Material Imprimible

Curso Ciberdelitos y Derecho Informático

Módulo 1

Contenidos:

- Repaso histórico sobre las condenas de los delitos
- El mundo de la informática y la revolución digital
- Ciencia forense e informática forense
- Delitos informáticos y ciberdelito

Repaso histórico sobre las condenas de los delitos

Es claro que los avances tecnológicos de las últimas décadas han modificado el vivir diario de las personas y de las organizaciones, pero los sistemas de información que han permitido mejorar ostensiblemente los procesos al interior de las organizaciones, son los que, al mismo tiempo, han generado una serie de comportamientos ilícitos. Pero… ¿a qué nos referimos cuando hablamos de comportamientos ilícitos?

Dentro de las ramas del derecho, la penal es considerada una de las más arcaicas, ya que el ser humano tuvo el requerimiento de que quien efectuara un perjuicio a otro tuviera un castigo, con la intención natural de establecimiento de justicia, que en sus inicios fue confundida con el sentimiento de venganza.

Las prohibiciones iniciales a los comportamientos mantuvieron una especie de carácter mágico a partir de los tabúes, cuya infracción traía como consecuencia en general, una sanción colectiva para todos los integrantes de la tribu. Las normas iniciales, que surgían de la costumbre, dejaban a la víctima del ilícito o a sus seres queridos al que pertenecía, la exigencia del castigo, surgiendo a menudo guerras entre tribus, sin mantener proporción entre la pena y el daño efectuado, generándose de este modo la venganza de forma privada, y condenándose con el homicidio delitos considerados leves.

Después de esta etapa de venganza se abrió paso a que sea viable la reparación pecuniaria. Un paso primordial en la erradicación de la venganza de forma privada, o también conocida como justicia por mano propia, se logró a partir de la Ley del Talión: "Ojo por ojo y diente por diente", donde la sanción tenía estrecha relación con la gravedad del delito ilícito efectuado. Como ejemplos antiguos de aceptación de esta proporcionalidad tenemos El Código de Hammurabi en Babilonia, la Ley de las XII Tablas de los romanos y la Ley Hebrea. Es por ello que la pena se va a determinar legalmente y ya no la va a decidir el interesado o sus familiares.

Cuando finaliza la República de Roma, la justicia vira de privada a pública. En la Edad Media, a partir del poder la Iglesia y del Derecho Canónico, los pecados se convalidan con los ilícitos en la práctica. El rey de España Alfonso X, en 1265, decreta penas muy graves, que incluyen la pena de muerte, torturas, el destierro, la confiscación de bienes, trabajar forzadamente, entre otros.

Durante el Siglo XVIII, con el surgimiento de los ideales iluministas, afloran nuevas formas de comprender al derecho penal. En la obra titulada “De los delitos y las penas” del filósofo italiano Cesare Beccaria, se estableció el principio de que las leyes y demás normativas son la únicas que pueden establecer las penas para los ilícitos que enumeran, que deben tener proporcionalidad con la gravedad de estos. Sus ideales más distinguidos son la humanización de los castigos, sugiriendo entre otras medidas, la abolición de la tortura.

Durante la escuela clásica, que tiene sus raíces en la existencia del Derecho Natural, que se encuentra por arriba del Derecho Positivo, se establecen límites y se aspira a hacer más justo al derecho penal. Su máximo exponente es Francesco Carrara, quien en 1859 expuso que el discurso debe fundamentarse sobre las normas legales. Asimismo, Carrara fundamenta la responsabilidad delictiva a partir del libre albedrío, por lo cual establece la inimputabilidad de aquel que no accionó teniendo la posibilidad de elegir.

Durante el siglo XIX, Augusto Comte establece los cimientos del positivismo, que enfocan en los hechos, sin cuestionar sus motivos o justicia. Estos ideales se expusieron en varios contextos, y en el legista, médico y criminólogo italiano Cesare Lombroso, que instauró la teoría del delincuente nato, donde establece que el mismo nace para consumar delitos según ciertos aspectos psíquicos y físicos que mantiene.

A partir de esta teoría de Lombroso, el criminal no es responsable de lo que realiza, ya que no puede evitarlo. Por tal motivo, en vez de puntualizar en el castigo, hay que especificar e implementar medidas de seguridad. Entre estas medidas se encontraban la pena de muerte, ya que se consideraba que en muchos de los casos no era factible la reinserción social y suponían un enorme peligro para la sociedad. Las penas estaban relacionadas fundamentalmente al grado de peligrosidad del criminal, dejando en segundo plano la gravedad del crimen efectuado.

Una vez culminadas las guerras mundiales, surge nuevamente la noción de la utilización del Derecho Natural. En la década de 1960 revive el vínculo entre la pena y la culpabilidad, y de la reinserción y rehabilitación del criminal. Además, aparecen medidas alternativas a la reclusión o prisión, como las labores comunitarias o la prisión

domiciliaria. Sin embargo, en la década de 1970 se retorna a un sistema con más represión debido a la sensación de inseguridad.

Hoy en día se estudia si el endurecimiento de las condenas y la reducción de edad de imputabilidad son medidas idóneas para frenar a la inseguridad, aunque se progresa respecto a la despenalización de hechos particulares que habían sido considerados ilícitos en el pasado, como el adulterio, el consumo de estupefacientes y el aborto.

Si vamos a indagar respecto a los delitos, es el país, y dentro del mismo, el Congreso de la Nación, quien tipifica las acciones que van a ser consideradas delitos y cuáles serán las penas correspondientes sobre estos. Asimismo, mediante el Código Penal, las provincias se encargarán de regular los procedimientos y las formas que deben establecerse para el juzgamiento, a partir de los códigos procesales penales.

Se va a definir al delito como una acción típica, antijurídica, imputable, culpable, que consecuentemente deriva a una sanción penal, y va a suponer una infracción del derecho penal, es decir, una acción u omisión punible tifiada por la ley. Cabe aclarar que no siempre es requerida la producción de un daño para que una conducta pueda tomarse como un delito, ya que además existen los ilícitos denominados “de peligro”. Estos se concretan con la mera realización de la acción prohibida, sin depender del resultado que allí se establezca.

A su vez, los delitos van a tener distintas clasificaciones pertinentes. A partir de las formas de culpabilidad, los delitos pueden clasificarse en:

- Delito culposo, que es el delito que el autor no ha querido realizar. El resultado no es directamente consecuencia de su voluntad, sino por imprudencia, negligencia, impericia o inobservancia de los deberes a su cargo
- El delito doloso es un hecho que el autor quiso efectuar. Hay coincidencia entre lo que el autor hizo y lo que quería hacer, es decir, es un acto voluntario
- Y sobre el delito preterintencional se puede establecer que si bien la conducta corresponde al deseo del autor, el resultado va a exceder esa voluntad. Un

ejemplo claro es cuando en una contienda se desea lesionar a su adversario, pero termina asesinándolo.

En función a la forma de acción, los delitos se clasifican en:

- Delito por omisión, el cual se basa en normas que ordenan hacer algo y se realizan abstenciones. El delito se establece cuando no se lleva a cabo una acción realizada en el momento en que debió efectuarse
- Y delito por comisión, el cual se establece mediante la acción del autor. A diferencia del anterior, la norma prohíbe realizar una determinada acción y el actor la efectúa.

A partir de la forma procesal, se clasifican en:

- Delito de instancia privada, el cual se refiere al que además de la denuncia, el que la realiza debe seguir dando impulso al proceso como querellante
- Delito de acción pública, que es aquel que para su persecución no necesita de denuncia previa
- Y delito dependiente de instancia privada, el cual requiere una denuncia que inicie el proceso, ya que no pueden ser perseguidos de oficio.

Por último, a partir del resultado, los delitos se clasifican en:

- Delito Material, el cual requiere de la generación de determinado resultado. Este está compuesto por la acción, la imputación y el resultado.
- Y delito formal, que es aquel en el cual la realización del tipo concuerda con el último acto de la acción, y por ende, no se genera un resultado disgregable de ella. El tipo se agota cuando se efectúa la acción, y la cuestión de la imputación de carácter objetivo es completamente ajena a estos tipos penales, dado que no tienen relación entre la acción y el resultado.

Cabe mencionar que dentro de la terminología jurídica, en español, las palabras crimen y delito son equivalentes, y que expresiones como “justicia criminal" o "procedimiento

criminal" son usadas con idéntico sentido, así como las palabras “criminal” y “delincuente”.

El mundo de la informática y la revolución digital

De acuerdo con la Organización de las Naciones Unidas, conocida como ONU, la revolución digital en las tecnologías de la información y las comunicaciones, también conocidas como TICS, ha creado una plataforma para el libre flujo de información, ideas y conocimientos en todo el planeta. Internet se ha convertido en un importante recurso, que resulta vital tanto para el mundo desarrollado por su función de herramienta social y comercial, como para el mundo en crecimiento por su función de pasaporte para la participación equitativa y la evolución económica, social y educativa.

Según los autores colombianos Iván Manjarrés y Farid Jiménez, en su escrito titulado “Caracterización de los delitos informáticos en Colombia” expresan que “estas tecnologías nos brindan la libertad para poder movernos y permanecer comunicados y conectados con miles de servicios construidos sobre redes de redes. Nos dan la posibilidad de participar; de enseñar y aprender, de jugar y trabajar juntos, y de intervenir en el proceso político. Pero también estas tecnologías de la información pueden utilizarse, y se utilizan, para perpetrar y facilitar diversas actividades delictivas, convirtiéndose en instrumentos para actividades que ponen en peligro o atentan contra la vida, la propiedad o la dignidad de los individuos o del interés público”.

Por su parte, el término informática proviene del vocablo francés informatique, que surge por parte del ingeniero francés Philippe Dreyfus a inicios de la década de 1960. La palabra es, al mismo tiempo, una abreviatura de information y automatique.

Cuando hablamos de la informática nos referimos al procesamiento automático de información. Podemos describirla como una ciencia que administra técnicas, métodos y procesos, con el objetivo de procesar, almacenar y transmitir datos e información en

formato digital a partir de sistemas computacionales y medios y dispositivos electrónicos.

La informática, además, contempla también los fundamentos esenciales de las ciencias de la computación, como lo son la programación para el desarrollo de software, las redes como el internet, la arquitectura del hardware y de los ordenadores, y la inteligencia artificial. Inclusive es aplicable a varios temas de electrónica.

Esta ciencia supuso una verdadera revolución que se inició culminando los años 70 con las computadoras caseras, pero adquirió más vigor durante los años 80 y terminó de estallar en los 90. Por ende, nos encontramos ante un proceso que llevó alrededor de 20 años florecer en su plenitud.

Sin embargo, es en el siglo XXI cuando se termina de masificar a partir de la conjugación de los tres elementos más relevantes de la informática: internet, los videojuegos y los teléfonos móviles. Sí, los dispositivos portátiles jugaron un papel fundamental en la difícil tarea de convencer a los más escépticos de derribar sus barreras y comenzar a disfrutar de la informática.

Una cuestión a tener en cuenta es que cualquier utilización que realicemos de un programa para automatizar nuestras acciones, puede encasillar dentro de la categoría de informática, independientemente de en qué aparato esté.

A partir de la aparición de los celulares y, más tarde, de las tablets y otros dispositivos electrónicos innovadores, muchos individuos se animaron a insertarse por primera vez en el mundo de la informática, a partir de la creación de las casillas de correo electrónico, de los mensajes de texto y de la redacción de documentos de manera digital, para más adelante adentrarse en el uso de computadoras y finalmente poder hacer uso de la serie de prestaciones que se iban sumando.

En el ámbito laboral, hoy en día la informática es la base de la mayoría de las tareas que se realizan en las empresas, debido a que nos permite controlarlas y organizarlas de una manera más eficiente y organizada que por los medios tradicionales.

Para incursionarnos en la temática, es necesario que aclaremos dos conceptos: datos e información. En la materia, los datos son los símbolos que representan situaciones,

hechos, condiciones o valores, y la información va a ser el resultado de transformar o procesar los datos, lo que va a ser significativo para el usuario.

Podemos decir que la historia y la evolución del delito informático coinciden directamente con la evolución de la informática.

Los primeros delitos efectuados en el mundo cibernético fueron hackeos sencillos para adquirir información de las redes locales, pero a medida que el internet fue tomando lugar, también lo fueron haciendo los ataques sobre el mismo.

La primera masividad de delitos informáticos llegó con la multiplicación de los correos electrónicos para finales de la década de 1980. Esto dio paso a que se lleven a cabo un gran número de fraudes a partir del envío de información maliciosa a la bandeja de entrada. Además, se empezaron a enviar virus a partir de conexiones a internet cuando se ingresaba a sitios web cuestionables. Algunos hacían que tu computadora funcionara de manera más lenta, otros hacían que aparezca publicidad molesta en la pantalla o la redirigiera a los sitios constantemente.

Fue a principios del 2000 cuando esta modalidad delictivita se intensificó notoriamente con el surgimiento de las redes sociales. La gente empezó a poner información personal en bases de datos del perfil, lo que conllevó a gran cantidad de información personal circulando en la red, por lo que, al mismo tiempo, se empezó a realizar robos de identidad. Esta información se utilizaba de varias formas, como por ejemplo, para acceder a cuentas bancarias, crear tarjetas de crédito, entre otros fraudes financieros.

La última ola se da por medio de la utilización de estas herramientas informáticas en el crimen organizado. Allí emplean distintos métodos bien establecidos y apuntan a distintos objetivos relacionados a este medio. Por eso podemos decir que los delitos informáticos contemplan acciones que quebrantan la integridad, la confidencialidad y la disponibilidad de la información, y engloban un amplio espectro de acciones ilícitas de distinta índole.

La evolución de la tecnología informática ha generado nuevas modalidades de delincuencia antes impensadas. A nivel internacional, ha tomado gran importancia el fenómeno de la criminalidad cibernética. Esta actividad está fuertemente vinculada al

crimen organizado, principalmente al narcotráfico, los delitos sexuales, la pornografía infantil, y el tráfico de armas.

Resulta imperioso partir del principio de que la información constituye un valor económico con relevancia jurídico-penal, por ser, por lo dicho anteriormente, un objeto factible de conductas delictivas, como sabotaje o daño informático, acceso no autorizado, espionaje informático, entre otras, y por ser una herramienta de comisión, aseguramiento, facilitación y calificación de los ilícitos considerados tradicionales, llegando a considerarse un bien jurídico protegido, susceptible de protección legal propia y específica del ordenamiento jurídico vigente.

La formación de los legistas y demás trabajadores del derecho, en el contexto del impacto de las tecnologías de la información en la comunidad, manifiesta la necesidad de incorporar modernas y novedosas disciplinas que avalen responder, desde un ámbito interdisciplinario, a las problemáticas y nuevos planteamientos generados día a día por dicha circunstancia.

Por eso podemos manifestar que el Derecho Informático consta del conjunto de principios y normas que reglan los efectos jurídicos que surgen de la informática y de las tecnologías de información y comunicación, también conocidas como TICS.

A partir de esta disciplina, la Ciencia Jurídica analiza los cambios que la informática genera en todos los ámbitos de las personas y sociedades con el objetivo de poder reglarlas idóneamente. Podemos decir que involucra un conjunto de leyes, las cuales van a integrar la política informática, y esta misma puede presentar o no diferencias de la legislación informática.

Estos principios surgen en función de los postulados otorgados por magistrados, jueces, tratadistas y estudiosos respecto a la materia. Además, se relaciona a hechos como consecuencia de un fenómeno aparejado a la informática inimputable al individuo. Asimismo, es importante tener en cuenta que se alude a actos como efecto de un fenómeno.

El último concepto por ver es el de Informática Jurídica, que va a ser la informática puesta al servicio del derecho, para modernizarlo y mejorarlo continuamente. A la vez,

se ramifica en Informática Jurídica de Gestión, Informática Jurídica Documental e Informática Jurídica Decisional.

A grandes rasgos, decimos que la informática jurídica va a abarcar las aplicaciones de la informática en la esfera del derecho. Esta surgió en 1959 en los Estados Unidos, y ha sufrido cambios relacionados a la evolución general de la propia informática.

En términos generales, es válido afirmar que, según el investigador Julio Téllez Valdés, "la informática jurídica es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como a la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación".

La aplicación de derecho informático se puede extender a casos completamente dispares, como lo pueden ser la intimidad, los contratos y la propiedad intelectual.

Sobre la intimidad se puede manifestar que los legistas especializados en informática abordan y contemplan cómo contener de manera segura la información sensible dentro de un planeta donde los datos pueden estar al alcance de cualquiera muy fácilmente.

Estos especialistas auxilian a sus clientes a concretar la mejor opción de asegurar la información del propietario, y además, a partir de la implementación de políticas para protección de empresas, establecen responsabilidades ante el incumplimiento de las mismas. Asimismo, guían a las organizaciones para definir si es factible o no compartir la información particular que recolectan y cuál es la vía para hacerlo de manera legal.

Por su parte, los contratos de compraventa de material informático, hardware, software y entre otras clases de tecnologías, fuera de línea o en la misma, están redactados por legistas especialistas en esta materia, que también ayudan a reglar los vínculos entre empresas e individuos u otros terceros que implementan su sitio web o un software particular. En los últimos años, se ha comenzado a redactar los contratos inteligentes, una clase de acuerdo que, además, está contemplado en la ley de informática mencionada anteriormente.

Por último, acerca de la propiedad intelectual se puede establecer que las empresas generan nuevos productos, estrategias de marketing y trabajos artísticos en función de

realizar negocios por la web. Los profesionales de este campo auxilian a estas organizaciones a proteger su trabajo a fin de que puedan beneficiarse de él. Lo que se hace es solicitar una patente para estas nuevas tecnologías, se registra la marca comercial para uso excluyente de la empresa o persona en cuestión y, de este modo, se protege el uso de sus productos a partir de violaciones de derechos de autor.

Además de estas cuestiones tan habituales que describimos, quienes comprenden qué es el derecho informático y se consagran en esta especialidad, pueden asistir a sus clientes para averiguar cuál es su obligación como propietarios de un sitio web y qué normas de privacidad son de utilización en cada región que operan.

Asimismo, los valores y principios como la igualdad, la equidad, la inclusión, la transparencia, la responsabilidad y la rendición de cuentas, pueden verse afectados notoriamente por distintos avances tecnológicos. Por eso es fundamental hacer una reflexión respecto de esto, debido a la importancia de comprender qué es el derecho informático y cómo puede auxiliarnos diariamente en las operaciones de negocio de forma operativa y positiva.

La ciencia forense y la informática forense

La palabra forense deriva del latín fórum, que significa "lo relativo a los tribunales de justicia". De acá que su concepto sea de la administración de justicia o lo vinculado con la misma.

A partir de la ciencia forense, se van a brindar las técnicas y los principios que auxilian a la investigación delictiva. Entonces, podemos decir, en otras palabras, que las ciencias forenses involucran a todos los principios y técnicas que pueden ser utilizadas para recuperar, identificar, analizar o reconstruir la evidencia durante una investigación criminal.

Un principio fundamental en esta materia es el Principio de Transferencia o Intercambio, del criminalista francés Edmond Locard. Este principio radica en que cualquier objeto que ingresa en la escena del crimen deja un rastro en la escena o en la víctima y

viceversa, es decir, se lleva algo consigo de estos elementos. A partir de aquí surge la frase “cada contacto deja un rastro”.

Un ejemplo concreto podría ser pisar la escena del crimen y dejar algo mío ahí, como por ejemplo, sudor, pelo, huellas, olores, etc. Pero además, llevarse algo al abandonar la escena del crimen, como podría ser olor, barro, una fibra, etc. Con estas evidencias, los peritos podrán demostrar, por ejemplo, que hay una alta posibilidad de que el delincuente estuviera en la escena del crimen.

Existen varios tipos de evidencias físicas:

- La evidencia patrón o curso es generada por el contacto. Podría ser por la trayectoria de una bala, patrones de posicionamiento de muebles, una rotura de un vidrio, entre muchas más.
- La evidencia transitoria, como su nombre lo indica, dura un lapso de tiempo reducido. Algunos ejemplos son la temperatura, un olor, una marca sobre la nieve o la arena, entre otros.
- Por su parte, la evidencia transferida se da habitualmente por contacto entre objetos, entre individuos o entre individuos y objetos
- Por último, la evidencia condicional es ocasionada por un evento particular en la escena del crimen. Como ejemplo se puede citar la posición de una evidencia en relación con el cuerpo, una cerradura forzada, una ventana abierta, una televisión encendida, etc.

A su vez, podemos entender a las evidencias transferidas a partir de dos clases:

- La transferencia por una huella, la cual abarca tanto las huellas dactilares, palmares y plantares, como la huella de calzado
- Y la transferencia por rastro, como son las fibras, el pelo, la sangre, el semen, etc.

Asimismo, las evidencias también pueden ser transferidas de dos maneras distintas:

- La transferencia indirecta es cuando en un principio es transferida a una posición y seguidamente es transferida a otro sitio
- Y la transferencia directa es cuando es transferida desde su origen hacia el destino final, sea objeto o individuo, de forma directa. La relación se llevará a cabo entre los distintos componentes, que son la evidencia física, la víctima, el victimario y la escena de crimen. Para la correcta interpretación del hecho, todos estos elementos deben estar vinculados.

A partir de lo expuesto, podemos resumir el Principio de Locard de la siguiente manera:

- La víctima mantendrá restos del victimario y puede dejar rastros de sí misma en éste
- El victimario se llevará lejos algún rastro de la víctima y de la escena
- El victimario dejará algún rastro en el lugar del hecho.

Entonces podemos concluir que las ciencias forenses otorgan los mecanismos, técnicas y metodologías científicas que pueden ser implementadas para el análisis de la evidencia y para la utilización de la misma en la reconstrucción del hecho con fin de vincular al autor, la escena del crimen y la víctima. Cabe destacar que además del trabajo desarrollado propiamente en el laboratorio, los peritos de las distintas disciplinas forenses actúan en escenas de hechos analizando, adquiriendo e identificando evidencia.

La **informática forense** se va a referir a la ciencia de preservar, adquirir, obtener y presentar datos que fueron procesados electrónicamente y almacenados en un medio computacional. Esta surge a partir de la necesidad de los legistas en poder hacerle frente a nuevas tareas probatorias.

Respecto a los fines que persigue la tarea del informático forense podemos distinguir los siguientes:

- El fin principal es adquirir evidencia digital referida a todo tipo de infracciones vinculadas a los delitos informáticos
- Los fines específicos son perseguir y procesar judicialmente a los delincuentes informáticos, reparar los daños generados por los delincuentes, y establecer medidas con fines de prevención.

Existen diversas utilidades en la implementación de la informática forense. Muchas de estas surgen del día a día, y por ello no tienen que estar estrechamente vinculadas a la informática forense.

- Sobre el usuario final se puede manifestar que cada vez es más habitual que los individuos utilicen el software para encriptar documentos, recuperar archivos borrados y buscar el origen, por ejemplo, de un correo electrónico
- Acerca de la prosecución delictiva se puede establecer que puede utilizarse evidencia digital para procesar gran cantidad de delitos, como lo pueden ser homicidios, tráfico y venta de drogas, fraude financiero, pornografía infantil y evasión de impuestos. Este medio se utiliza cada vez en más variedad de delitos.
- Respecto a la investigación en seguros se puede explicitar que la evidencia hallada en las computadoras puede auxiliar a las compañías de seguros a aminorar los costos de los reclamos por accidentes. Por estos medios es más sencillo la detección de fraudes sobre seguros
- Por su parte, los casos que pueden necesitar del auxilio de la litigación civil son el fraude, el acoso, los divorcios, entre otros.
- En cuanto a los asuntos corporativos, puede ser adquirida información relacionada a acoso sexual, apropiación de información confidencial, robo, espionaje industrial, etc.
- Sobre la investigación científica se puede manifestar que las universidades y distintas instituciones utilizan las herramientas que brinda la informática forense para efectuar estudios de seguridad, observar la evolución de las amenazas, y

además determinar cuáles serán las tendencias de las modalidades delictivas informáticas

- Por último, el sostenimiento de la ley puede ser utilizado en la investigación sobre órdenes judiciales, así como en la búsqueda de información una vez adquirida la orden judicial a razón de realizar una pesquisa intensiva.

El área propia de la informática forense surge en la década de 1980, luego de que los ordenadores personales se vuelvan en una opción factible para los individuos.

En 1984, el FBI crea un programa, conocido en sus inicios como el Programa de Medios Magnéticos, y que actualmente se reconoce como CART, que en español significa análisis de informática y equipo de respuesta. Un tiempo después, Michael Anderson, la persona que se la distingue como padre de la informática forense, empezó a trabajar en esta área a partir del rol que tenía en su profesión, que era la de un agente especial de la División de Investigación Criminal del IRS. Luego, a mediados de los 90, realizó diversas actividades para el gobierno en esta materia, por lo cual fundó New Technologies Inc., un equipo de informática forense.

La informática forense es considerada una herramienta fundamental que toda estructura debe tener en cuenta dentro de sus políticas de seguridad, así como designarla en el proceso de respuesta ante percances en los sistemas informáticos. En las últimas décadas esta ciencia ha manifestado una gran expansión, y las distintas fuerzas de seguridad y armadas siguen manteniendo una presencia notoria en las áreas de informática forense y seguridad de la información.

En cuanto a las empresas de índole privado, han definido en líneas generales la necesidad de contratar de manera directa a profesionales de seguridad de informática forense, o bien requerir de otras empresas especializadas en estos campos. En la última década, además, en el sector privado ha surgido la necesidad de efectuar investigaciones forenses en los conflictos legales de índole civil.

El área de la informática forense sigue creciendo todos los días, aumentando de manera constante los investigadores privados en informática forense, así como las

especializaciones dentro de esta área, que cada vez requiere de conocimientos más amplios.

Las compañías informáticas producen continuamente programas forenses nuevos y más vigorosos de software, y en lo que respecta a las fuerzas de la ley y de seguridad, hay una búsqueda continua de capacitación para su personal, así como de aumentar las investigaciones respecto a los ilícitos vinculados con la tecnología.

Existen distintos roles que pueden llevarse a cabo en las investigaciones:

- Los examinadores de evidencia digital son los responsables de procesar toda la evidencia digital adquirida por los técnicos en las escenas de hechos informáticos. Por eso, para este rol, es necesario mantener un grado elevado de especialización en el campo de informática y sistemas.
- Los técnicos en escenas de hechos con evidencia informática son los responsables de preservar y recolectar las evidencias que se encuentran allí. En necesario que mantengan una formación respecto al manejo de documentación y de evidencia, como también en el criterio de localización y selección de elementos de convicción de las escenas y en reconstrucción del delito.
- Por su parte, el Diccionario de la Real Academia Española define a los peritos con los términos "sabio, experimentado, hábil, práctico en una ciencia o arte". Dentro del ámbito forense, se puede decir que es el que teniendo conocimientos especiales teóricos o prácticos, informa al juez, bajo juramento, respecto a los puntos litigiosos cuando éstos se vinculan con su especialidad o experiencia.

Los peritos son auxiliares de la justicia que, ya sea en el ejercicio de una función pública o en roles privados, son llamados para dictaminar sobre interrogantes de casos que se relacionan a su ciencia, arte o práctica, realizando asesoramientos a los legistas en las materias que no pueden desarrollar en su respectiva competencia.

Es sumamente fundamental para poder valorar las pruebas o los elementos de convicción y la participación de personas que mantengan conocimientos especiales en materias específicas, en este caso, de informática. Asimismo, estos individuos prestan su

saber específico al Fiscal y al Juez a la hora de ilustrar respecto a las técnicas, materias o artes que son de su entendimiento, con el objetivo de que dichos funcionarios, a partir de dichas explicaciones, puedan brindar su criterio en el momento conveniente.

El dictamen o informe elaborado por el perito conforma la llamada prueba pericial, que puede resultar de la aplicación a toda clase de juicios y de distintos fueros. El nombramiento de los peritos puede realizarse a pedido de las partes o de oficio por el juzgador, ya sea para resolver el conflicto entre los peritos de las partes, o porque el juez lo considera necesario para su mejor entendimiento e ilustración del caso respectivo.

También es importante tener en cuenta que son varios los requisitos que debe tener un perito para poder desempeñar su ejercicio. Una de las condiciones de los peritos va a ser la capacidad, la cual se va a referir a la suma de las condiciones subjetivas que le otorgan la aptitud para participar en los distintos procesos. La capacidad va a estar presente cuando se complementen la personalidad física y habilidad testifical de carácter subjetivo.

La cualidad principal de la función del perito consta de la transmisión de conocimiento. Por esta razón, solo pueden desempeñarse en este rol las personas físicas. Si bien es factible que durante el proceso se efectúen consultas a determinadas personas jurídicas, como distintas instituciones o universidades, sus informes no van a contar con valor jurídico de prueba pericial, sino que simplemente se va a limitar a ser una prueba informativa.

En relación de la habilidad subjetiva, no podrán ejercer como peritos quienes no mantengan la aptitud física mental o moral para decir la verdad. Algunos ejemplos de incumplimiento de esta primicia serían los menores de 18 años, los que no tengan habilidad conocida, los que mantengan impedimentos para manifestar sus ideas de palabra o por escrito, los condenados por falso testimonio y los procesados por algún delito.

Con respecto a la legitimidad, esta se establece ante la presencia de tres factores: la competencia técnica, la habilidad objetiva y la impersonalidad procesal.

- La competencia técnica se comprueba con el título habilitante, y se establece cuando la especialidad del perito tiene coincidencia con el saber que es necesario incorporar al caso judicial
- Sobre la habilidad objetiva se puede establecer que el perito debe ejercer con independencia de su opinión personal
- La impersonalidad procesal establece que el perito deber ser un individuo distinto de los sujetos procesales.

Por último, en función con el objeto procesal, no podrán ejercer como peritos los individuos que se encuentren en las siguientes condiciones: secreto profesional, tutela o parentesco, entre otras relaciones objetivas.

Los delitos informáticos y el ciberdelito

Los delitos informáticos son acciones que vulneran la integridad, confidencialidad, y disponibilidad de la información.

A continuación, se enumerarán los ciberdelitos más frecuentes que se cometen a través de programas maliciosos, también denominados malwares, desarrollados para dañar, deteriorar, borrar, hacer inaccesibles, suprimir o alterar datos informáticos sin la autorización del propietario y con fines pecuniarios y de daño.

- El fraude es el acto efectuado de manera deliberada en el que se manipulan datos y se perjudica a personas físicas y jurídicas que de esta manera pueden sufrir una pérdida económica. De esta forma, habitualmente el autor del ilícito consigue un beneficio normalmente pecuniario.
- El sabotaje es la acción por la cual, generalmente, se quiere perjudicar a una empresa obstaculizando deliberadamente su marcha, averiando sus herramientas, programas, equipos, entre otras cosas. En general, el delincuente no logra con ello beneficios pecuniarios, pero entorpece la labor de una organización

- El chantaje es la acción que consta de reclamar una cantidad de dinero a cambio de no dar a conocer información confidencial y que puede tener efectos muy negativos hacia una empresa, principalmente a su imagen corporativa
- Por su parte, la mascarada es el empleo de una clave por un individuo no autorizado y que se introduce al sistema suplantando una identidad. De esta manera, el intruso se hace dueño de la documentación, información y datos de otros usuarios con los que puede realizar una variedad de ilícitos, como por ejemplo, chantajear a la organización.
- El virus es un código diseñado para entrar en un programa, destruir o modificar información, el cual se copia de forma automática a otros programas para seguir su ciclo. Asimismo, es habitual que se expanda a partir de plantillas, archivos ejecutables y macros de aplicaciones
- Los gusanos son virus que se activan y transmiten por medio de la red, y que tiene como objetivo su multiplicación hasta terminar con el espacio en disco o RAM. Este suele ser uno de los ataques que generan más daño, porque habitualmente produce un colapso en la red.
- Por último, el caballo de Troya es un programa que se introduce a la computadora y luego actúa de forma similar a la de este hecho de la mitología griega. Es por esto que parece ser una cosa o programa inofensivo, pero en realidad está realizando otra y expandiéndose.

A su vez, existen ciberdelitos que utilizan la ingeniería social para amenazarte, engañarte y sacarte datos personales e información de otros individuos u organizaciones, sustraerte dinero, acosarte digital y sexualmente, y suplantar tu identidad. Algunos ejemplos son los siguientes:

- En el Phishing, los delincuentes informáticos se hacen pasar por diferentes entidades, como empresas, oficinas de gobierno o conocidos de la persona, y te solicitan los datos que necesitan para suplantar tu identidad y así ingresar a tus cuentas en bancos, redes sociales, servicios y aplicaciones.

- El Ciberbullying se refiere al acoso por distintas redes sociales con la intención de acechar o perseguir a otro individuo, difamarlo, atentar contra su integridad moral, etc. Generalmente la metodología empleada es el descubrimiento y revelación de secretos a partir de la publicación de comentarios o videos discriminatorios, el etiquetado en foros y publicaciones, y la creación de "memes".
- Por otro lado, la Sextorsión consiste en solicitar dinero a cambio de no difundir a través de las redes sociales imágenes que surgieron en un intercambio erótico consentido.
- El Ciberodio se refiere a la violencia, la xenofobia, mensajes que incitan al odio, el racismo y otros tipos de discriminación a partir del empleo de medios cibernéticos. Estos contenidos considerados inapropiados pueden llegar a vulnerar personas
- Por último, la pornografía infantil se refiere a la corrupción de menores de edad y su explotación sexual para producir y comercializar videos e imágenes de actividad sexual

Desde otro punto de vista podemos mencionar al delito informático en función a la violación de la privacidad de los individuos, como por ejemplo:

- Espionaje ilícito sobre las comunicaciones privadas de los habitantes
- Acceso ilegal a las comunicaciones privadas de un empleado, como redes sociales, correos electrónicos, etc.
- Violación a la intimidad por parte de las organizaciones proveedoras de servicios sin el consentimiento del cliente, en función de conocer sus gustos y preferencias y generar la venta de productos y servicios asociados

Existen muchos más delitos de los expuestos anteriormente. Incluso surgirán nuevos ilícitos y ataques a las redes y sistemas informáticos que al día de hoy no sabemos cómo serán ni qué vulnerabilidad atestarán.

Sin embargo, en el año 2008, se incorporó en el Código Penal de la República Argentina la ley 26388 de Delitos Informáticos, la cual tipifica diversos delitos que conoceremos en los siguientes módulos.

Los delitos tipificados en la ley de Delitos Informáticos son:

- Delitos informáticos
- Delitos contra la integridad sexual
- Pornografía infantil
- Violación de secretos y de la privacidad
- Acceso a sistema informático
- Acceso a banco de datos
- Publicación de una comunicación electrónica
- Fraude informático
- Daño informático

Asimismo, en noviembre del año 2013 se aprobó en Argentina la ley número 26904, que incluyó a los "Delitos contra la integridad sexual" en el Código Penal, y que configura como tipo penal al grooming.
Dicha ley define a esta actividad como un delito dentro del Código Penal, como al 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."

Por su parte, el decreto 349/2018 promulgó la ley 27436, que castiga la simple tenencia de material pornográfico infantil. Esto es "toda representación de un menor de 18 años dedicado a actividades sexuales explícitas o de sus partes genitales con fines predominantemente sexuales".

La falta de conocimiento informático es un factor fundamental en el impacto de los delitos de esta índole en la sociedad en general. Por eso, cada vez se hace más necesario contar con mayores conocimientos en tecnologías de la información, las cuales permitan mantener un contexto de referencia idóneo para el manejo de dichas situaciones.

Debido a la razón virtual de los ilícitos informáticos, puede volverse compleja la tipificación de los mismos, ya que, habitualmente, se tienen escasos conocimientos y experiencias en el manejo de esta ciencia. Desde el enfoque legislativo, la tipificación de estos actos lleva un procedimiento extenso, así como la creación de instrumentos legales, que pueden no obtener los resultados esperados. Resulta un desafío adaptarse constantemente a la innovación tecnológica, y esto obliga a manejar un dinamismo adecuado en las leyes relacionadas con la informática.