

# **“Naturaleza Jurídica de los delitos informáticos”**

## **INDICE:**

<b>1) Resumen - Abstract.</b> .....	<b>Pág. 3</b>
<b>2) Definición de los Delitos Informáticos.</b> .....	<b>Pág. 3</b>
<b>3) Distintas técnicas legislativas de los delitos informáticos.</b> .....	<b>Pág. 8</b>
<b>4) Ensayo de clasificación.</b> .....	<b>Pág. 11</b>
<b>5) Naturaleza Jurídica de los Delitos Informáticos.</b> .....	<b>Pág. 14</b>
<b>6) Conclusiones.</b> .....	<b>Pág. 16</b>
<b>7) Bibliografía.</b> .....	<b>Pág. 18</b>

## **1) Resumen - Abstract:**

*La intención de este trabajo es abarcar los principios clásicos del derecho y aplicarlos a los efectos de identificar la naturaleza jurídica de los delitos informáticos. Sin la intención de resolver conflictos legislativos o problemas sociales, el objeto del presente se limita a analizar la legislación y doctrina existentes, al efecto de consolidar una postura jurídica sobre el tema analizado. La intención del presente, es clarificar el panorama jurídico, para que eventualmente y "a posteriori", aporte orden y criterio desde la doctrina, para su aplicación práctica.-*

*The intention of this document is to contemplate the classical main values of the Science of Law, and apply them to identify the legal nature of cybercrime. Without trying to resolve legislative or social problems, the object of this work, is limited to analyze the law and doctrine existent, to clarify the legal landscape, in order to bring eventually order and criteria from the doctrine, to its practical application.-*

## **2) Definición de los Delitos Informáticos**

Como parte inicial del presente trabajo y con la intención de obtener la definición mas específica posible del objeto de estudio –Naturaleza Jurídica de los Delitos Informáticos-, comenzaremos por describir, qué son a nuestro criterio, los delitos informáticos. A tal fin, la metodología de trabajo, será la de ofrecer, una serie de definiciones acompañadas de ciertas reflexiones, para que de manera inductivo-deductiva, podamos aproximar a una definición de los mismos.

Elegimos para comenzar y justamente tratándose de Delitos informáticos, buscar inicialmente en algún diccionario de la Red, en este caso, “Wikipedia”, donde nos encontramos con la siguiente definición:

*"Delito informático, crimen genérico o crimen electrónico, que agobia con 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 datos críticos), 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.<sup>1</sup>*

Siendo que mas adelante, en la definición respecto de sus generalidades, aclara lo siguiente:

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

1. *Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos (Spam), ataques masivos a servidores de Internet y generación de virus.*
2. *Crímenes realizados por medio de ordenadores y del Internet, por ejemplo, espionaje por medio del Internet, fraudes y robos, pornografía infantil, pedofilia Internet, etc."*

Con esta definición, puede uno darse idea (aunque no exactamente jurídica) de lo que trata la temática. Pero alguien que se dedica al derecho, inmediatamente pasaría a buscar opiniones doctrinarias al respecto, entonces nos encontramos por ejemplo con las siguientes:

*"En principio, para comenzar a hablar del tema que nos ocupa, es fundamental referir ciertos aspectos que pueden unificar el lenguaje y facilitar el acuerdo. Al hablar de delitos informáticos, el primer distingo necesario, dentro del término delito, aparece al diferenciar el penal del civil. Al encontrar al derecho punitorio como un sistema cerrado, al cual solo le interesaran las conductas descriptas expresamente en el derecho positivo, con una importancia suficiente que amerite una sanción, se diferencia automáticamente del delito civil donde no necesitamos una definición de conducta típica tan concreta, sino mas bien una serie de situaciones y acontecimientos que resulten en la responsabilidad de una persona, ya sea de manera subjetiva o incluso objetiva.*

*Una vez seleccionado el tipo de delito del que consta la investigación, diremos para hablar de éste, lo que explica la teoría general del delito, precisamente, que necesitamos de una acción típica, antijurídica y culpable. Solo entonces, podremos analizar la segunda palabra que titula este trabajo (informático). Ahora bien, el primer inconveniente surge a la hora de definir si los delitos informáticos se diferencian de su género y demás especies por las herramientas y métodos que se utilizan o si por el contrario, se definen por el objeto que persiguen. Es decir, ¿nos encontramos frente a un delito de estafa realizado a través de una herramienta informática? ¿O por el contrario, nos enfrentamos a un nuevo tipo delictual? Una tercera opción sería que nos encontráramos frente a un delito ya consagrado penalmente, pero que por las*

---

<sup>1</sup> Recuperado el 1/10/2010 en [http://es.wikipedia.org/wiki/Delito\\_inform%C3%A1tico](http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico)

*herramientas que fueron utilizadas para cometerlo, sea necesario considerarlo agravado y requiera de una sanción mayor.”<sup>2</sup>*

Claramente mas jurídico y preciso, este texto nos da una idea jurídica del contexto donde se encuentran los delitos informáticos y plantea una serie de interrogantes, que deberemos responder para alcanzar el objetivo de este trabajo, que es precisamente la definición de la naturaleza jurídica de este tipo de delitos.

Otra definición podría ser la ofrecida por Luciano SALELLAS<sup>3</sup> quien refiere lo siguiente:

*“Delitos informáticos, son todos aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático”*

*El Delito Informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.*

*Dado que la seguridad completa no existe, el margen para un nuevo incidente de seguridad siempre se tiene, por tanto, cuando éste se presenta, se verifica en un alto porcentaje que las organizaciones no se encuentran preparadas para enfrentar la realidad de una intrusión o incidente.*

*Un incidente representa un reto para demostrar la diligencia de su organización para enfrentar el hecho, tomar el control, recoger y analizar la evidencia, y finalmente generar el reporte sobre lo ocurrido, que incluye las recomendaciones de seguridad y conceptos sobre los hechos del incidente.”*

Esta definición es clara y contundente, pareciera ser que existe un único delito informático, que es el mal uso, o para ser mas precisos el “uso indebido” de las computadoras. Lo que lógicamente pareciera innegable, pero igual de innegable es el hecho de que muchos hechos ilícitos relacionados con la informática, no se realizan a través de una “computadora” con lo cual es al menos imprecisa dicha definición. En segundo término, vocablos como “indebido” dan siempre lugar a interpretación, a grises, lo cual no es para nada deseable en el derecho penal. Ciento es, sin embargo, que muchas legislaciones la adoptan, pero sería muy amplio encuadrar en un mismo y único tipo delictual, por ejemplo; a una red internacional de pedofilia, que genera contenido a través del ordenador, lo procesa y lo distribuye a título oneroso, con un joven de 16 años que consiguió acceder a la cuenta de correo de su novia para saber si lo engañaba. De manera que tampoco preferimos esta definición, que aunque tentadora por la simplificación que implica, no resultaría aplicable sin generar más problemas que soluciones, en cuanto a la interpretación y la seguridad jurídica del ámbito penal.-

<sup>2</sup> RUANI, HUMBERTO FELIX, “Delitos Informáticos” XIII Congreso Iberoamericano de Derecho e Informática, Lima, Perú, Noviembre de 2009

<sup>3</sup> SALELLAS LUCIANO, “Delitos Informáticos - Ciberterrorismo” Recuperado el 1/10/2010 de [http://www.cabinas.net/monografias/informatica/delitos\\_informaticos\\_ciberterrorismo.pdf](http://www.cabinas.net/monografias/informatica/delitos_informaticos_ciberterrorismo.pdf)

Así mismo, nos encontramos con un autor mexicano que para definir el delito informático, le caracteriza dividiéndolo en su forma típica y atípica, entendiendo por la primera a "las conductas que encuadran con un tipo penal, cumpliendo con la antijuridicidad y culpabilidad que exige la teoría clásica del delito, en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"<sup>4</sup>

El mismo autor, a su vez establece que a su criterio, los delitos informáticos reúnen las siguientes características especiales:

- ✓ "Son conductas criminales de cuello blanco, porque sólo un determinado número de personas con ciertos conocimientos técnicos puede llegar a cometerlas.
- ✓ Son acciones ocupacionales, porque en muchas veces se realizan cuando el sujeto se halla trabajando.
- ✓ Son acciones de oportunidad, porque se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- ✓ Provocan serias pérdidas económicas.
- ✓ Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- ✓ Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- ✓ Son muy sofisticados.
- ✓ Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- ✓ En su mayoría son imprudencias y no necesariamente se cometen con intención.
- ✓ Ofrecen facilidades para su comisión los menores de edad.
- ✓ Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- ✓ En algunos casos siguen siendo ilícitos impunes ante la ley."<sup>5</sup>

Finalmente y luego de las citadas referencias, nos atrevemos a decir que el vocablo "Delito Informático" (descartando los delitos civiles) tiene necesariamente más de una acepción.

a) Acepción Penal Jurídicamente Relevante: Guiados por la teoría clásica del delito, será delito informático, únicamente *aquella acción que implique un contenido de tratamiento automático de la información<sup>6</sup> y que cumpla con los requisitos de ser típica, antijurídica y culpable, sin distinguir si la informática se entiende como medio o*

<sup>4</sup> TÉLLEZ VALDÉS, Julio, Derecho Informático, 3<sup>a</sup>.ed., Ed. Mc Graw Hill, México, 2003, Pág. 8

<sup>5</sup> TÉLLEZ VALDÉS, Julio. Ob Cit. Pág. 09 y ss.

<sup>6</sup> NOTA: Ofrecemos respecto de la informática la siguiente definición: "Ciencia aplicada que abarca el estudio y aplicación del tratamiento automático de la información, utilizando sistemas computacionales, generalmente implementados como dispositivos electrónicos".

Recuperado el 6/10/2010 en <http://es.wikipedia.org/wiki/Inform%C3%A1tica.->

*como finalidad delictiva en sí misma.* (Serían los que el Dr. Téllez Valdés define como delitos informáticos típicos)

b) Acepción Vulgar: Diremos también que hay conductas ilícitas que se realizan mediante los medios electrónicos y aún con intención de dañar, pero que mientras no estén contempladas en el ordenamiento jurídico y no cumplan con los requisitos que establece la teoría del delito, no pueden ser llamadas Delito Informático con otra acepción que no sea la vulgar y técnicamente incorrecta. (Serían los que el Dr. Téllez Valdés define como delitos informáticos atípicos)

c) Acepción Específica: Finalmente y no por eso definitivo, también podría existir una acepción de los delitos informáticos genéricamente hablando, como aquellos cuyo tipo penal, tuviera únicamente la finalidad de proteger intereses propios a la tecnología y la informática. Aunque resulta relevante recordar, que el bien jurídicamente tutelado, deviene eterna y necesariamente en un derecho personal o subjetivo.-

### ***3) Distintas técnicas legislativas de los delitos informáticos:***

Este trabajo intenta dilucidar cual es la naturaleza jurídica de los delitos informáticos, para lo cual tomaremos de referencia lo hecho a nivel legislativo por los siguientes estados Iberoamérica, a saber:

**Perú:** La legislación de este país contempla dos tipos de delitos, aquellos que son específicamente informáticos, como ser en el capítulo “X” de su código penal, “Delitos Informáticos”, donde por ejemplo el Art. 207 establece con mucho atino, diferentes penas para el acceso a bases de datos específicamente informáticas, para su modificación o destrucción y con ciertos agravantes dependiendo del interés pecuniario que pudiera perseguir el eventual delincuente, lo privilegiado de la información en cuestión y/o si la seguridad nacional se encontrara en peligro. Pero lo interesante, es que además de reconocer delitos específicamente informáticos dentro de su propio capítulo, establecen un doble régimen, V. G.: En su artículo 186 “hurto agravado” encontramos tres penas distintas según la gravedad, y coloca en la segunda clase, con una pena no menor de cuatro, ni mayor de ocho años si el hurto es cometido... Inc. 3) “Mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas.” Lo cual como veremos mas adelante, puede ser motivo de desacuerdo en cuanto el encuadre típico, pero en principio establece el criterio dualista adoptado por la legislación peruana, teniendo aquí dos formas de legislar tan distintas como válidas.

**Argentina:** en esta legislación, la ley 26.388 del año 2008, enumera una serie de delitos informáticos, ubicándolos en distintos títulos del código penal de la nación, según el objeto del delito. Por ejemplo, ubica en el artículo 273 Inc. 16 -correspondiente

al título de estafas y otras defraudaciones, dentro de los delitos contra la propiedad-, la sanción al que: "...defraudare a otro mediante cualquier técnica de manipulación informática *que altere el normal funcionamiento de un sistema informático o la transmisión de datos*", con lo cual la técnica legislativa deja en claro su postura, es decir que para la legislación argentina, los delitos informáticos no son tales por los fines que persiguen, sino exclusivamente por las herramientas de que se valen. En este caso, encontramos al tipo delictual como una defraudación para la cual se implementa un medio informático, pero que a su vez, dicho medio requiere de ciertos recursos y capacitación del delincuente, por lo que se constituye en un peligro mayor, que lo hace posible de una sanción agravada, siendo que el delito continua basándose en la defraudación y tiene a la informática como un medio, como una "técnica de manipulación". Mientras que en lo referido a las comunicaciones, el congreso argentino, mantiene su antiguo tipo penal, agregando las comunicaciones electrónicas como susceptibles de ser interceptadas, publicadas, etc. Confirmando de esta manera, la inconsistencia material de estos delitos como tipos penales y la elección de sancionar los mismos como medios del "Iter Crimis".

**España y C. E.:** Aquí, tomamos únicamente y por ejemplo, la Decisión marco 2005/222/JAI del consejo de la Comunidad Europea (la cual recoge España en su proyecto de ley orgánica publicado en el B. O. del 15 de enero de 2007), la que sugiere una concepción de delito informático mas específica y relevante a nivel punitivo, sin necesidad de recurrir a otro tipo de delito. Es claro el ejemplo de lo que sanciona su Art. 2 Inc. 1) –

"Acceso ilegal a los sistemas de información.

1. Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad."

No se habla de derecho a la privacidad, ni los datos personales, se habla específicamente de un conjunto o parte de un sistema de información. Aparentemente un bien novedoso entre los que gozan de la tutela jurídica.-

Aclaramos que se toma este sencillo ejemplo que marca una tendencia, pero que es muy amplio lo legislado por la comunidad europea respecto de delitos informáticos, haciendo expresa mención del convenio del ciber crimen y el de Lanzarote aun sin vigencia.-

**Venezuela:** Es destacable el modo en que la LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS de Venezuela, eonecta las distintas perspectivas de la naturaleza de los delitos informáticos, separando en 4 títulos a saber: 1) “disposiciones generales”, donde especifica alcances y definiciones; 2) “ de los delitos” donde diferencia en sus capítulos entre los delitos puramente informáticos y luego los que son contra la propiedad; contra la privacidad de las personas y de las comunicaciones; contra los niños, niñas y adolescentes y finalmente contra el orden económico. Continuando luego con un título de disposiciones generales donde se configuran varios agravantes y penas accesorias como la divulgación de sentencia, que resulta al menos interesante. Finalmente su último título de disposiciones finales que son de forma. Siendo que es esta ley un auténtico resumen de lo expuesto hasta el momento y considerándola como un verdadero modelo por su simpleza y potencial eficacia.-

**CHILE:** En lo que hace a este país andino, su legislación respecto de los delitos informáticos, tiene la particularidad de regular expresamente la necesidad de malicia (dolo) a la hora de realizar la acción para incurrir en el delito, protegiendo en 4 artículos, los “sistemas de tratamiento de información o sus partes o componentes” y “La información contenida en los mismos”<sup>7</sup>

**México:** El estado Mexicano, en su Código Penal Federal, dedica el capítulo II del noveno título de su Segundo libro, al “ACCESO ILÍCITO A SISTEMAS Y EQUIPOS

---

7 Ley 19.223 (Chile)

“Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.”.

DE INFORMÁTICA”, donde de manera extremadamente sintética, establece la protección de las comunicaciones. Es en principio escasa la legislación penal al respecto, pero aclaramos, que hay estados mexicanos que tienen sus propias tipificaciones al respecto, a los que no remitiremos en orden a la extensión que implicaría contemplar cada uno de ellos

#### **4) Ensayo de clasificación:**

Habiendo dado una recorrida por algunas definiciones y diferentes legislaciones, consideramos que una posible clasificación de las acciones previstas, sería considerando la existencia de 2 tipos de agravamiento por la utilización del método y únicamente una especie de delito informático propiamente dicho.

Tendremos entonces:

Agravamiento General: Implica delitos como la distribución de pornografía infantil, en la cual, la informática es únicamente un medio para realizar la acción típica. Si bien es un delito específico -la sola reproducción o distribución-, estas acciones, podrían llevarse a cabo de muchas otras maneras, es decir por otros medios. Si bien el delincuente lo elige por una variedad de ventajas que ofrece, es muy claro que no es la única forma de cometer el delito. Motivo por el cual, diremos que este tipo de acciones delictivas, debería en realidad, tener la pena de la distribución e independientemente de eso, un agravamiento en la condena, que podría legislarse de forma genérica, como ser aumentando en tanto por ciento la sanción mínima y máxima del tipo penal, fundados en las siguientes razones a saber:

- a) La necesidad de contar con equipos especiales (computadoras o cualquier otro medio informático).
- b) La capacidad especial que requiere el delincuente, ya que debe tener conocimientos especiales y calificados para la realización de la acción requerida
- c) La peligrosidad mayor del delincuente muñido de herramientas para realizar la acción típica
- d) El anonimato del que se vale al utilizar herramientas como Internet, para evadir las responsabilidades penales correspondientes

- e) El aumento del potencial dañino que ofrece una herramienta mundial como es la red de redes.-

Agravamiento Especial: Otro tipo de delitos que se cometen por medio de herramientas electrónicas, tiene la particularidad de que si bien la informática se utiliza como un simple medio, sin ella no existiría otra forma obtener el resultado esperado. Es el caso por ejemplo del daño informático. En este supuesto, si bien es cierto que se puede producir daño a herramientas informáticas tirando un gabinete de un décimo piso; no es menos cierto, que la única forma de acceder a esa información es a través de los medios informáticos. Entonces se estaría violentando un derecho de propiedad, pero de una manera única. En este caso, consideramos que el agravamiento debiera ser aun mayor, dado que igualmente mayor será la especialidad del delincuente y la eficacia de su acción.-

Delitos informáticos propiamente dichos: Finalmente, hay dos casos en los que requerimos definitivamente un tipo penal nuevo y específico, distinto de los agravamientos; el primero es cuando se genera un nuevo bien que precisa de tutela jurídica –como es en este caso la información<sup>8</sup>– y el segundo es cuando un bien jurídicamente tutelado, es vulnerado de una manera que no estaba prevista en las tipificaciones del ordenamiento penal. No hablamos de un nuevo medio de cometer el mismo delito, sino de un nuevo delito que vulnera el bien ya protegido. Es decir, una forma de atacar el bien tutelado con características tan especiales que no encuadra en los verbos o acciones típicas existentes. A modo de ejemplo, en la Argentina, requisitos de la estafa eran:

*"Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de*

---

<sup>8</sup> NOTA: En este caso no nos referimos a la información personal, protegida desde tiempos romanos con el habeas data, sino a la información en general, la que pueda almacenar un servidor, un computador, una empresa o un ente del gobierno. El punto de inflexión, es que esta información existe en la Red con sistemas vulnerables y no estaba protegida, es decir, uno puede reclamar por el secreto industrial, la correspondencia, etc. Pero la actualidad no requiere de una protección especial de la información, sino de una protección general, abarcadora de todos los aspectos desde los que pueda ser violentada y en un mundo de vertiginoso avance tecnológico, resulta cada vez más difícil dicha protección. En lo que difícilmente encontraremos oposición, es en la necesidad de protegerla como un nuevo bien jurídico.

*confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardido o engaño.<sup>9</sup>*

La razón por la que Argentina tuvo la necesidad de un nuevo tipo penal, es que en un análisis de tipificación referente al artículo transcripto, observamos desde el comienzo, cuando se habla del que defraudare “a otro” que ya se presupone la existencia de una víctima humana. Lo cual no se adecua por ejemplo, al caso de ingresar a una base de datos bancaria y generar un crédito a favor del propio delincuente. Tampoco se estaría cumpliendo con las formas de defraudación mencionadas en los verbos típicos, ni podría existir engaño respecto de un ordenador. Siendo que ni las personas jurídicas, ni los sistemas informáticos son susceptibles de ser engañados, queda suficientemente claro a nuestro entender, que el bien jurídico “propiedad privada” es vulnerado sin encontrar en el ordenamiento legal, acción típica alguna que lo proteja. En este caso estamos frente a un nuevo tipo penal, de los pertenecientes a los delitos informáticos. A dichos efectos se creó finalmente una nueva figura penal ubicada en el Art. 173 Inc. 16 del respetivo Código Penal<sup>10</sup>.-

---

<sup>9</sup> Código Penal Argentino, Título VI “Delitos Contra La Propiedad”, Capítulo IV “Estafas Y Otras Defraudaciones” Artículo 172.

10 Cod. Penal Argentino Art. 173 Inc. 16: “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. (Inciso incorporado por Art. 9º de la Ley N° 26.388, B.O. 25/6/2008)”

## *5) Naturaleza Jurídica de los Delitos Informáticos*

Para definir la "Naturaleza Jurídica de los Delitos Informáticos"<sup>11</sup>, diremos que se trata del lugar que ocupa un instituto dentro del Universo Jurídico del que forma parte. Es el lugar que sus propias características le asignan, haciéndolo parte de un complejo sistema de Género - Especie. Para identificar la Naturaleza Jurídica, debemos analizar el complejo objeto de la ciencia del derecho, considerando los elementos característicos de cada género y cada especie, lo que los hace comunes y lo que los diferencia. Entonces, desde una metodología deductiva, partiremos de los géneros más amplios, hacia los más específicos de la siguiente manera:

- 1) Dentro del derecho positivo (ya que las actividades no comprendidas en los ordenamientos vigentes no pueden denominarse "delitos", siguiendo el principio de "*Nullum crimen, nulla poena sine praevia lege*")<sup>12</sup>), distinguiremos como lo hace la escuela clásica entre derecho público y derecho privado<sup>12</sup>. Aquí necesariamente optamos por seguir la rama descendiente del Derecho Público.
- 2) Continuando con la ubicación específica y dentro del género del Derecho Público, Ubicamos a los "delitos Informáticos" en la rama del Derecho penal, dado que su función es la protección de un bien jurídicamente tutelado de importancia tal, que puede eventualmente coartar la libertad de aquel que pudiera atentar en su contra, previendo en distintos ordenamientos jurídicos, penas de este tipo, razón

---

<sup>11</sup> NOTA: cuando me encontraba cursando mi carrera de grado, mientras repetía continuamente la definición de distintos institutos jurídicos, -previo a dar un examen- y sin olvidar nunca la definición de la naturaleza jurídica de cada uno de ellos, le pedí a mi padre -abogado de profesión- que evaluara mis conocimientos; Luego de escucharme disertar por casi una hora, le pregunte si le parecía que tenía conocimientos suficientes para presentarme a la mesa examinadora; y en ese momento me pregunto: -"¿Qué es la Naturaleza Jurídica?", al igual que ahora al encarar este tema, toda la seguridad que el estudio me había dado, se desmoronó instantáneamente, cuando sincerándome, respondí que no tenía la más remota idea. finalmente él me dijo: -"No te preocupes, tal vez no sea necesario para aprobar una asignatura, pero cuando sepas qué es la Naturaleza Jurídica de las cosas, **habrás aprendido algo de derecho**"

<sup>12</sup> NOTA: Si bien es cierto que la tendencia general, es la de privatizar el derecho penal, ofreciendo a los damnificados la posibilidad de acordar con los criminales una forma de resarcimiento convencional y dejar de lado la rigidez clásica de la privación de la libertad como sanción para la rehabilitación del delincuente -que en su generalidad, ni cumple su función rehabilitadora, ni compensa a la víctima por el daño sufrido-; no es menos cierto que siempre se conserva un interés público relativo a la preservación de ciertos derechos y libertades, que ameritan una protección jurídica de "Última Ratio", como lo es la sanción penal. Dándole a esta un innegable carácter público..

por la cual avanzamos en la definición de su naturaleza, ubicándolo en el sub-género del derecho penal.

- 3) Adentrándonos en la clasificación de los delitos, seguiremos la técnica legislativa dominante, consistente en agrupar las acciones típicas según el bien jurídico al que tengan como destino proteger. -V. G.: La propiedad privada, los derechos personalísimos, la integridad del estado, etc.- En este orden de ideas, para la clasificación de los Delitos Informáticos debemos abrir un pequeño abanico de opciones, según este nuevo género en el que ubicaremos estas distintas especies:
  - a. Por un lado, los agravamientos por el medio utilizado, deberían identificarse con su naturaleza general dentro de un sistema penal codificado. Es decir que integrarían una generalidad aplicable a las distintas especies de delitos específicos, ya que como las demás especies del género "aggravantes" serán aplicables a todos los delitos que fueran susceptibles de acoger este tipo de metodología delictiva.
  - b. Por otro lado, resulta necesaria y adecuada, la creación de un nuevo Sub-género dentro del género "delitos", que contemplará los que clasificamos anteriormente como "*Delitos Informáticos Propiamente Dichos*". Esto resulta, de encontrarnos con acciones típicas que responden a las generalidades de los delitos, pero que se caracterizan especialmente por proteger nuevos intereses socialmente relevantes, o bien proteger intereses ya existentes pero de nuevos riesgos creados por las nuevas formas delictivas, para los cuales no existía tipicidad previa y que se relacionan y aúnán por surgir específicamente a través de los adelantos tecnológicos de la informática.-

## **6) Conclusiones:**

### **6.2- Definición:**

Concluimos que la definición jurídicamente correcta del delito informático es, acorde a nuestro criterio, la que nominamos como “*Acepción Penal Jurídicamente Relevante*”, es decir: “será delito informático, únicamente aquella acción que implique un contenido de tratamiento automático de la información<sup>13</sup> y que cumpla con los requisitos de ser típica, antijurídica y culpable, sin distinguir si la informática se entiende como medio o como finalidad delictiva en sí misma.”

### **6.3- Legislación comparada**

Respecto de este tópico, creemos que ninguna de las legislaciones plasma en su texto la naturaleza jurídica de los delitos informáticos, ni se los define, ni se los clasifica, a nuestro entender, de manera suficiente. Siendo Venezuela el ordenamiento jurídico más próximo a la línea de este trabajo, concluimos que resulta necesario continuar trabajando para dar claridad a los conceptos jurídicos y normativos, relativos a este tipo de delitos en particular.-

### **6.4- Clasificación**

Entendemos que metodológicamente, este tipo de actividades, debieran clasificarse y codificarse como “Agravantes generales”; “Agravantes especiales” y “Delitos Informáticos Propiamente dichos”

### **6.5- Naturaleza Jurídica:**

Siguiendo con la línea de clasificación anterior, consideramos que si bien todos pertenecen al género Delito, de la rama penal del Derecho Público, como Sub-género del Derecho; Destacamos la necesidad de escindir los clasificados como agravantes generales y especiales, que serían especies del género Agravantes; de los Delitos Informáticos propiamente dichos, que conformarían un nuevo Sub-género dentro de los delitos.-

---

13 NOTA: Ofrecemos respecto de la informática la siguiente definición que explica la redacción de la definición: “Ciencia aplicada que abarca el estudio y aplicación del tratamiento automático de la información, utilizando sistemas computacionales, generalmente implementados como dispositivos electrónicos”.

Recuperado el 6/10/2010 en <http://es.wikipedia.org/wiki/Inform%C3%A1tica>.

Con estas conclusiones, damos por finalizado este trabajo realizado a los efectos de ser expuesto en el XIV Congreso Iberoamericano de Derecho e Informática, a realizarse en la Universidad Autónoma de Nuevo León, Ciudad de Monterrey, Nuevo León, México. Octubre de 2010.-

## **7) Bibliografía:**

1. Código Penal Argentino, Título VI “Delitos Contra La Propiedad”, Capítulo IV “Estafas Y Otras Defraudaciones” Artículo 172 y 173 Inc. 16. Recuperado el 1/10/2010, de [http://www.csjn.gov.ar/cmf/codigo\\_penal.html](http://www.csjn.gov.ar/cmf/codigo_penal.html)
2. Código Penal Federal Mexicano. Recuperado el 6/10/2010 de <http://info4.juridicas.unam.mx/ijure/tcfed/8.htm>
3. FERNÁNDEZ DELPECH, Horacio, “Internet: Su Problemática Jurídica” Segunda Edición Ampliada y Actualizada. Ed. Lexis Nexis, Buenos Aires, Argentina, Publicado en Julio del Año 2004.-
4. Ley 19.223 del estado chileno, recuperado el 1/10/2010 de <http://red.gov.cl/ley19223.htm>
5. PALAZZI, Pablo A. “Los Delitos Informáticos en el Código Penal. Análisis de la Ley 26.388”, Ed. Abeledo Perrot, Buenos Aires Argentina, 2009.
6. RUANI, Humberto Félix, “Delitos Informáticos” XIII Congreso Iberoamericano de Derecho e Informática, Lima, Perú. Noviembre de 2009
7. SALELLAS LUCIANO, “Delitos Informáticos – Ciberterrorismo” Recuperado el 1/10/2010 de [http://www.cabinas.net/monografias/informatica/delitos\\_informaticos\\_ciberterrorismo.pdf](http://www.cabinas.net/monografias/informatica/delitos_informaticos_ciberterrorismo.pdf)
8. TÉLLEZ VALDÉS, Julio, Derecho Informático, 3<sup>a</sup>.ed., Ed. Mc Graw Hill, México, 2003, Pág. 8
9. TÉLLEZ VALDÉS, Julio. Ob Cit. Pág. 09 y ss.
10. Wikipedia. “informática”, Recuperado el 6/10/2010 en <http://es.wikipedia.org/wiki/Inform%C3%A1tica.-%20>
11. Wikipedia, “Delito Informático” Recuperado el 1/10/2010 en [http://es.wikipedia.org/wiki/Delito\\_inform%C3%A1tico](http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico)
12. Ley Especial Contra Los Delitos Informáticos de Venezuela, recuperado el 1/10/2010 de <http://web.laoriental.com/leyes/L007M/L007mT1Cap0.htm>
13. proyecto de ley orgánica española, publicado en el B. O. del 15 de enero de 2007, Recuperado el 1/10/2010 de [http://www.boe.es/aeboe/consultas/bases\\_datos/doc.php?id=BOE-A-1996-1069](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1996-1069)
14. Decisión marco 2005/222/JAI del consejo de la Comunidad Europea, Recuperado el 1/10/2010 de <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0044:0048:ES:PDF>