

DAÑO VS. DAÑO INFORMÁTICO

Autores: Francisco Luís Frati- Analía María Elizabeth Mercado

I- SUMARIO:

I- Sumario. II- Introducción. III- Delitos Informáticos: Concepto IV- Daño informático o sabotaje informático: a) Bien Jurídico Protegido. b) Objeto. c) Acciones Típicas o medios comisivos. d) Elemento subjetivo. e) Sujeto activo f) Consumación y tentativa. g) Subsidiaridad - Especialidad. V- Difusión o Transmisión de Virus: a) Acciones Típicas. b) Objeto. c) Elemento Subjetivo d) Consumación y Tentativa. VI- Figura Agravada. VII- Conclusiones.-

I- INTRODUCCIÓN:

La ley 26.388, incorporó al C.P. en el Título VI: Delitos contra la propiedad, Capítulo VII: Daño, el segundo párrafo al art. 183 (daño informático y transmisión de virus), el inc. 5 (última parte) y el inc. 6 del art.184 introdujo agravantes a dicho delito. Esta ley creó delitos modificando ciertos aspectos de los existentes con el objeto de regular las nuevas modalidades delictivas que se valen de modernas tecnologías como medios de comisión¹, manteniendo la misma pena prevista para el daño tipificado en el art. 183 (al que podríamos llamar clásico).-

Con esta norma, nuestro país, siguiendo los antecedentes legislativos², adecuó su normativa a lo que desde hace años se había regulado en otros países³, encontrándose, de esta forma, un principio de solución al problema suscitado en la jurisprudencia⁴ que consideraba atípica la destrucción de datos o programas de ordenador o incluso la difusión de virus informáticos en redes informáticas.-

Este trabajo tiene por objeto analizar el delito de daño informático (art. 183, 2do. Parr. C.P.), comparándolo con la figura de daño clásico (art. 183, 1º parr C.P.), y así

¹ Fundamentos de Proyecto de Ley de Delitos Informáticos.-

² Ley 24.769, la ley 25.036, Ley Nº 25.286, Ley Nº 24.766.-

³ Alemania (1986), Estados Unidos (1986 y 1994), Austria (1987), Francia (1988), Inglaterra (1990), Italia (1993), Holanda (1993), España (1995), Chile (1993), Bolivia (1997), Paraguay (1997), Perú (2000), Costa Rica (2001), Venezuela (2001), etc.-

⁴ "Pinamonti, Orlando M.", JA 1995-III-236. Sala 6ta, 30/4/93; "Marchione, Gabriel la C. Nac. Crim. y Corr. Fed., sala 2ª, 15/11/2005" "Gornstein, Marcelo Hernán y otros s/delito de acción pública" Juzgado Nac.Crim.y Corr. Fed. Nº 12 Sec.24"

poder determinar si realmente se trata de dos figuras autónomas o si éstas comparten aspectos esenciales que hubiesen permitido hablar de un mismo delito al que se le podría haber agregado un nuevo objeto.-

III- DELITOS INFORMÁTICOS

Concepto:

Para Hugo Daniel Carrión “*Son todas aquellas acciones típicas, antijurídicas y culpables, que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien jurídico de naturaleza colectiva o macro-social (abarcativo de otros intereses, vgr.: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos, fe pública, etc.), en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas*”. Mientras que para el autor mexicano Julio Téllez Valdez los delitos informáticos son “*las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin*”.-

IV- DAÑO INFORMÁTICO o SABOTAJE INFORMÁTICO

Nuestro Código Penal en el art. 183 2º párrafo prevé dos tipos delictivos. En la primera parte contempla “*el acto de alterar, destruir, inutilizar datos, documentos, programas o sistemas informáticos*”, que es el que pretendemos analizar en el presente y que denominaremos “daño informático” y en la segunda parte, contempla *el acto de “vender, distribuir hacer circular o introducir en un sistema informático cualquier programa destinado a causar daño*”, que trataremos brevemente como “difusión o transmisión de virus”.-

a) Bien jurídico protegido:

Para algunos autores “*es el patrimonio que se ve privado de estos elementos o instrumentos inmateriales de suma utilidad y que son propiedad de los sujetos pasivos a quienes sirve para el desenvolvimiento de sus intereses personales*”⁵.-

Precisamente nos referimos al valor patrimonial que tienen esos objetos informáticos que enumera la ley que, pese a ser intangibles, sin dudas integran el patrimonio

⁵ BALCARCE, Fabián y Otros “*Derecho Penal Parte Especial*”. Córdoba, 2.009, t II, Pág. 136

del individuo y merecen protección penal. No debe ser confundido esto con el valor patrimonial que tienen los medios de almacenamiento (disco rígido, pendrive, memoria flash, etc) que generalmente es menor y quedarían incluidos en la figura clásica ya que estos constituyen cosas muebles. La acción típica del delito analizado afecta la información que ellos contienen, por ejemplo pensemos en el video digital de la fiesta de 15 años de una adolescente o el sistema de gestión de una empresa celular.-

b) Objeto:

En el año 2002, frente al ataque (hackeo) de la página Web de la Corte Suprema de Justicia de la Nación, nuestra jurisprudencia sostuvo que “...*la violación del sistema de seguridad de una página Web, reemplazándola por otra no encuadra dentro de la figura penal del delito de daño pues no es dable considerar a la citada página Web o a los datos o sistemas informáticos como "cosa" en los términos del art. 2311 del Cód. Civil, en tanto por su naturaleza no son objetos corpóreos ni pueden ser detectados materialmente...*”⁶.-

Previo a la reforma al art. 183 del C.P.A. donde se agrega en su 2º párrafo una nueva figura cuyo objeto serían bienes inmateriales o intangibles (datos, documentos, programas y sistemas informáticos), algunos autores estimaban que el art. 183 del C.P., al tipificar el daño a una cosa mueble, podía comprender algunas de las nuevas situaciones. En ese sentido debe recordarse que nuestros tribunales consideran “cosa” a la electricidad, los pulsos telefónicos y las señales de televisión o de cable (arg. cf. art. 3211 C.C.). De allí derivaría una posibilidad de aprehender típicamente algunas de las actividades que desarrollan los llamados *crackers* y *cyberpunks* (vándalos). Es así que para evitar el uso de la analogía prohibida, se habían propuesto varias alternativas: a) Una de ellas era agregar bienes inmateriales a la lista de elementos pasivos de daño (“...cosa mueble o inmueble, un animal *bienes inmateriales...*”), precisando a su vez en el art. 77 del mismo Código Penal que con este término se hace referencia a datos manejados en sistema informático;⁷ b) Incorporar una nueva figura delictiva -como se hizo posteriormente a través de la ley 26.388.-

Podemos hacer algunas consideraciones para comprender mejor el problema suscitado en razón de estos objetos inmateriales: uno siempre escucha: “se me lleno el disco, lo grave en el pen drive, cuanto espacio ocupa ese archivo de música”, parecería entonces que

⁶ “Gornstein, Marcelo Hernán y otros s/delito de acción pública” Juzgado Nac.Crim.y Corr. Fed. N° 12 Sec.24’

⁷ Proyecto de ley de Dip. **Marta OSORIO** 1225-D-05.

estamos hablando de cosas materiales que “ocupan un lugar en el espacio” y serian asimilables a cosas muebles, pero ello no es así.-

No hay duda sobre la materialidad de los objetos tangibles: pueden ser vistos, ocupan un espacio físico, etc., el conflicto se presenta con los otros objetos, los intangibles. Esta clase de “*objetos digitales*” no pueden percibirse directamente a través de los sentidos (es decir, no pueden verse, tocarse). Para poder “notar” su existencia se necesita de la ayuda de los objetos tangibles – en adelante *hardware*-. Por ejemplo, para leer una correspondencia electrónica o e-mail se necesita de un monitor o impresora que “*materialice*” el contenido, lo que permitirá al lector leer el mensaje. No obstante esta materialización no es más que la expresión de un objeto digital que persiste de alguna manera en medios de almacenamiento (magnéticos, electrónicos, ópticos) como lo son los discos rígidos, dvd, memorias flash, pen drive, etc. Lo que se logra a través de métodos físicos de escritura a través de un lenguaje específico de la informática llamado lenguaje binario (secuencia de bits, acrónimo de dígito binario por sus siglas en inglés). Pueden encontrarse en una computadora, celular, ipod, cámara digital o cualquier soporte digital con capacidad de contenerlos.-

Volviendo a nuestro tema debemos tratar de interpretar a que se refiere la ley con cada uno estos objetos informáticos inmateriales, a excepción de los documentos⁸ que el legislador definió claramente en la parte general del código. Un *dato* podemos decir que es cualquier información que tenga un significado tanto para una persona como para un programa o sistema (ej. Fotos, trabajos en Word, música, videos, base de datos, etc), *programa* es un conjunto de instrucciones y datos dispuestos de determinada manera para que cumplan funciones automatizadas de procesamiento de datos o ejecuten funciones preestablecidas (el juego buscaminas, un programa de consulta de padrón electoral) y sistema informático es una interrelación de programas, hardware y recursos humanos orientada a cumplir un fin determinado (sistema de gestión de alumnos de la Universidad, o el sistema de gestión de un supermercado).-

El daño clásico, requiere que la conducta recaiga sobre cosas “total o parcialmente ajenas”, pensamos que el legislador en el daño informático no quiso redundar en aclarar el requisito de ajenidad del objeto pues si fuese propio no habría necesidad de castigar el daño que se autoprovoca una persona a su patrimonio por ello debemos interpretar que los objetos informáticos sobre los que van a recaer las conductas típicas deben ser ajenos.-

⁸ "El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión" Según Art 77 Código Penal Argentino.-

c) Acciones típicas o modos comisivos:

En este delito, las acciones típicas son tres: “*destruir*” e “*inutilizar*”, no variando el significado de tales verbos en lo que respecta al daño clásico, pero a diferencia de él se agrega el término “*alterar*” y no se incluye “*hacer desaparecer*”.⁹ Concretamente “*alterar*” es realizar modificaciones en los objetos informáticos de manera que éstos no sean los que el operador ¹⁰ haya programado o creado o tengan menor rendimiento que el que corresponde, lo cual ocurriría si se modifica el contenido de una tesis realizada en Word; una fotografía, o un programa, por ejemplo Windows de manera que comience a funcionar más lentamente, se trata en definitiva de realizar cambios que no impliquen la destrucción ni la inutilización del objeto, modos que a continuación analizaremos; “*inutiliza*” el que realiza “*modificaciones, sin alterar su naturaleza o estructura*”¹¹, de tal magnitud que dañan la funcionalidad del objeto informático, de manera que ya no sirva para lo que fue creado, por ejemplo borrar la extensión de un archivo o parte de la base de datos de un programa; la modificación de una la imagen, que por su magnitud no permite que sea visible; un tema musical totalmente distorsionado. Por otra parte, “*destruir*” implica hacer que el objeto informático deje de existir, deshacer o arruinar de manera total o parcial la cosa alterando su naturaleza o estructura, por ejemplo borrar un documento de Word del dispositivo de almacenamiento (disco rígido, memoria, pen drive, cd.). Debemos tener presente que en la mayoría de los sistemas operativos la acción de borrar no implica que el hecho se produzca indefectiblemente, pues los archivos borrados se almacenan en una carpeta conocida como basurero o papelera de reciclaje y para poder concluir la acción de borrado de datos el usuario debe reconfirmar el borrado para eliminar los documentos e incluso en estos casos es posible recuperarlos en algunas situaciones. Entonces, si es posible recuperarlos, ¿el daño se ha producido? compartimos con algunos autores¹² que entienden que sí, pues la restauración requiere un esfuerzo que ya implica reparar el daño causado.-

⁹ El Código Penal español en su art 264. 2, emplea una redacción similar a nuestro art. 183, aunque empleando la expresión “o de cualquier otro modo dañe” dejando la posibilidad de que pueda ser cometido por acciones distintas a las expresadas en la norma, es interesante la redacción el art. 415 del Código Penal ecuatoriano que prevé “el que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenidos en un sistema de información o red electrónica...”.-

¹⁰ Por operador entiéndase a cualquier persona que utiliza la computadora, desde el simple usuario domestico que redacta un e-mail hasta los licenciados en sistemas que programan software.-

¹¹ CREUS, Carlos, ob. cit. pág. 574 - DONNA, Edgardo, ob. cit. pág. 761

¹² PALAZZI, Pablo A, “Los delitos informáticos en el Código Penal – Análisis de la Ley 26.388”, Buenos Aires, Abeledo Perrot, 2009, 1ª Edición, pág. 188.-

A diferencia de la figura de daño clásico en donde la enumeración es enunciativa concluyendo “o de cualquier modo dañare” dejando de esta manera la posibilidad que se cometa este tipo de delito a través de otras acciones típicas generadoras de la producción del resultado “Dañare”, en el daño informático la enumeración es taxativa quedando excluidas otras maneras de dañar como podría ser “hacer desaparecer”, es decir ocultarla de manera que el operador no tenga posibilidades de disponer de ella (sería el caso que se cambie de ubicación el dato, documento, programa o sistema o que a través de la función “ocultar” se la deje fuera de la vista), u otras acciones que al momento de legislar no se conocen y que con los avances de la tecnología pueden surgir de un momento a otro quedando de esta manera atípicas hasta tanto se realicen las actualizaciones pertinentes.-

Consideramos entonces, que no hubiese sido dificultoso subsumir el objeto informático dentro del párrafo del daño tradicional, pues prácticamente comparte las acciones típicas de este y gracias a su redacción, hubiese permitido compartir los modos comisivos enunciados o aquellas que posteriormente surjan encuadrados en la frase “...o de cualquier modo dañare...”.-

d) Elemento subjetivo:

En su aspecto subjetivo este delito comparte las características del daño clásico, es decir requiere *dolo específico*, de dañar el objeto informático. Es decir un dolo directo. No admite dolo eventual ni está prevista en este tipo la figura culposa que en otras legislaciones si la contemplan. No son necesarias motivaciones especiales ni finalidades trascendentes¹³.-

e) Sujeto Activo:

En cuanto al sujeto activo la ley, tanto en el daño clásico como en el informático, no hace distinciones especiales en cuanto a la persona que pueda ejecutar este tipo de acciones.-

Pese a ello nosotros podemos establecer algunas particularidades que presentan los sujetos activos de este delito informático. Se suele denominar “*Hackers*” (piratas informáticos) a los sujetos que producen daños informáticos de manera habitual o profesional; Esta denominación, que no es unánime y puede incluso analizarse y encontrarse muchas subclasificaciones que exceden el objeto de este trabajo, hace referencia a un grupo de

¹³ CREUS Carlos, ob. cit. pág. 573

personas que tienen aptitudes para el manejo de los sistemas informáticos que tienen conocimientos informáticos suficientes como para poder vulnerar los sistemas de seguridad o bien son personas que sólo cuentan con una computadora, acceso a Internet y habilidades en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.-

El agente puede aprovechar la falta de medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema, para producir el daño. Un ejemplo del segundo caso podría ser persona que consigue la contraseña del sistema de una inmobiliaria, ingresa en el y procede a borrar la carpeta “Clientes morosos”.-

El criminólogo Sutherland, ha catalogado estos delitos como “delitos de cuello blanco”, es decir, “*el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional*”¹⁴, denominación que puede ser descartada, ya que en la actualidad cualquier persona con medianos conocimientos de informática puede llegar a ser un delincuente informático, sin llegar a tener el status referido por Sutherland.-

f) Consumación y tentativa:

Es un *delito de resultado*, por lo cuál se consuma cuando se produce efectivamente el daño en los objetos informáticos, es decir, exige que el objeto sufra un detrimento funcional o estructural, sea leve (alterar), moderado (inutilizar) o grave (destruir).-

Admite tentativa. Podríamos enunciar algunos ejemplos: un sujeto realiza modificaciones en una planilla de Excel pero olvida guardar los cambios; o que intente desinstalar un programa, pero una vez confirmada la acción de desinstalar se apague la computadora a raíz de un corte de luz y que por ese motivo no llegue a consumarse el delito.-

g) Subsidiariedad - Especialidad

Respecto a la regla de subsidiariedad contemplado en el daño clásico la ley no lo tuvo en cuenta para el daño informático pese a no resultar incompatible con éste. Sin embargo el daño informático va a verse desplazado por el principio de especialidad cuando el daño sea realizado para cometer otros delitos informáticos, como el caso de destruir un correo

¹⁴ SUTHERLAND, Edwin, “*Teoría de la Criminología*”, Washington, Estados Unidos de América. 1943.

electrónico para obstruir una “comunicación electrónica”, o se altere un programa de un banco para que nos acredite capital a nuestra cuenta y así cometer un “fraude informático”.-

V) DIFUSION O TRANSMISIÓN DE VIRUS

En el presente haremos algunas observaciones a este tipo delictivo previsto en el art. 183 segundo párrafo segunda parte C.P.A, referido a conductas que implican un peligro abstracto y tiene como medio a los virus informáticos (programas destinados a causar daños).-

Aquí el legislador realmente innova en materia de daño ya que se castiga un “medio” para producir daños. Es decir no se castiga el daño producido sino instancias anteriores como lo son vender, distribuir, hacer circular e introducir en un sistema el programa dañino (virus) que potencialmente pueda producir daños-

a) Acciones Típicas:

En este delito, las *acciones típicas* son “vender”, “distribuir”, “hacer circular” “introducir”.-

Vende el que entrega un virus a otra persona a cambio de un precio, *distribuye* el que pone a disposición de un número determinado de usuarios este tipo de programas dañinos, *hacer circular* el que realiza lo anterior pero respecto de un número indeterminado de personas e *introduce* el que efectivamente coloca el virus dentro de un sistema informático.-

Podemos ejemplificar el “vender”, como la conducta de quien a cambio de un precio entrega a otra persona un virus para dañar los sistemas de la empresa telefónica de la competencia para que deje de funcionar cierta cantidad de días y así imponerse en el mercado, en tanto que “distribuir” la persona que entrega ese virus a los empleados de su empresa para que cumplan con su cometido; “hacer circular”: el que adjunta el virus a un mail para que se propague por todos los correos electrónicos; ”*introducir*”: una persona que coloca un virus en la computadora de la empresa en la que trabaja para que se active y destruya todo si es que él desaparece del listado de empleados

b) Objetos:

“*Son programas destinados a causar daños*”, podemos tomar la definición de virus según el contenido del artículo 2 de la Ley Especial Contra los Delitos Informáticos (LECDI), de la Gaceta Oficial No 37.313 de la República Bolivariana de Venezuela. Señala

que: “es un programa de computación o segmento de programa indeseado que se desarrolla, se multiplica, se auto-reproduce, se contamina incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente de un sistema.” como por ejemplo un *virus maker* o herramientas específicas de destrucción de datos, que son potencialmente dañosas. Por ende quien de alguna manera pone en el comercio un programa de tales características, con conocimiento del daño a producir, ayuda de alguna manera a cometer el delito de daño a quien usará la herramienta.-

Al hablar de la acción dañina de los virus debemos referirnos solo a la que recae sobre Software como refieren algunos autores en un sentido bien amplio, es decir, dato, documento, programa o sistema informático y no al Hardware ya que por tratarse de daños físicos quedarían incluidos en la figura de daño tradicional.-

No analizaremos los tipos y denominaciones ya que al ser múltiples, exceden nuestro trabajo, si diremos que un “*virus troyano*” puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada los cuales suelen ejecutar acciones ocultas e indeseables; un “*gusano*” (los más comunes), programas que se transmiten a través de las redes e Internet, se fabrican de forma análoga al virus troyano con miras en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus por que puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es tumor maligno, pero sus consecuencias suelen ser más graves. También se habla de *bomba lógica cronológica*: a través de ellas se programa que la destrucción o modificación de datos se produzca en un momento dado del futuro. Son las que poseen el máximo potencial de daño porque son las más difíciles de detectar antes de que exploten.-

c) Elemento Subjetivo.-

Coincidimos con el Dr. Palazzi, quien sostiene que también podría cometerse con *dolo eventual*: por ejemplo al introducir o distribuir un programa informático que está destinado y tenga capacidad de dañar, y que podrá replicarse y propagarse, el autor sabe que probablemente causará algún perjuicio pero desconoce su extensión y sus víctimas, el dolo entonces recae sobre el eventual daño que pueda causar el programa que libera y sobre su aptitud técnica para realizarlo¹⁵.-

¹⁵ PALAZZI Ob. Cit., pág. 194.-

En nuestra legislación, a diferencia de otras legislaciones¹⁶, no se contempla el tipo culposo, esto nos lleva a plantearnos algunos supuestos: es muy común que un usuario desprevenido reciba un mail indicando “*si lo reenvías a 10 personas ayudarás a un niño enfermo*”, y simplemente de manera ingenua obedece al texto del mail, reenviándolo, desconociendo que el mismo contenía un virus, propagándolo de este modo a sus contactos. En este caso, el usuario inexperto – que a su vez es víctima del virus que recibe en su computadora.- no tiene el conocimiento ni la intención de hacer circular este tipo de programas dañinos, sin embargo lo hace. Otro supuesto se daría respecto al usuario que mientras chatea, su computadora de manera automática envía una invitación a ver una foto o video, el interlocutor al aceptarla, haciendo click sobre el archivo, permite en forma automática que ingrese el virus a su computadora introduce a través del Messenger, inutilizando el sistema operativo Windows. La respuesta a tales interrogantes es que siendo la transmisión de virus una figura dolosa, no resultará punible quien sin conocimiento, o por negligencia en la protección de sus sistemas, resulte un involuntario distribuidor de código malicioso o sea utilizado como parte de una “botnet” (red de computadoras infectadas con código malicioso) u otro artilugio para realizar ataques masivos a sistemas informáticos.-

d) Consumación y tentativa:

El delito se consuma con la realización de algunas de las acciones típicas, ya que tratándose de un delito de peligro abstracto, aquéllas conllevan la presunción de la producción del daño.-

VI) FIGURA AGRAVADA

El art. 184 inc. 5 “...Ejecutarlo en datos, documentos, programas o sistemas informáticos públicos”, es decir, perteneciente, almacenados u operados por reparticiones públicas. Cuando dice “públicos” se refiere a cualquier dato, documento, programa o sistema, que se encuentre en computadoras o cualquier artefacto tecnológico con funciones de contenerlos de la administración pública, sea nacional, provincia, municipal y de cualquiera de las funciones del estado, ejecutivo, legislativo o judicial, Universidades, colegios, museos y de toda administración pública, establecimiento público o de uso público de todo género. La especialidad de la información protegida y la condición pública o de uso público de los establecimientos ameritan agravar la pena en estas hipótesis.

¹⁶ El derecho penal venezolano contempla el supuesto de sabotaje o daño culposo, en este caso la pena se reduce entre la mitad y dos tercios.-

El inc. 6 prevé “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”;

La agravante prevé como *acción típica* la de “ejecutar” (poner en obra) cualquiera de las acciones previstas en el art. 183 2º párrafo, 1º supuesto, pero en los sistemas informáticos destinados a cualquier servicio público, sea prestado por el Estado o por particulares, debido a la mayor incidencia que el daño informático pueda producir dado el número indeterminado de beneficiarios y por el papel decisivo que cumplen en la producción de la riqueza.- Este agravante tiene antecedentes tales como los reclamos de las grandes empresas prestadoras de servicio las cuales eran objeto de ataque de Hacker aficionados o profesionales contratados por la competencia para desestabilizar la prestación del servicio que brindan, se podría dar como ejemplo el caso de virus introducidos en los servidores de “Hotmail” que generan la imposibilidad de acceder a las casillas de correo electrónico. O mas grave aun seria servicios de salud en donde a través de virus obstaculicen la normal funcionamiento del sistema de una prepaga a través del cual hacen la derivación de ambulancias ante una emergencia.-

VII- CONCLUSIONES:

Podemos concluir que el delito de daño informático comparte casi todos los aspectos del delito de daño clásico, al que se le ha agregado un objeto y un nuevo modo de comisión, “*alterar*”. Creemos que hubiese sido más factible incorporar al daño clásico el término bienes intangibles, para que de esta manera sea alcanzado por el principio de la subsidiariedad “si no resultare un delito mas gravemente penado” y no hubiese quedado estático ante las tres acciones típicas previstas actualmente ya que la expresión “de cualquier modo dañare” incluida en el daño tradicional hubiese permitido adaptarse a las nuevas tecnologías.-

IX- BIBLIOGRAFÍA:

BALCARCE, Fabián y Otros “*Derecho Penal Parte Especial*”. Córdoba, 2.009, t II, Pág. 136-138.-

CREUS, Carlos, “*Derecho Penal-Parte Especial*”. Buenos Aires, 1.998, t I, Pág. 573 -578.-

DONNA, Edgardo Alberto, “*Derecho Penal-Parte Especial*”. Buenos Aires, t II B, Pág. 759 a 766.-

PALAZZI, Pablo A., “*Los delitos informáticos en el Código Penal – Análisis de la Ley 26.388*”, Buenos Aires, Abeledo Perrot, 2009, 1ª Edición.-

FERNANDEZ, Delpech Horacio, “*Internet, su problemática jurídica*”, Bs. As., Abeledo Perrot, 2004, 2º edición, Pág. 194-201.-

SOLER DE ARESPACOHAGA, José Antonio, “*Manual de Seguridad Informática*”, Bs. As., Bureau Internacional de información y negocios”, 1998, 1º edición, pág. 143-197.-

RIQUERT Marcelo Alfredo, “*Hacking, Cracking, E-mail y dos fallos judiciales que denuncian lagunas en la legislación penal argentina*” (en línea). Dirección URL: www.carlosparma.com.ar/index.php?...hacking-cracking-e-mail-y-dos-fallos-judiciales-que-denuncian-lagunas-en-la-legislacion-penal-ar

Ley comentada de delitos informáticos (en línea). Dirección URL: [www.sgp.gov.ar/contenidos/onti/.../Ley comentada delitos informaticos.pdf](http://www.sgp.gov.ar/contenidos/onti/.../Ley_comentada_delitos_informaticos.pdf)

RIQUERT Marcelo Alfredo “*Algo más sobre la legislación contra la delincuencia informática en Mercosur a propósito de la modificación al Código Penal Argentino por Ley 26388*” (en línea). Dirección URL: www.ciidpe.com.ar/.../DELINCUCENCIA%20INFORMATICA.RIQUERT.pdf

FIGARI Rubén E. “*Daño informático (arts. 183, 2º párr. y 184 incs. 5º y 6º del C.P. Ley 26.388)*” (en línea). Dirección URL: www.rubenfigari.com.ar/?p=219

Proyectos de Delitos Informáticos del año 2006 (en línea). Dirección URL: www.habeasdata.org/ProyectosDelitosInformaticos2006