**DELITO INFORMATICO**

El delito informático, o crimen electrónico, o bien ilícito digital es el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración o supresión de datacredito), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros.

Actualmente existen leyes que tienen por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos en las variedades existentes contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías.

Índice [ocultar]

1 Generalidades

2 Crímenes específicos

2.1 Spam

2.2 Fraude

2.3 Contenido obsceno u ofensivo

2.4 Hostigamiento / Acoso

2.5 Tráfico de drogas

2.6 Terrorismo virtual

3 Sujetos activos y pasivos

4 Regulación por países

4.1 Argentina

4.1.1 La ley vigente

4.1.2 Definiciones vinculadas a la informática

4.1.3 Delitos contra menores

4.1.4 Protección de la privacidad

4.1.5 Delitos contra la propiedad

4.1.6 Delitos contra las comunicaciones

4.1.7 Delitos contra la administración de justicia

4.2 Colombia

4.3 España

4.4 México

4.6 Estados Unidos

**Generalidades**

El delito informático incluye una amplia variedad de categorías de crímenes. Generalmente este puede ser dividido en dos grupos:

Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos, Spam, ataque masivos a servidores de Internet y generación de virus.

Crímenes realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, pornografía infantil, pedofilia, etc.

Un ejemplo común es cuando una persona comienza a robar información de websites o causa daños a redes o servidores. Estas actividades pueden ser absolutamente virtuales, porque la información se encuentra en forma digital y el daño aunque real no tiene consecuencias físicas distintas a los daños causados sobre los ordenadores o servidores. En algunos sistemas judiciales la propiedad intangible no puede ser robada y el daño debe ser visible. Un ordenador puede ser fuente de pruebas y, aunque el ordenador no haya sido directamente utilizado para cometer el crimen, es un excelente artefacto que guarda los registros, especialmente en su posibilidad de codificar los datos. Esto ha hecho que los datos codificados de un ordenador o servidor tengan el valor absoluto de prueba ante cualquier corte del mundo.

Los diferentes países suelen tener policía especializada en la investigación de estos complejos delitos que al ser cometidos a través de internet, en un gran porcentaje de casos excede las fronteras de un único país complicando su esclarecimiento viéndose dificultado por la diferente legislación de cada país o simplemente la inexistencia de ésta.

**Crímenes específicos**

**Spam**

El Spam o los correos electrónicos, no solicitados para propósito comercial, es ilegal en diferentes grados. La regulación de la ley en cuanto al Spam en el mundo es relativamente nueva y por lo general impone normas que permiten la legalidad del Spam en diferentes niveles. El Spam legal debe cumplir estrictamente con ciertos requisitos como permitir que el usuario pueda escoger el no recibir dicho mensaje publicitario o ser retirado de listas de email.

**Fraude**

El fraude informático es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio por lo siguiente:

Alterar el ingreso de datos de manera ilegal. Esto requiere que el criminal posea un alto nivel de técnica y por lo mismo es común en empleados de una empresa que conocen bien las redes de información de la misma y pueden ingresar a ella para alterar datos como generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas.

Alterar, destruir, suprimir o robar datos, un evento que puede ser difícil de detectar.

Alterar o borrar archivos.

Alterar o dar un mal uso a sistemas o software, alterar o reescribir códigos con propósitos fraudulentos. Estos eventos requieren de un alto nivel de conocimiento.

Otras formas de fraude informático incluye la utilización de sistemas de computadoras para robar bancos, realizar extorsiones o robar información clasificada.

**Contenido obsceno u ofensivo**

El contenido de un website o de otro medio de comunicación puede ser obsceno u ofensivo por una gran gama de razones. En ciertos casos dicho contenido puede ser ilegal. Igualmente, no existe una normativa legal universal y la regulación judicial puede variar de país a país, aunque existen ciertos elementos comunes. Sin embargo, en muchas ocasiones, los tribunales terminan siendo árbitros cuando algunos grupos se enfrentan a causa de contenidos que en un país no tienen problemas judiciales, pero sí en otros. Un contenido puede ser ofensivo u obsceno, pero no necesariamente por ello es ilegal.

Algunas jurisdicciones limitan ciertos discursos y prohíben explícitamente el racismo, la subversión política, la promoción de la violencia, los sediciosos y el material que incite al odio y al crimen.

**Hostigamiento / Acoso**

El hostigamiento o acoso es un contenido que se dirige de manera específica a un individuo o grupo con comentarios vejatorio o insultativos a causa de su sexo, raza, religión, nacionalidad, orientación sexual, identidad etnocultural, etc. Esto ocurre por lo general en canales de conversación, grupos o con el envío de correos electrónicos destinados en exclusiva a ofender. Todo comentario que sea denigrante u ofensivo es considerado como hostigamiento o acoso.El acto de destruir los artículos, desaparecer el nombre de un determinado autor, el 'delete' de los nombres de las publicaciones de un intelectual, que realizan supuestos guardianes de wikipedia es otra forma de acorralamiento o bullying digital, atentando contra los derechos humanos y la libertad de expresión, mientras no afecten a terceros.Aun el fraude al justificar por un causal no claro, por decir desaparecer una asociación cultural y decir "banda musical promocional".

**Tráfico de drogas**

El narcotráfico se ha beneficiado especialmente de los avances del Internet y a través de éste promocionan y venden drogas ilegales a través de emails codificados y otros instrumentos tecnológicos. Muchos narcotraficantes organizan citas en cafés Internet. Como el Internet facilita la comunicación de manera que la gente no se ve las caras, las mafias han ganado también su espacio en el mismo, haciendo que los posibles clientes se sientan más seguros con este tipo de contacto. Además, el Internet posee toda la información alternativa sobre cada droga, lo que hace que el cliente busque por sí mismo la información antes de cada compra.

**Terrorismo virtual**

Desde 2001 el terrorismo virtual se ha convertido en uno de los novedosos delitos de los criminales informáticos los cuales deciden atacar masivamente el sistema de ordenadores de una empresa, compañía, centro de estudios, oficinas oficiales, etc. Un ejemplo de ello lo ofrece un hacker de Nueva Zelandia, Owen Thor Walker (AKILL), quien en compañía de otros hackers, dirigió un ataque en contra del sistema de ordenadores de la Universidad de Pennsylvania en 2008.

La difusión de noticias falsas en Internet (por ejemplo decir que va a explotar una bomba en el Metro), es considerado terrorismo informático y es procesable.

**Sujetos activos y pasivos**

Muchas de las personas que cometen los delitos informáticos poseen ciertas características específicas tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible.

En algunos casos la motivación del delito informático no es económica sino que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943. Esta categoría requiere que: (1) el sujeto activo del delito sea una persona de cierto estatus socioeconómico; (2) su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni por inestabilidad emocional.

El sujeto pasivo en el caso de los delitos informáticos puede ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

Para la labor de prevención de estos delitos es importante el aporte de los demanificados que puede ayudar en la determinación del modus operandi, esto es de las maniobras usadas por los delincuentes informáticos.

**Regulación por países**

**Argentina**

**La ley vigente**

La Argentina sancionó el 4 de junio del 2008 la Ley 26.388 (promulgada de hecho el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

**Definiciones vinculadas a la informática**

En el nuevo ordenamiento se establece que el término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión (art. 77 Código Penal).

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente (art. 77 Código Penal).

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente (art. 77 Código Penal).

Delitos contra menores

En el nuevo ordenamiento pasan a ser considerados delitos los siguientes hechos vinculados a la informática:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Protección de la privacidad

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) 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 un (1) a cuatro (4) años.

**Delitos contra la propiedad**

Artículo 173 inciso 16: (Incurre en el delito de defraudación)...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.

Artículo 183 del Código Penal: (Incurre en el delito de daño)...En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

Artículo 184 del Código Penal: (Eleva la pena a tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes):

Inciso 5: Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

Inciso 6: Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

**Delitos contra las comunicaciones**

Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

**Delitos contra la administración de justicia**

Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

**Colombia**

En Colombia el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según estadisticas, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

En Colombia existen instituciones de educación como UNICOLOMBIA que promueven capacitaciones en temas relacionados con Delitos Informáticos, el mejor manejo y uso de la prueba digital, establecer altos estándares científicos y éticos para Informáticos Forenses, Llevar a cabo investigación y desarrollo de nuevas tecnologías y los métodos de la ciencia del análisis forense digital e Instruir a los estudiantes en diversos campos específicos sobre nuevas tecnologías aplicadas a la informática Forense, la investigación científica y el proceso tecnológico de las mismas.

**España**

En España, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estas sanciones se recogen en la Ley Orgánica 10/1995, de 23 de Noviembre en el BOE número 281, de 24 de Noviembre de 1.995. Estos tienen la misma sanción que sus homólogos no-informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

El Tribunal Supremo emitió una sentencia el 12 de junio de 2007 (recurso Nº 2249/2006; resolución Nº 533/2007) que confirmó las penas de prisión para un caso de estafa electrónica (phishing).

**México**

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el titulo noveno capítulo I y II.

El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que intencionalmente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

La reproducción no autorizada de programas informáticos o piratería esta regulada en la Ley Federal del Derecho de Autor en el Título IV, capítulo IV.

También existen leyes locales en el código penal del Distrito Federal y el código penal del estado de Sinaloa.

**Estados Unidos**

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).