del Derecho, puesto que todas sus áreas de estudio se han visto afectadas por la aparición de la denominada Sociedad de la Información, cambiando de este modo los procesos sociales y, por tanto, los procesos políticos y jurídicos.

Por este grado de evolución de la tecnología y su impacto en todas las actividades humanas se ha convertido en una rama del Derecho donde sus especialistas investigan cada implicancia legal en el uso y aplicación de la informática y las tecnologías de información (TIC).

SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

Gobiernos, empresas, organizaciones y profesionales, a nivel mundial, se esfuerzan en garantizar la seguridad de la información digital, de los sistemas informáticos, de los servicios digitales y de las infraestructuras de red. Este esfuerzo se materializa en destinar más recursos profesionales y económicos en investigación tecnológica y seguridad de las TIC.

Por otro lado, el incremento de la Cibercriminalidad y delitos relacionados con la tecnología digital bien de forma directa o donde la información digital es parte de las pruebas de una investigación judicial, abren las puertas laborales a expertos en ciberseguridad y análisis forense digital.

Sin duda el mercado laboral de las TIC, la Ciberseguridad e Informática Forense digital está en auge y es uno de los menos afectados por la crisis económica mundial.

La SEGURIDAD INFORMÁTICA es un proceso preventivo para detectar usos no autorizados de datos, información o sistemas informáticos. Lleva implícito el proceso de proteger el uso de los recursos informáticos contra intrusiones maliciosas o no (puede que se acceda a ellos por accidente). Forma parte de la SEGURIDAD DE LA INFORMACIÓN e incluye una cantidad de medidas de seguridad que abarcan Software y Hardware. La información es uno de los activos más importantes de las empresas. Por eso, es fundamental protegerla y resguardarla.

El vertiginoso avance de los servicios digitales y de las Tecnologías de la Información y la Comunicación (TIC), su accesibilidad y su rápida adaptación en la sociedad, están aportando grandes beneficios a nivel social, cultural y económico. Si añadimos, la hiperconectividad, como fruto de la globalización, que ofrece formas más rápidas y efectivas de comunicación, con acceso a gran cantidad de información digital en una nueva dimensión donde se desdibujan las fronteras geográficas, nos encontramos ante un nuevo entorno, el ciberespacio, el cual ha cambiado la forma en que las organizaciones, empresas, administraciones públicas e individuos se relacionan.

Este traslado de la actividad diaria y la dependencia de la sociedad en los servicios que ofrece el ciberespacio –internet, redes sociales, correo electrónico, cibereconomía, teletrabajo, administración electrónica, etc. – aumenta drásticamente el número de riesgos y amenazas con un alto grado de repercusión económica y social. Incluso los gobiernos, dentro del marco de la Seguridad Nacional, consideran de vital importancia la seguridad del ciberespacio, sobre todo ante los posibles ciberataques dirigidos a las infraestructuras críticas y sistemas de defensa.

Las ciberamenazas se pueden englobar en dos grandes grupos:

1) **las dirigidas contra la información**, y

2) **las que su objetivo son las infraestructuras TIC**. A nivel general las ciberamenazas se caracterizan por:

(a) Ser difíciles de prever, identificar, controlar y erradicar.

(b) Su dimensión global.

(c) Su gran impacto social. Y

(d) Su sofisticación y bajo coste de ejecución.

Por todo ello, gobiernos, empresas, organizaciones e instituciones necesitan aplicar medidas de seguridad no solo reactivas sino también proactivas, y adoptar la Ciber- Resiliencia5 como elemento primordial de respuesta ante los "inevitables" ataques.

Así pues, en el supuesto de sufrir un ciberataque, es vital identificar: a su autor/es, el objetivo, los sistemas informáticos afectados, como se ha realizado –brechas de seguridad- y el impacto global en la organización. Aquí es donde la figura del perito informático forense es un eslabón esencial en la cadena de la seguridad informática. Su labor de investigación y análisis, sus habilidades y su experiencia en hacking ético, y su conocimiento en sistemas y redes informáticas, entre otras muchas cualidades, proporciona valiosos conocimientos en la investigación del incidente. Además, en calidad de perito, su informe o pericia resultado de su investigación, puede ser presentada ante un tribunal en el supuesto que el incidente termine en los tribunales, o puede utilizarse como prueba del ataque o incidente en la denuncia presentada ante las autoridades.

Otro aspecto relevante, desde el punto de vista penal y criminal, es la indudable existencia en cualquier investigación policial de un componente tecnológico y el "rastro" que éste deja –huella digital-. La gran cantidad de delitos colapsa el sistema policial y jurídico del país. Para agilizar y mejorar los procedimientos jurídicos, se contratan los servicios de expertos tecnológicos privados, provocando un aumento de la demanda de profesionales -peritos informáticos forenses- con capacidades técnico- legales en el desarrollo de informes periciales que aporten evidencias digitales válidas.

Por otro lado, los gobiernos, en su apuesta de implantar la administración electrónica, y ante el riesgo de ciberamenazas que esto acarrea, están implantando medidas de seguridad que permitan proteger la confidencialidad de los datos personales de los ciudadanos.

Otras ciberamenazas emergentes como las relativas al uso de soluciones basadas en la "nube" –de bajo coste y utilizadas por la mayoría de PYMES-, el uso de dispositivos móviles, la inclusión del Internet de las cosas, la difusión de empresas en prácticas BYOD6 (Bring Your Own Device), y la aparición de amenazas persistentes (APT), están abriendo grandes oportunidades laborales en el mercado de la seguridad.

Sectores críticos como el aeroespacial, la defensa, la banca, la administración pública, la inteligencia y las industrias, coinciden que la ciberseguridad es una de sus principales preocupaciones de este siglo XXI.

Si a lo comentado en párrafos anteriores, le sumamos el aprovechamiento tecnológico y sofisticación de las técnicas y tácticas utilizadas por los cibercriminales, el interés económico o terrorista que les motiva y la difícil atribución del delito informático, es patente la incapacidad de gobiernos, departamentos de las TI (Tecnologías de la Información) y profesionales para garantizar la seguridad global del ciberespacio.

Principales riesgos en el ciberespacio:

- Seguridad en Internet de las cosas
- Seguridad en Smart Grid
- Seguridad en infraestructuras críticas
- Seguridad en dispositivos móviles, BYOD
- Crime-as-a-service
- Ciberespionaje y Ciberguerra
- Malware
- Hacktivismo
- Estafas
- Ataques contra el punto de venta

A fin de contrarrestar los riesgos, algunas medidas tomadas por empresas y Estados son las siguientes:

- Security as a Service
- Big Data Analytics
- Seguridad en movilidad: MDM y MAM
- Servicios de Seguridad Gestionada (MSS)
- Autenticación mejorada
- Simulación de incidentes de ciberseguridad
- Hacking ético

MEDIDAS DE SEGURIDAD INFORMÁTICA

- Asegurar que todo Software instalado sea legalmente adquirido.
- Instalar programas antivirus.
- Colocar Hardware y Software cortafuegos o firewalls para bloquear el acceso a usuarios no autorizados que puedan intentar intrusiones maliciosas.
- Usar claves y contraseñas de alta seguridad (que contengan letras, números y caracteres especiales).
- Hacer uso de la encriptación en toda aquella información que requiera mantenerse segura y secreta.

TODAS ESTAS MEDIDAS SON DE CARÁCTER PREVENTIVO. La mayoría de estas medidas son fáciles de implementar y, aunque algunas tengan costos, éstos son menores a las pérdidas de datos e información que se puedan tener.

Áreas que cubre la seguridad informática

AUTENTICACIÓN: para garantizar que el intercambio de información sea con la/s persona/s correcta/s.

CONFIDENCIALIDAD: para asegurar que sólo las personas autorizadas tienen acceso a los recursos informáticos, incluyendo datos e información.

DISPONIBILIDAD: para garantizar que los datos estarán disponibles cuando los usuarios los necesiten.

INTEGRIDAD: para asegurar que solamente las personas autorizadas puedan modificar los datos cuando sea necesario.

Fortalezas en seguridad informática

FORMACIÓN: es importante tener conocimiento acerca de las medidas de seguridad informática para poder aplicarlas efectiva y eficazmente.

SOLUCIONES DE SEGURIDAD: como todos podemos ser victimas, hay que asegurarse de poseer soluciones para reaccionar convenientemente.

ACTUALIZACIONES: identificar amenazas, tomar acciones y corregir a tiempo es posible, si el plan de respuesta ante incidentes está actualizado.

Los ataques más utilizados en contra de un sistema informático son los troyanos, los gusanos y la suplantación y espionaje a través de redes sociales.

Seguridad de la información, Ciberseguridad y Seguridad Informática

Muchas veces, estos términos son utilizados como sinónimos, pero lo cierto es que eso no es del todo correcto. La principal diferencia entre CIBERSEGURIDAD y SEGURIDAD DE LA INFORMACIÓN se encuentra en el alcance.

La **SEGURIDAD DE LA INFORMACIÓN** tiene un alcance mayor que la CIBERSEGURIDAD: la primera busca proteger a la información de riesgos que puedan afectarla, en sus diferentes formas y estados. Por el contrario, la ciberseguridad se enfoca principalmente en la información en formato digital y los sistemas interconectados que la procesan, almacenan o transmiten, por lo que tiene un mayor acercamiento con la SEGURIDAD INFORMÁTICA. Además, la SEGURIDAD DE LA INFORMACIÓN se sustenta en metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, que soportan la idea de protección en las distintas facetas de la información. Hace referencia a la protección de la información en todo tipo de medios, no importa que sean digitales, físicos u otro medio, por lo que se basa en protegerla de cualquier tipo de riesgo, ya sea de un ataque informático o de un incendio, por ejemplo.

La **CIBERSEGURIDAD** se encarga del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas que se encuentran interconectados a la red. Es decir, es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.

SEGURIDAD INFORMÁTICA: conjunto de procesos, técnicas y herramientas para la protección de los sistemas informáticos (redes e infraestructura) y la información en formato digital, es decir, los sistemas que no están conectados a la red y aun así pueden sufrir amenazas.

TEORÍA DEL DELITO

Es aquella parte del derecho penal que enumera las características generales o presupuestos que debe tener una acción para ser considerada delito (todos los delitos deben tener esas mismas características o elementos).

La teoría del delito sirve para facilitarle al juez, fiscal, defensor, etc. la tarea de determinar si la acción en cuestión es delito o no. Una vez que se comprueba que dicha conducta tiene esas características básicas (es decir que ya se sabe que es un delito) se deberá analizar de qué delito en particular se trata (robo, hurto, violación, etc.) a través del análisis de las características específicas de dicha acción.

Como dice Zaffaroni, "la teoría del delito es la facilitación de la averiguación de la presencia o ausencia del delito en cada caso concreto".

Clasificación de las modalidades del delito:

1) Acción y omisión:- Es de acción cuando la norma pena realizar una determinada conducta y el actor la realiza (ej: "al que matare a otro" y el actor mató). - Es de omisión cuando la norma pena el no realizar determinada conducta y el actor omite realizarla (ej: "omitiere prestarle auxilio.." y el actor no ayudó).

2) Dolosos y culposos:- Es doloso cuando el autor tuvo la finalidad de realizar la conducta típica (ej: mató queriendo hacerlo). - Es culposo cuando pese a no tener la intención de cometer la conducta típica, la realizó por falta de cuidado (ej: mató por imprudencia, negligencia o impericia).

3) Consumados y tentativa:- Son consumados aquellos en donde el autor realizó todos los elementos del tipo objetivo (ej: si el autor mató a la víctima, el delito consumado es homicidio). - La tentativa es la conducta de quien, queriendo cometer un delito, comienza a ejecutarlo pero no lo puede terminar (consumar) por causas ajenas a su voluntad. En la tentativa la escala de las penas disminuye entre un tercio y la mitad, de reclusión perpetua a reclusión entre 15 y 20 años, de prisión perpetua a prisión de 15 a 10 años, etc.

4) Autoría y participación.-Cuando los delitos son cometidos por una sola persona (autor) o por varios, en este último caso pueden existir coautores y partícipes cómplices o partícipes instigadores.

El profesor Hilgendorf define al dolo como la voluntad de realizar un tipo penal, en conocimiento de todas sus circunstancias de hecho objetivas. El autor actúa con dolo eventual cuando reconoce como posible y no totalmente remota la realización

del tipo y la asume aprobándola. Hay imprudencia consciente cuando el autor confía seriamente en que la realización del tipo legal no se producirá. Delito y hecho punible son sinónimos

DELITO: Es la conducta típica antijurídica y culpable. Este concepto toma en cuenta primero a la conducta (que sea típica y antijurídica) y luego a su autor (que sea reprochable su proceder).

- Acción: se refiere a una acción u omisión que realiza una persona en busca de una finalidad.
- Típica: es una conducta tipificada por la ley.
- Antijurídica: esa conducta es contraria a las disposiciones legales.
- Culpable: porque la acción u omisión realizada encuadra en las conductas no deseadas.

De esta forma, las preguntas que debemos hacernos son:

1) ¿Hubo conducta? si no hubo, no se hacen más preguntas.

2) Si hubo conducta, ¿es típica o no? si la conducta no es típica, no se hacen más preguntas.

3) Si la conducta es típica, ¿es antijurídica (es decir, es contraria a derecho o hubo alguna causa que justifica esa conducta)? si la conducta típica no es antijurídica, no se hacen más preguntas.

4) Si la conducta es típica y antijurídica, ¿se le puede reprochar a su autor (es culpable de esa conducta)? si la conducta es típica y antijurídica pero su autor no es culpable, no habrá delito (es lo que se llama injusto penal).

Si la conducta es típica, antijurídica y culpable, habrá delito

DELITOS INFORMÁTICOS

AMENAZAS

El art. 149 bis del código penal, que establece: "Sera reprimido con prisión de seis meses a dos años hiciere uso de amenazas para alarmar o amedrentar a una o más personas. en este caso la pena será de uno a tres años de prisión "Será reprimido con prisión de seis meses a dos años si se emplearen armas o si las amenazas fueran anónimas." "Será reprimido con prisión o reclusión de dos a cuatro años el que hiciere uso de amenazas con el propósito de obligar a otro a hacer, no hacer o tolerar algo contra su voluntad."

GROOMING (LEY 26904):

No cualquier contacto virtual con un menor de edad configura este delito, sino solo aquel que se realiza con la finalidad específica de cometer un delito contra la integridad sexual del mismo.

Es un delito que consiste en el acoso sexual y virtual a niños y adolescentes por parte de un adulto. El acosador simula ser un niño o niña a través de un perfil falso para establecer una conexión y control emocional con el fin de disminuir las inhibiciones de los chicos. A través de distintas técnicas de manipulación, el adulto consigue que el niño se desnude o realice actos de naturaleza sexual.

LEY 26.904 de Grooming, que incorpora el art. 131 del Código Penal que pena con prisión de 6 meses a 4 años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma. La figura del art. 131 es sin duda un acto preparatorio de la comisión de un delito contra la integridad sexual (abuso sexual, estupro, pornografía infantil, exhibiciones obscenas, rapto, etc.). Para que el art. 131 se aplique es necesario que esos delitos no se hayan consumado, porque en ese caso el delito consumado desplazará al art. 131.

La acción típica consiste en "contactar", es decir, tomar contacto, entablar una conexión personal a través de cualquier medio de comunicación. Se trata de un contacto virtual, no de un contacto corporal.

La forma de hacer contacto debe ser por un medio de comunicación electrónica, o de telecomunicación o de cualquier otra tecnología que utilice la transmisión de datos. Ej: entablar contacto usando computadoras, celulares, tablets, que permitan enviar mensajes, chatear, recibir o enviar fotos, etc.

El elemento subjetivo, la intención del actor es esencial: se contacta con el menor con la finalidad de cometer cualquier delito contra la integridad sexual del mismo. Es un delito doloso. La imprudencia o negligencia no encuadran en la figura.

Sujeto activo: debe tratarse de una persona mayor de edad, sea del sexo masculino o femenino. Es indiferente que el autor haya ocultado o no su sexo o edad.

La víctima: debe ser un menor de edad, de cualquier sexo. Se aplica a todos los menores, sin hacer distinción -como en otros delitos contra la integridad sexual- acerca de si la víctima es o no menor de 13 años.

La pena es de 6 meses a 4 años. resulta criticable que en algunos casos corresponde la misma pena (de 6 meses a 4 años de prisión) para quien contacta al menor que para quien efectivamente consumó el abuso. (Ej: abuso sexual simple contra un menor -art. 119 1ra parte-, exhibiciones obscenas -art. 129, 2do párrafo-)

Leyes relacionadas: Ley 27.590 "Mica Ortega" (16/12/2020).

PHISHING.

El phishing es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias.

DELITOS CONTRA LA PROPIEDAD INTELECTUAL (LEY 11723 ART 71, 72 Y LEY 25036)

Definimos como propiedad intelectual cualquier creación de la mente humana sujeto a explotación económica por parte de los poseedores legales de dicha propiedad. Son propiedad intelectual: los inventos, las obras literarias y artísticas, los símbolos, los nombres, las imágenes, los dibujos y modelos utilizados en el comercio.

DELITOS CONTRA LOS DOCUMENTOS (LEY 25506 DE FIRMA DIGITAL)

La falsificación de un documento puede consistir en una falsedad material: cuando se falsifican -se imitan- las formas del documento verdadero o en una falsedad ideológica: cuando la forma del documento es auténtica, pero lo falso es el contenido, lo que dice el documento.

El documento puede definirse como "todo escrito fijado sobre un medio idóneo, debido a un autor determinado, que contenga manifestaciones o declaraciones de voluntad o atestaciones de verdad, destinadas a fundar o a abonar una pretensión jurídica, o a probar un hecho jurídico trascendente, en una relación procesal o en otra vinculación jurídica" (conf. oderigo, Gómez y manzini).

Esas manifestaciones o declaraciones de voluntad, expresadas a través de un lenguaje, constituyen el contenido del documento y es lo que lo caracteriza como tal, distinguiéndolo de los instrumentos vistos en el Capítulo anterior (monedas, títulos, sellos, timbres y marcas).

Documento público: es el otorgado con las formalidades que la ley establece en presencia de un oficial público al cual la ley le confiere facultades para autorizarlo. La característica fundamental de los instrumentos públicos es que ellos se celebran en presencia de un oficial público. La intervención del oficial público otorga al acto seriedad y seguridad pública y da fe acerca del contenido del instrumento. El Código Civil y Comercial los enuncia en el art. 289.

Art. 289 (CCCN).- "Enunciación. Son instrumentos públicos:

a) las escrituras públicas y sus copias o testimonios;

b) los instrumentos que extienden los escribanos o los funcionarios públicos con los requisitos que establecen las leyes;

c) los títulos emitidos por el Estado nacional, provincial o la Ciudad Autónoma de Buenos Aires, conforme a las leyes que autorizan su emisión."

Esta enumeración no es taxativa, ya que también existen otros instrumentos públicos, por ejemplo: las cédulas de identidad, las actas policiales, los certificados de transferencia de automotores, etc.

Documentos privados: son aquellos que las partes otorgan privadamente, sin que medie intervención de un oficial público. Respecto de ellos, rige el principio de la libertad de formas: las partes pueden otorgarlos en la forma que crean más conveniente y sólo un requisito limita esa libertad; dicho requisito es la exigencia de la firma, lo cual constituye un elemento esencial en este tipo de documento.

El mundo de la informática con sus avances tecnológicos nos trajo una nueva clase de documentos: "los documentos informáticos, electrónicos o digitales" cuya existencia jurídica es hoy aceptada por la doctrina y la legislación.

La Ley 25.506 de Firma digital define al "documento digital" como la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura. (conf. art. 6 de la ley 25.506).

Y el C.Penal en el art. 77 dice: "El término 'documento' comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos 'instrumento privado' y 'certificado' comprenden el documento digital firmado digitalmente". (C.Penal, art. 77 conf. Ley 26.388).

La firma digital permite saber si un documento digital es auténtico y no fue alterado, y nos permite saber que un documento digital corresponde a una persona determinada. Una serie de operaciones matemáticas hacen que esa firma sea única, auténtica y pueda ser verificada por la persona que recibe el documento.

DELITOS CONTRA LOS DATOS PERSONALES (LEY 25326)

Definimos como datos personales a la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables (conf. art. 2, ley 25.326 de Protección de los datos personales).

Archivo, registro, base o banco de datos: indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso (conf. art. 2, ley 25.326).

Art. 157 bis.- (Conf. Ley 26.388 – Ley de Delitos Informáticos).- "Será reprimido con la pena de prisión de un mes a dos años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

De estas definiciones surge que la base de datos puede estar contenida o registrada tanto en soportes de alta tecnología informática o electrónica (como ser, discos rígidos de computadoras, dvd, videos, etc.), como en soportes clásicos (tales como, libros, carpetas, fichas, expedientes, legajos, etc.).

Conforme a la ley 26.388, los nuevos tipos penales del art. 157 bis son:

- Acceso ilegítimo a un banco de datos personales. - La acción consiste en "acceder" (entrar, penetrar, meterse) a un banco de datos personales.

- Revelación ilegítima de información registrada en un banco de datos personales.- La acción consiste en "proporcionar o revelar a otro" información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

- Inserción ilegítima de datos en un archivo de datos personales, - La acción consiste en "insertar o hacer insertar" datos en un archivo de datos personales.

Subjetivamente se trata de conductas dolosas, ya que la ley dice "a sabiendas". El autor debe saber que, al acceder, revelar o insertar datos lo hace ilegítimamente (sin tener derecho a ello) y que, según el caso, está violando sistemas de seguridad y confidencialidad de datos, o está revelando información que debía preservar, o está agregando datos sin tener derecho a hacerlo. El sujeto activo puede ser cualquier persona, pero si fuese un funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años. El sujeto pasivo es el propietario o titular de la base de datos.

ACCESO ILEGÍTIMO A DATOS O SISTEMAS Y DAÑOS INFORMÁTICOS

HACKING: acceso ilegítimo a un sistema o dato informático de acceso restringido.

Hacking es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

CRACKING: daño, alteración o destrucción de datos, programas o sistemas

Tiene dos definiciones, según se hable de seguridad informática o de crackeo de programas. En el caso de seguridad informática es el permanente intento de violación de seguridad de los sistemas informáticos, con fines justificados o no. En el caso de crackeo de programas la definición es la de creador de cracks, iteralmente romper, que son programitas destinados a la desprotección de programas comerciales para que puedan ser usados sin límite

Violación de comunicaciones electrónicas

CÓDIGO PENAL DE LA NACIÓN ARGENTINA, art. 153 (violación de comunicaciones electrónicas ajenas), art. 155 (violación de la privacidad de las comunicaciones electrónicas) y art. 197 (interrupción de comunicaciones electrónicas).

Estafas y defraudaciones informáticas

CÓDIGO PENAL DE LA NACIÓN ARGENTINA, art. 172 y 173, inc. 3, 8 y 16 (defraudación mutilando y ocultando expedientes o documentos digitales o manipulando el normal funcionamiento de un sistema informático o la transmisión de datos).

El Inc. 16). (conf. Ley 26.388).- El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

El fraude informático se logra mediante "cualquier técnica de manipulación informática" (ej: introduciendo elementos materiales en el aparato que contiene el sistema o introduciendo programas tipo virus, gusanos, bombas cronológicas, etc.) que altere (modifique la función normal) el normal funcionamiento de un sistema informático o la transmisión de datos.

Estos delitos cometidos manipulando un sistema informático (tal el caso de un "cajero automático") dieron lugar a opiniones y fallos contrarios. Para muchos se trataba de un hurto (art. 162) y no de una estafa (art. 172) porque en estos casos estaban ausentes las notas típicas de la estafa al no existir error que determinara a la víctima a realizar una disposición patrimonial que lo perjudicara, ya que el engaño no lo sufría la víctima sino la máquina (C.N.Crim. y Correc. Sala I, JA 1998 t 4 p. 459).

La ley 26.388 despejó las dudas sobre que delito era al ubicarlo como un caso especial de estafa o defraudación.

Seguridad en Entidades Financieras

COMUNICACION "B" 9042 del Banco Central de la República Argentina (BCRA), relativa a los requisitos mínimos de gestión, implementación y control de los riesgos relacionados con Tecnología Informática y Sistemas de información y recursos asociados para las entidades financieras.

EL TRABAJO PERICIAL

El uso fraudulento de Internet y de las Nuevas Tecnologías de la Información y la Comunicación (TIC) ha elevado la cantidad de delitos informáticos como el *hacking*, el *phishing*, el *pharming*, el acoso a través de las redes sociales, el fraude-online o la pornografía infantil. Hoy en día prácticamente todas las formas de delincuencia tienen un componente tecnológico digital que puede ser usado como prueba – evidencia digital- ante un proceso judicial. Esto obliga a gobiernos, empresas, abogados, jueces y cuerpos de seguridad del estado solicitar los servicios de peritos informáticos forenses. Esta demanda proporciona una interesante salida laboral para universitarios y profesionales en Informática.

De la mano del avance tecnológico, es necesario y primordial que los gobiernos adapten su marco legal y jurídico a las nuevas actividades delictivas, elaboren normas, y firmen acuerdos internacionales para combatir el Cibercrimen organizado.

Por otro lado, los peritos tienen que conocer las últimas herramientas y metodologías en análisis forense informático, y estar al día en seguridad informática, delitos cibernéticos y ciberseguridad. Además de ser expertos informáticos, por la importancia de sus dictámenes periciales, y su vinculación con el 'mundo' jurídico, han de conocer la legislación vigente y su responsabilidad civil, penal y profesional en la investigación y dictamen pericial. El profesionalismo, la ética y la deontología son pilar fundamental para un buen perito informático.

En este contexto**, la finalidad de este trabajo es ofrecer un documento de referencia actualizado, de carácter general y práctico, con los aspectos técnico-legales que el futuro perito informático forense debe conocer, y brindar una mirada introductoria a la tecnología *hardware* y *software* utilizada en la investigación forense digital, mediante un caso práctico completo, donde la evidencia digital es la protagonista del proceso que finaliza con el dictamen o informe pericial**.

EL PERITO INFORMÁTICO

Se define **perito informático** como "*Un profesional experto y titulado, dotado de conocimientos legales, teóricos y prácticos especializados en informática y tecnologías de la información, capaz de asesorar o elevar un dictamen comprensible y a la vez técnico sobre un litigio o cualquier otra situación que se le requiera*" (del Peso Navarro, 2001).

Respecto a sus ámbitos de actuación estos se agrupan básicamente en dos, aquellos que tienen carácter judicial y los que no son requeridos por un tribunal, los extrajudiciales. Aunque el resultado de sus dictámenes, así como el propio procedimiento de investigación y análisis, no deben estar condicionados a esta situación. Por esto, el perito debe realizar su labor profesional al margen de si ha sido requerido por acto judicial como si no. Este aspecto es una cualidad que diferencia al "buen" perito informático.

De forma generalizada **el perito informático en el desempeño de su labor tiene como objetivos**:

- el desarrollo de un informe pericial -tasación, estudio, auditoria, dictamen forense- tanto en el ámbito judicial como extrajudicial
- el desarrollo de una actividad particular de consultoría, asesoramiento, mediación y arbitraje solicitada por empresas u organismos privados.

Las áreas de conocimiento de un perito informático son extensas y requieren de una constante actualización tanto en aspectos tecnológicos y metodológicos como legales. Por ello, el perito informático forense, debe ser consciente de sus limitaciones profesionales, -es imposible ser experto en todas las ramas y especialidades- y recurrir a equipos de peritos, en caso de necesidad, para abarcar todas las áreas de especialización. No basta con poseer los conocimientos

técnicos, legales y prácticos, sino que debe garantizar que el resultado de su trabajo sea objetivo, metódico, demostrable, reproducible, veraz, auditable, creíble, honesto y profesional.

En el ámbito penal y criminal, el fin en toda investigación policial, es poner a los delincuentes y criminales en manos de la justicia. Para ello, es importante que el perito informático forense proceda de acuerdo a derecho, aplicando técnicas y métodos que garanticen la autenticidad e integridad de la información procesada para que esta sea válida ante un tribunal.

Por lo expuesto anteriormente, es relevante conocer en que ámbito se desarrolla la labor de un perito informático forense y ser conscientes del grado de responsabilidad legal que tiene en el procedimiento de la causa.

Ámbitos de actuación del perito informático

La mayoría de demandas de peritaciones informáticas se desarrollaban dentro del ámbito particular o empresarial, pero cada vez más, la figura del perito informático forense es requerida como auxiliar de la justicia para el dictamen de evidencias tecnológicas que faciliten al juez el esclarecimiento de un litigio.

Por otro lado, sus conocimientos de análisis forense digital son demandados por empresas, organizaciones y gobiernos para fortalecer la seguridad informática, y del resultado de su investigación ante un ciberataque, determinar las medidas de respuesta y nuevas políticas de seguridad a implantar.

Apuntar, que los especialistas en ciberseguridad requieren de conocimientos, entre otros, de análisis forense, análisis de malware, análisis y evaluación de vulnerabilidades, gestión de incidentes, manejo de herramientas hacking ético, auditoria de redes; áreas todas ellas con competencias del perito informático forense.

1) ***ÁMBITO JUDICIAL***

   El perito informático judicial, es aquel perito informático que desarrolla su labor dentro de un procedimiento judicial sea penal o criminal. Puede ser designado por cualquiera de las partes o a petición del tribunal. **Cuando un perito informático forense es nombrado por un magistrado o un juez, se transforma en auxiliar de la justicia y debe realizar la función pública según el cargo conferido y de acuerdo a derech**o.

   En el ámbito judicial, el perito informático forense, es un experto designado por la autoridad del proceso judicial, para que mediante investigación especializada en materia informática en base a los requerimientos exigidos, dictamine con objetividad, honestidad, imparcialidad y veracidad, las conclusiones de su pericia mediante un informe o dictamen pericial.

   El resultado de su investigación es aportado en función de la localización de las evidencias digitales, las herramientas utilizadas para el análisis forense, los métodos y normas aplicadas y su desempeño como experto en la materia encomendada.

   La administración de justicia y abogados, están comprobando lo expeditivo e infalible que resulta la localización de las evidencias digitales, que sirven de apoyo para el esclarecimiento de los casos, por lo que contar con un perito informático forense puede ser vital para evitar o imputar una condena.

   Además, al perito informático judicial se le exigen ciertas cualidades adecuadas para su correcta función, entre ellas su neutralidad hacia las partes. Y poseer un perfil técnico en análisis forense digital, con conocimientos legales suficientes que le permitan ejercer ante los tribunales de modo que su labor no sea impugnada o descalificada por la parte contraria.

   Hay que tener en cuenta que este documento servirá como asesoramiento a los abogados en el momento de aportar la prueba ante un tribunal, de manera que el principal objetivo del informe o dictamen pericial será la reproducción exacta de lo requerido. Por tanto, el perito informático judicial deberá recopilar la información que es puesta a su disposición –pruebas originales-, analizar la misma en busca de los datos –evidencias- que el juez le ha requerido y formular un informe o dictamen pericial donde se reflejen las conclusiones de la investigación realizada.

2) <u>ÁMBITO EXTRAJUDICIAL</u>

La peritación extrajudicial surge de las relaciones entre empresas, profesionales y particulares en situaciones en las que se requiere a un experto en la materia en cuestión, garantizando una visión objetiva, imparcial y experta en la investigación. Es posible que el informe pericial aportado por el perito sea utilizado como prueba en un futuro procedimiento judicial. Por norma general, el perito es solicitado para casos de arbitraje y de mediación.

Los casos de **Arbitraje** se ejercen con el fin de evitar juicios en los tribunales, siempre que no se haya infringido la ley. Serán los árbitros quienes tomen las decisiones e informen ante cuestiones litigiosas surgidas o que puedan surgir en una materia. Este arbitro independiente –perito- debe tratar a las partes con igualdad y garantizar los derechos de las partes en litigio. El proceso arbitral es más flexible que el judicial llegando incluso a llevarse a cabo por escrito sin necesidad de parte oral, según las reglas del arbitraje que se elijan.

La **Mediación** es un proceso voluntario en el que dos o más partes involucradas en un conflicto trabajan con un profesional imparcial, el mediador, para generar sus propias soluciones para resolver sus diferencias.

A diferencia de un juez, o un árbitro cuyas decisiones obligan a las partes, e implican que una parte gana y la otra pierde, la mediación busca obtener una solución válida para ambas partes.

La mediación es una forma flexible de resolución de conflictos, que permite a las partes en disputa una solución previa a lo que hubiera constituido un litigio. La mediación ofrece a las partes una oportunidad de ganar una mayor comprensión de su conflicto, y disminuir el coste (tanto en tiempo como en dinero) que implica un procedimiento legal completo.

Deberes del perito informático

- Ser objetivo y ajeno completamente al proceso en el cual se le requiere o se presenta su participación.
- Ser una persona imparcial y sin intereses particulares.
- Poseer los conocimientos, la experiencia y la formación teórico-práctica como experto en la materia.
- Rechazar cualquier proceso que le sea imputado por coacción y no pueda ejercer de manera voluntaria.
- Aceptar el cargo que le es asignado, colaborar con los asesores jurídicos y el resto de los peritos o consultores técnicos y declarar ante el juez en el caso de que este lo requiera.
- Fundamentar sus conclusiones técnicas, expresando claramente los elementos analizados y las técnicas utilizadas para llegar a las mismas.
- Respetar el código de ética que le impone su profesión.

El informe pericial

El valor del trabajo realizado en una investigación de análisis forense digital reside en la documentación que se entrega como resultado de todo el proceso, el informe pericial, siendo este el principal elemento de juicio respecto de la labor del perito informático forense.

A la hora de afrontar el desarrollo de un informe pericial hay que tener en cuenta que:

- El objetivo es transmitir información objetiva y clara, con la mínima carga de términos técnicos, pero sin desestimar aquellos datos técnicos que puedan producir una pérdida de rigor en la información presentada.
- Es necesario dejar constancia de la condición de imparcialidad del perito.
- Posiblemente, el receptor del informe no sea un experto en la materia, y por tanto, el informe debe ser redactado utilizando métodos pedagógicos que faciliten su comprensión.
- No debe parecer que sea una demostración de las habilidades y capacidades técnicas del perito.
- El informe debe dar respuesta a las cuestiones planteadas en el inicio de la investigación.
- No debe contener otra información que no sean los resultados objetivos obtenidos durante la investigación.
- Debe presentar una línea maestra bien definida.

- Los objetivos iniciales deben estar alineados con el desarrollo del informe.
- No puede presentar cuestiones no resueltas adecuadamente.
- La información recabada debe de justificar cuestiones relativas a la resolución del caso.
- El informe debe seguir una estructura documental claramente definida.

Informática forense digital

La Informática forense digital es la disciplina, dentro de la seguridad informática, encargada de la identificación, preservación, análisis, interpretación y presentación de evidencias digitales. Nos permite detallar, validar y sustentar las hipótesis que sobre un evento se formulen.

El análisis forense informático, se podría decir que es "***la forma de aplicar los conceptos, estrategias y procedimientos de la criminalística a la tecnología digital, con el fin de apoyar a la justicia en su lucha contra la delincuencia y el crimen, o como recurso especializado en esclarecimiento de incidentes de seguridad informática***".

En concreto, análisis forense digital es la aplicación de la tecnología informática a una cuestión de derecho en la que las pruebas –evidencias digitales - incluyen, información digital, creada por los individuos y la generada por los propios dispositivos –*logs*, *caché*, temporales, etc.- como resultado de la interacción con el individuo u otros elementos.

Es importante ser meticuloso y cuidadoso en todo el proceso de análisis para que las evidencias no se alteren o contaminen.

El proceso de análisis forense ante incidentes de seguridad, básicamente y de forma general, intenta dar respuesta a cuestiones como:

- ¿qué investigar? … tipo de delito. pruebas a buscar …
- ¿dónde? … sistemas, redes, ordenador, móvil, etc
- ¿cuándo se cometió el delito? … fecha y hora local / UTC
- ¿por qué? … el fin buscado

✓ ¿Quién o quiénes son los autores? tarea difícil en el mundo virtual

✓ ¿Cómo se llevó a cabo? … importantes aspectos de resiliencia.

Fases del análisis forense digital

Dentro de procedimiento del análisis forense digital, se pueden destacar las siguientes fases:

- Identificación del incidente.
- Recopilación de evidencias.
- Preservación de la evidencia.
- Análisis de la evidencia.
- Documentación y presentación de los resultados.

La presentación del informe o dictamen tiene que ser de fácil comprensión, donde se detalle objetivamente las conclusiones obtenidas y se explique claramente el proceso de obtención de las evidencias. No realizar juicios de valor ni afirmaciones que no se puedan demostrar.

La evidencia digital

La evidencia digital es: "*cualquier información digital, que sujeta a la intervención humana u otra semejante, ha sido extraída de un medio informático*". En términos generales, evidencia digital, se puede utilizar para describir "*cualquier registro generado por o almacenado en un sistema informático o dispositivo digital que pueda ser utilizado como prueba en un proceso legal*".

Las evidencias deben ser:

- Auténticas: Para ello se debe poder demostrar que no han sufrido ningún cambio. Mediante obtención de *hashes* se puede asegurar su integridad. Se verá más adelante en qué consiste esta técnica.
- Creíbles: Se puedan entender y comprender fácilmente.
- Completas: Desde el punto de vista objetivo y técnico de la prueba a la que representa. Dejando de lado perjuicios o valoraciones personales.
- Confiables: Las técnicas para su obtención no pueden generar dudas sobre su autenticidad y veracidad.
- Admisibles: Desde el punto de vista legal.

BIBLIOGRAFÍA

Torres / Neuquén (2022). GE Derecho Penal Parte Especial 2022.

https://www.digital.editorialestudio.com.ar/reader/ge-penal-especial-2022?location=2

Montserrat Andrea (2021). GE Derecho Penal Parte General, enfoque finalista 2021.

https://www.digital.editorialestudio.com.ar/reader/ge-penal-finalista-2021?location=2

Ley 25.326 – Ley de Protección de los datos personales

Ley 11.723 – Ley de Propiedad Intelectual

Ley 26.388 – Ley de Delitos Informáticos

Ley 25.506 – Ley de Firma Digital

Ley 26.904 – Ley de Grooming

Código Penal de la Nación Argentina