DELITO INFORMATICO[1]
(Análisis comparativo con el delito de daños y otros tipos del Código Penal costarricense)

Alonso Salazar[*]
Licenciado en Derecho
Especialista en Ciencias Penales
Profesor Asociado de la Facultad de Derecho
Universidad de Costa Rica

(1) En el sistema jurídico costarricense, no se puede hablar del delito informático en sentido estricto, pues la legislación penal costarricense adolece de normativa en este campo. Igual situación se presenta en otros sistemas jurídicos, como por ejemplo el español. No obstante, se utiliza la terminología delito "informático" simplemente por conveniencia, pues casualmente uno de los objetivos del presente artículo es precisamente hacer conciencia de la necesidad de regularlo. Al respecto y en relación con el estado de la situación en España, se recomienda la lectura de la obra de Miguel Angel Devara Rodríguez, ***Manual de Derecho Informático***, Aranzandi Editorial, 1997.

(*) Dirección: Herr Salazar. Erwin Straße 13. Appartement Nr. 7. 79102 Freiburg im Breisgau. Deutschland.

SUMARIO:

A) Introducción

B) Algunos casos de criminalidad por computadora

C) Resumen

D) Regulación de la criminalidad por computadoras en la República Federal de Alemania

E) Síntesis

A) INTRODUCCION

Desde hace muchos años, se habla de la necesidad de regular algunas conductas que hasta el momento permanecen impunes, conductas que se vinculan de una u otra forma con el abuso, la destrucción, variación, modificación o utilización fraudulenta de programas o paquetes de cómputo (*Software*) o bien bases de datos, cuya información se encuentra protegida por leyes especiales o simplemente su acceso es restringido, sea por razones de privacidad, protección de los derechos individuales (*habeas data*), o que por cualquier otro motivo, como por ejemplo, fines comerciales, se desea proteger.(2) Los tipos penales tradicionales resultan inadecuados para encuadrar las nuevas formas delictivas,(3) la tecnología avanza a pasos agigantados, mientras las leyes penales se estancan y no dan respuesta a las nuevas formas de criminalidad que con ocasión de la utilización de los avances tecnológicos del mundo moderno, se encuentran a

---

(2) Es una idea difundida entre quienes se ocupan del tratamiento del derecho penal, que "en nuestros días, la criminalidad económica que tiene mayor trascendencia es aquella que se apoya en medios fraudulentos. Estos se han ido adaptando paulatinamente a las nuevas formas de delinquir que han surgido con los avances técnicos, de forma particular de los que se deben a la informática". BERDUGO Gómez de la Torre, Ignacio en GUTIERREZ Francés, María Luz, *Fraude Informático y estafa* (Aptitud del tipo de estafa en el Derecho español ante las defraudaciones por medios informáticos), Ministerio de Justicia, Secretaría General Técnica, centro de publicaciones, Madrid, 1991, p. 11.

(3) Ver CORREA y otros, *Derecho Informático*, Ediciones Depalma, Buenos Aires, 1987, p. 295. Cfr. con DEVARA, p. 287. También TIEDEMANN: "El concepto de criminalidad mediante computadoras, descrito sintéticamente en los párrafos precedentes, resume una nueva categoría de comportamientos punibles desde la perspectiva del medio empleado. Esa delincuencia opera a menudo sobre objetos intangibles, como activo en los bancos, secretos comerciales, como *know how* y otras informaciones. Por lo tanto, no debe sorprender que las normas penales existentes solo logren abarcar aquellos comportamientos en forma parcial y más bien casual, aunque con diferentes resultados en los diversos sistemas jurídicos", p. 129. Para el autor "con la expresión criminalidad mediante computadoras se alude a todos los actos, antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizados en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos, p. 122. Así TIEDEMANN, Klaus, *Poder Económico y Delito*, Ariel, 1985. Cfr. con GUTIERREZ, p. 598 sgtes.

disposición de criminales que se sirven de ellas. Estas formas de criminalidad por lo general tienen un carácter transfronterizo, por lo que el Comité de Ministros del Consejo de Europa, ha recomendado la armonización de manera intensa, tanto de la legislación como de la práctica en todos los países miembros, con el propósito de poder dar una respuesta adecuada al problema.(4) La pregunta que surge en este momento es: ¿ha sido el problema correctamente entendido?

De la respuesta que se dé a dicha pregunta, dependerá la o las soluciones que se puedan plantear al problema.

El presente artículo, no pretende de manera alguna, dar respuesta a la interrogante planteada, para ello se requiere una profunda y pormenorizada investigación, solo se pretende demostrar, por medio de la experiencia acumulada en otros sistemas jurídicos específicamente el Alemán, y unas pocas referencias a los sistemas español, italiano y estadounidense,(5) que en definitiva se requiere de regulaciones especiales, las cuales permitan sancionar a los infractores y que el tipo penal contemplado en el artículo 228 del Código Penal,(6) se encuentra muy lejos de ser la panacea al problema señalado.(7)

Para lograr el objetivo propuesto, en la primera parte del artículo se plantean 10 ejemplos de casos que se encuentran fuera del tipo de daños, y que han sido recogidos y documentados en otros países. En la segunda parte, se aportan algunos de los tipos penales, que en la materia existen en Alemania,(8) a efectos de que el lector, pueda tener una idea del tipo de regulación que existe en dicho país.

---

(4) Ver en este sentido la Recomendación R (89) 9, del Comité de Ministros del Consejo de Europa a los Estados Miembros del 13 de septiembre de 1989, durante la sesión 428ª, reunión de los Delegados de los Ministros, aparece citada por DEVARA, p. 284, nota Nr. 4.

(5) Otros países que contienen legislación en esta materia son la Nueva Federación Rusa de 1996 y el Código Penal Francés, que fue modificado mediante la Ley 19/1988 de 5 de enero, publicada en el Boletín Oficial del 6 de enero de 1988, que añadió los artículos 462.2 y 462.9. citado por DEVARA, p. 289, nota 10.

(6) Ley 4573 del 8 de noviembre de 1971.

(7) Posición que al parecer y según el diario *La Nación*, en su artículo del 30 de agosto de 1998 titulado *Vándalos informáticos actúan aquí*, es la de algunos profesionales en derecho, conocedores del tema. El artículo también se encuentra por medio de Internet en: http://www.nacion.co.cr/Inee/1998/agosto/30/paisl.html.

(8) Con algunas referencias al Código Penal italiano (Codice Penale).

B) Algunos casos de criminalidad por computadora

Los siguientes son casos y/o hipótesis de delitos cometidos por medio de la utilización de computadoras.(9) Para su identificación, han sido titulados y numerados, lo cual permitirá un adecuado manejo. Para cada caso, se presenta un pequeño comentario y explicación del por qué no se encuentra dentro de la regulación del delito de daños.

Caso Nr. 1. Manipulación en el ingreso de los datos a la computadora

El procesamiento de datos por medio de computadoras, supone en primera instancia la introducción y almacenamiento de los mismos. Se parte en este supuesto de una realidad, documentos, fichas,. hojas de trabajo, etc., que contienen la información. Esta información será luego ingresada a la computadora,(10) y éste por medio de los programas respectivos, procederá a ordenarla, archivarla, clasificarla y/o realizar operaciones aritméticas, mediciones, etc. Surge entonces aquí el problema de que en este supuesto, no se produce un daño en sentido estricto tal y como lo plantea el artículo 228 del CP (Código Penal), sino que por el contrario, si el autor altera la información que ingresa a la computadora y de esta forma obtiene un beneficio económico para sí o bien un perjuicio para un tercero, en el primer caso nos encontramos frente a una hipótesis de hurto (art. 208 del CP), pero nunca de daños. Tampoco sería posible sancionar por medio del art. 216 del CP (estafa), pues el tipo de estafa supone el engaño al sujeto pasivo, que realiza un acto dispositivo perjudicial para sí o para un tercero, y ese sujeto pasivo no puede ser una computadora. Si por el contrario, quien realiza la manipulación, no obtiene un beneficio con la conducta, no podría ni siquiera pensarse en la hipótesis de hurto, sino que la misma es impune.

---

(9) La mayoría de los casos han sido tomados de *Sieber, Ulrich, Computerkriminälitat und Strafrecht, 2., um einen Nachtrag ergänze Auflage 1980, Carl Heymanns Verlag KG, Köln Berlin Bonn München.*

(10) En cuanto al uso del término pareciera que se acepta tanto computador como computadora o bien ordenador, este último que se utiliza particularmente en España, no obstante, para nuestros efectos se seguirá empleando computadora, por ser el más comúnmente utilizado en Costa Rica. Al respecto puede consultarse Rothe, Martin, Rechtswörterbuch Spanisch-Deutsch 1996.

Este caso ya se ha vivido en Costa Rica. El sujeto A, quien labora en una dependencia estatal, manipula los datos y por medio de dicha manipulación, logra que el Sistema de pago de pensiones, todos los meses transfiera a la cuenta de su esposa una pensión a la que ella no tenía derecho alguno.(11)

Caso Nr. 2. Manipulación de datos ingresados a la computadora

En este supuesto, el autor manipula los datos de la computadora. Por ejemplo manipula la información de la cuenta de impuestos de un contribuyente, de manera tal que obligue a la Administración Tributaria a pagarle el contribuyente (devolución de los impuestos pagados), así se genera un beneficio para quien se encuentra obligado al pago de tributos. La manipulación se puede hacer al menos de dos formas, introduciendo información falsa a la computadora (ya tratado en el caso anterior) o bien, alterando los datos una vez que éstos han sido correctamente introducidos al sistema o bien eliminando información. En ninguno de estos supuestos se puede hablar de daños, por el contrario, la hipótesis se asemeja más a la estafa, con la salvedad ya apuntada de ausencia de agente pasivo (conducta atípica en nuestro sistema). Tampoco se podría hablar en sentido estricto de falsicación de documento art. 357 y siguiente del CP, pues el documento en sentido penal se define como "una idea aclaratoria incorporada" esto es, unida con una cosa, en general o así entendida, en sentido humano, apropiada y determinada, para dar seguridad en el tráfico y que deja reconocer a quien lo emite".(12) En este sentido, el documento como tal está compuesto por un elemento subjetivo, concepto o "idea aclaratoria" y un elemento material, "papel, cartón, etc." que permite transmitir la idea, más, aún, pareciera que la posibilidad de conocer al emisor es un elemento constitutivo del documento, con lo cual un anónimo estaría fuera del concepto. De esta forma, no podría admitirse que la base de datos de una computadora, pueda encajar dentro de la idea de documento. De tal forma, la manipulación de los datos ingresados a la

(11) El caso está a la espera de resolución judicial. Vgl. Fall Nr. 1, Kindergeld, en SIEBER, p. 47 y sgtes.

(12) Es la definición del Tribunal Supremo Federal Alemán, BGH 3, 85, 4, 285, 13, 239, 16, 96, 18, 66. Vgl. en ese sentido Dreher/Tröndle, StGB und Nebengezetze, 46 Aufl., § 267, Rdn. 2., S. 1596, también Lackner StGB, 20 Aufl., § 267, Rdn. 2, S. 1315.

computadora, no podría sancionarse como daños en sentido estricto, aun y cuando en realidad produzca un daño en términos económicos, pues en realidad la base de datos sigue intacta, solo que contiene datos alterados. Por otra parte, los datos contenidos en la base, no encajan en el concepto de cosa contenido en el tipo del art. 228 del CP.

Caso Nr. 3. Manipulación de Programas. (Técnica del Salami)[13]

En este caso, el autor no manipula ni altera los datos de la computadora, sino que por el contrario, la manipulación y/o alteración se genera en el programa. Un ejemplo de este caso, relativamente sencillo es el del empleado bancario, que altera el programa de cálculo de intereses de las cuentas de ahorro, de manera tal que solo los dos primeros dígitos de los decimales, se tomen como intereses y los restantes dígitos se transfieran a una cuenta, por él controlada. De esta manera tan simple, es posible obtener grandes sumas de dinero, pues los cuentahabientes no lo pueden detectar. Por otra parte, se puede aplicar a programas de redondeo, pensiones, amortizaciones, etc., es decir, se presenta para el inescrupuloso, una gama de posibilidades muy amplias. El problema al igual que en el caso anterior, es que el programa de cómputo como tal, no encuadra dentro del concepto de cosa en sentido estricto, con lo cual queda fuera del artículo 228 del CP. En todo caso, la alteración no está contemplada dentro de dicho artículo como uno de los verbos típicos. Por otra parte, no solo en los cálculos se puede alterar el programa, sino que es perfectamente posible lograr transferencias de fondos por medio de rutinas programadas, esto es, se puede programar una transferencia de fondos automática, de manera que en el programa se convierta en una rutina.[14]

Caso Nr. 4. Manipulación en los datos que salen de la Computadora. (Caballo de Troya)[15]

Cuando los datos se transfieren a otra computadora, en los programas de impresión (*output*), o en programas de actualización, es

---

(13) Así denominada por PARKER, D. Computer Crimes, Editorial Scribners, New York, 1980. Citado por DAVARA, p. 290, nota 13.

(14) Puede confrontarse en este sentido Sieber, *op. cit.*, Fall Nr. 4: Kontoüzichungs-Fall. El caso sucedió en el City Bank of Minneapolis, USA, 1966.

(15) Así, PARKER, *op. cit.*

decir, una vez que los datos son ingresados, ordenados y los procesos de cálculo elaborados, la información final, por lo general se imprime y almacena. Es posible manipular la información que se imprime y almacena, de manera tal que la alteración no pueda detectarse, durante el procesamiento de datos. Esta forma de comisión es una de las más complejas de detectar, pues por lo general se realiza en la etapa final de proceso. En programas de contabilidad, para citar un ejemplo, una vez que los datos del período son procesados, revisados contra los comprobantes y verificados, los mismos pasan a un proceso de actualización de saldos de cuentas, con lo cual se borran los movimientos del período y los saldos al final del período anterior se acumulan con los movimientos de ese período, generando un saldo inicial para el período siguiente. Esto es lo que se denomina *feedback* o retroalimentación, que es cuando la computadora asume, y aprovecha los resultados de un proceso, como fuente de información para otro nuevo tratamiento.(16) Si el programa es alterado en el momento en que los datos se actualizan, es muy difícil determinar la alteración, pues en la práctica se parte de la base, de que los cálculos de la computadora son los correctos y que el cuidado debe tenerse, precisamente cuando se introducen los datos al mismo. Esta forma de manipulación es prácticamente impensable en condiciones normales de trabajo y por eso suele pasar inadvertida, por lo general se descubre mediante la realización de un procedimiento de auditoría, por lo demás caro, lento, complejo y muchas veces tardío.

Caso Nr. 5. Intromisión en bases de datos

Otra hipótesis de criminalidad electrónica, constituye en la mera intromisión en bases de datos, las cuales contienen información no disponible al público, por ejemplo archivos médicos, criminales, de bancos, etc. Este tipo de información en manos de personas inescrupulosas genera, un alto riesgo pues con ella se pueden cometer una gran cantidad de conductas criminales. Piénsese solo en un caso: un delincuente o una banda de delincuentes, logra accesar la base de datos de un banco, por medio de la cual determina la frecuencia de los depósitos en la cuenta corriente de una empresa, de igual forma determina qué porcentaje de dichos depósitos se realiza en efectivo y qué porcentaje en otros valores, determina la hora del depósito y la agencia bancaria en la que los mismos se realizan. Con todos esos datos,

(16) Así, DAVARA, *op. cit.*, 293 sgts.

solo requerirán identificar al depositante y con seguridad darán un buen golpe. El simple acceso a la base de datos no genera por sí solo, un daño, pues más bien, las bases de datos estan diseadas parea ser accesadas, con lo cual se requiere de tipos penales específicos que sancionen la conducta.

Caso Nr. 6. Sabotaje de Computadoras (Bombas lógicas)

En 1973 en Estados Unidos de Norteamérica, cerca del 18% de los casos de criminalidad por computadora se encontraba en esta categoría.(17) Esta forma de criminalidad tiene por objeto la afectación o destrucción tanto del programa, como de los datos almacenados en la computadora, bien puede provocarse un daño al *hardware* o disco duro (en cuyo caso se podría hablar de daños en sentido del art. 228 del CP), pero la forma más común de comisión es a través del deterioro de los datos almacenados y los programas. En ausencia de archivos de respaldo y programas para la reinstalación y restitución del sistema, este tipo de criminalidad genera pérdidas enormes tanto para particulares, como pare empresas o instituciones. La forma de comisión más común es la intromisión de los denominados virus, que son programas que se almacenan o instalan en determinados sectores del *hardware y/o* programas de la computadora y que se encargan de destruir la información, inutilizarla o bien producir daños al mismo disco duro, que lo hacen inaccesable y/o inservible. Normalmente consisten estos virus en rutinas, instrucciones o partes de programas que se introducen a través de un soporte físico que los contiene, o a través de la red de comunicaciones, que pueden actuar en el momento o incluso con efecto retardado.(18)

Caso Nr. 7. Espionaje por Computadoras

Se puede afirmar que una de las mayores ventajas que el uso de computadores ha producido, es precisamente el poder almacenar, clasificar, ordenar y disponer de grandes cantidades de información en

(17) Así Parker, Don B./Nycum, Susan/Oüra, S. Stephen: Computer Abuse. Hgs., 1973, vom Stanford Research Institute, Menlo Park California 94025, citado por Sieber op. cit. 93 y sgtes.

(18) Más sobre el tema se puede encontrar en DAVARA, p. 294 y sgtes.

un reducido espacio y de manera inmediata. De igual forma, para muchas empresas, la información es uno de sus principales activos, que dicho sea de paso, no se encuentra valorado en libros y no existe en Costa Rica, la posibilidad de cuantificarla y dotarla de valor contable,[19] situación que desde el punto de vista legal, genera un problema de grandes magnitudes en cuanto a la determinación no solo del daño, sino de un posible resarcimiento. La forma posible de determinar el monto del daño causado, sería entonces por medio de la determinación de lo gastado en el restablecimiento de la información, no obstante, al restablecerse la información ésta se actualiza, y el valor de la actualización debe restarse al valor original de la información, esto pues, la información desactualizada no sirve y consecuentemente no tiene valor o por lo menos el que originalmente tuvo (se encuentra depreciada), p ero no cabe duda que como un todo, la información antes del daño era útil para su tenedor, con lo que no podría negársele un valor. Basta por ahora lo dicho, por no ser el objeto de este comentario, sin embargo se deja planteada la interrogante, para despertar el interés del rector en ese tema. De tal forma, por ejemplo, para una empresa, la información correspondiente a sus dientes, es quizás la más valiosa, esta información en manos de la competencia podría irrogarle pérdidas cuantiosas. Otra hipótesis, es el caso de empresas que invierten en el desarrollo de programas para hacer más eficiente su labor y obtener mayores ganancias, sin embargo, los programas e investigaciones, son transferidos a sus competidores de manera fraudulenta, así obtienen aquellas ganancias enormes al aprovechar la inversión de un tercero y disfrutan de sus beneficios. Ejemplos de este tipo de criminalidad es el caso de la British Overseas Airlines Corporation (BOAC) que en el año de

(19) Técnicamente es posible, pues se puede determinar el costo de la información, sin embargo las leyes fiscales no permiten registrarla como activos de la empresa, con signfficación contable, por lo que la elaboración de la información desde el punto de vista contable, se trata como un gasto de operación, pues se contabiliza como activos el equipo de cómputo como tal y los programas aquiridos, no obstante, en el levantamiento de la información y la elaboración de las bases de datos, tanto la mano de obra, energía eléctrica, depreciación del equipo de cómputo y demás gastos que se generan, se contabilizan como gastos de operación, que afectan de manera directa la Renta Bruta y por lo tanto, se reducen de impuestos para efectos de determinar la Renta Líquida Gravable, de tal suerte, que si se gmera una destrucción de los datos contenidos en una base determinada, no existe por lo general, la posibilidad de determiner el valor de la información y el mismo solo se puede estimar.

1968 invirtió cerca de 43 millones de libras esterlinas para desarrollar un programa que permitiera controlar en todas sus agencias alrededor del mundo, el itinerario de sus vuelos, conexiones, etc. Al poco tiempo de haberlo desarrollado, uno o varios de sus empleados le hicieron una copia y la vendieron a la competencia obteniendo ganancias de aproximadamente 2 millones de libras esterlinas.(20) De igual forma existen muchos otros casos en este mismo sentido.

Caso Nr. 8. "Estafa" Electrónica

Técnicamente no es ninguna estafa, por ausencia de un sujeto pasivo que realice el acto dispositivo, sin embargo, se asemeja a la hipótesis de la estafa triangular, la cual supone que el "engañado" y el estafado son personas diferentes. Sin embargo, en la estafa triangular el engañado tiene la facultad de realizar un acto dispositivo perjudicial para el estafado, de manera que el autor le produce a través de ese engaño, una lesión a su patrimonio y obtiene para sí o para un tercero un beneficio patrimonial antijurídico.(21) En el caso de la aquí denominada "estafa electrónica" lo que el autor hace es engañar a la computadora (que sustituye al sujeto pasivo), y produce con esto que la computadora realice un acto dispositivo perjudicial para un tercero, desde luego, pues para la computadora no puede existir un perjuicio patrimonial en ningún supuesto. El caso ya se conoce en Costa Rica: el acusado A formó una banda para la comisión de este tipo de fraudes. En asociación con B, logró instalar en un Club Nocturno (*Night Club*), una máquina capaz de copiar la información contenida en la banda magnética de determinadas tarjetas de crédito (de alto límite) seleccionadas por B (cajero del *Night Club*). Esa información era almacenada en la memoria de la máquina, luego transferida a una computadora, por medio del cual A, lograría transferir esa misma información a otras tarjetas de crédito, robadas por C y D, de manera tal que las tarjetas de crédito robadas (debidamente reportadas como tales) no serían determinadas por la computadora al ser utilizadas, toda vez que la información que contenían, era la de otras cuentas, de tarjetahabientes que tenían en su poder sus tarjetas y no habían advertido la copia de la información. De esta forma, al solicitar los

(20) Vgl. Sieber, *op. cit.*, pág. 101.

(21) Sobre la construcción dogmática de la estafa triangular, véase por ejemplo SCHROTH, Ulrich, Strafrecht Besonderer Teil, 2. Auflage, 1998.

dueños de negocios la autorización para la aceptación de la tarjeta cuando los delincuentes las utilizaban para comprar artículos de alto valor, las mismas eran aprobadas, pues la autorización se hace en la mayoría del los casos por medios electrónicos o telemáticos sin la intervención de personas. Los delincuentes fueron descubiertos por dos razones. Primero, por la reincidencia en la utilización de tarjetas adulteradas en un mismo establecimiento, en el que los propietarios habían sido advertidos del fraude después de la primera vez por las compañías administradoras de tarjetas y colaboraron para la detención de la banda. Segundo, por el hecho de que todos los supuestos perjudicados(22) habían asistido al mismo Club Nocturno, lo que permitió iniciar las investigaciones, de otra forma hubiese sido casi imposible dar con el paradero de la banda. En este caso solo se puede hablar, de una eventual falsificación de documento y uso de documento falso, para lo cual debería entenderse que la información contenida en la banda magnética es parte integral del documento, lo cual trae sus problemas, pues no encaja dentro de la definición de documento en sentido penal, claro es sin embargo, que no existe un delito de daños ni una estafa.

Caso Nr. 9. Compras por Internet

Hoy día existe en la Red Internet, una gama muy amplia de posibilidades de adquirir bienes y servicios, los cuales por lo general se pagan a través de tarjetas de crédito. Para pagar y ordenar el servicio, quienes ofrecen servicios o bienes por este medio, solicitan únicamente los datos del tarjetahabiente, nombre, número de tarjeta, fecha de vencimimiento y tipo de tarjeta, si todos esos datos coinciden, por lo general, sin ninguna otra verificación el producto se adquiere o se despacha. Desde luego el tarjetahabiente no advierte el hecho, sino hasta que el estado de cuenta es recibido y aparece el cargo hecho por la compañía administradora de la tarjeta. La situación se dificulta aún más, cuando existen tarjetas adicionales, o bien, el estado de cuenta es recibido por una persona distinta del tenedor de la tarjeta, pues muchas veces escapan al control, sobre todo cuanto el monto de los cargos no es muy elevado como por ejemplo, suscripciones a revistas, periódicos, programas de cómputo (*software*), etc.

(22) Una vez descubierta la manipulación, resultaron perjudicadas las compañías administradoras de tarjetas y no sus tenedores.

Caso Nr. 10. Divulgación de información y/o imágenes

En este caso, no se trata del daño o intromisión en bases de datos privadas, sino por el contrario, la utilización de bases de datos abiertas[23] con fines criminales. Por esa vía se pueden hacer circular a nivel mundial datos e imágenes, sin autorización de quien legítimamente puede darla, o bien como ha sucedido y que recientemente ha sido objeto de persecución policial a nivel mundial,[24] se hace circular pornografía. Desde luego en este caso, quedan a salvo los derechos de las víctimas en relación con los delitos contra el honor, sin embargo, es claro que la pena establecida en el CP es mínima en relación con el daño que se puede causar.[25]

C) RESUMEN

Como puede apreciarse, los casos planteados no son más que ejemplos de la gran variedad de formas de comisión y conductas eventualmente punibles, que como producto del avance tecnológico, son necesarias en nuestro sistema jurídico. En este sentido, de cara a la reforma del Código Penal Costarricense, es el momento de empezar a

---

(23) Para nuestros efectos, se denominarán bases de datos abiertas, aquellas que se encuentran a disposición de los usuarios por medio de las denominadas páginas World Wide Web (www) o Red Mundial, a las que se tiene acceso con solo establecer la conexión con un proveedor de Internet, o bien aquellas que como el Registro Público de la Propiedad, permiten su acceso a todos, siendo esa su función, o la base de datos de la Sala Constitucional, etc.

(24) Vgr. la así denominada, "Operación Catedral", con la cual se trató de desarticular una banda de pedófilos que actuaba a nivel mundial, la cual divulgaba imágenes pornográficas infantiles. En esta operación intervinieron entre otros: Gran Bretaña, Australia, Austria, Bélgica, Finlandia, Francia, Alemania, Italia, Noruega, Portugal, Suecia, Estados Unidos, Brasil, Dinamarca, España, Rusia, Canadá, Israel, Chile y Japón. Así *La Nación* Digital, "Golpe a red de pedófilos" en http://www.nacion.co.cr/In ee/septiembre/03/mundo4html y "Más arrestos en Alemania" en http:/h~ww.nacion.co.cr/ln_ee/septiembre/04/mundo4.html.

(25) El art. 146 del Código Penal señala una pena de 20 a 60 días multa al que deshonrare a otro o propalare especies idóneas para afectar su reputación.

estudiar y discutir, acerca de la necesidad de tipificar estas nuevas formas de criminalidad.[26]

D) REGULACION DE LA CRIMINALIDAD POR COMPUTADORA Y ELECTRONICA EN LA REPUBLICA FEDERAL DE ALEMANIA

Para nuestros efectos, todas las normas citadas pertenecen al Código Penal Alemán (Strafgesetzbuch, por sus siglas en alemán StGB, los artículos se citan con el símbolo de artículo §).

§ 152 a Falsificación de tarjetas de pago o formularios impresos de Eurocheques.

(1) Quien para engañar en el comercio o, para posibilitar un engaño de este tipo,

1. Copia o falsifica tarjetas de pago nacionales o extranjeras o formularios impresos de Eurocheques.

2. Proporciona para sí o para un tercero una de esas tarjetas de pago o formulario, la ofrezca para la venta, la ceda a otro o abuse de ella, será sancionado con pena privativa de libertad de un año hasta diez años.

(2) Si el autor actúa profesionalmente o como miembro de una Banda, que se ha constituido para la acción continua de delitos contenidos en el inciso 1, será la pena no menor a dos años.

(3) En los casos menos graves del inciso 1 será la pena de tres meses hasta cinco años, en casos menos graves del inciso 2 la pena privativa de libertad será de un año hasta diez años.

(4) Tarjetas de pago en el sentido del inciso 1 son tarjetas de crédito, tarjetas Eurocheques y otras tarjetas.

---

(26) "Si se concluye que es necesario definir nuevos tipos, este es el momento para hacerlo, pues durante los próximos meses se discutirá la Reforma al Código Penal y podrían introducirse, a través de mociones, normas sobre el tema". Otto Guevara, Diputado de la Asamblea Legislativa por el Partido Movimiento Libertario e integrante de la Comisión de Asuntos Jurídicos, citado por el Diario *La Nación* Digital en http://ww.nacion.co.cr/ln_ee/1998/agosto/30/paisl.html.

1. Que hacen posible, al librador garantizar el pago en el comercio y,

2. A través del perfeccionamiento o codificación se encuentran protegidas particularmente contra la falsificación.

(5) El artículo 149, en tanto se refiere a la falsificación de dinero y el 150 párrafo segundo se aplican correspondientemente.[27]

§ 202 a Espionaje de Datos

(1) Quien ilícitamente se apercibe de datos, los cuales no han sido para él determinados y que han sido protegidos contra el desautorizado acceso, por sí o por medio de un tercero, será sancionado con pena privativa de libertad de hasta tres años o con multa.

(2) Datos en el sentido del inciso (1) son solo semejantes, los que electrónicamente, magnéticamente o sino los que indirectamente perceptibles son almacenados o se transmiten.

§ 263 a Estafa por computadora[28]

(1) Quien con la intención de obtener para sí o para un tercero, una ventaja patrimonial antijurídica, para ello lesiona el patrimonio de otro, influyendo sobre el resultado de un procesamiento de datos por medio de una incorrecta organización del programa,[29] por medio de la

---

(27) Se refiere a la confiscación del dinero falso, en este caso las tarjetas adulteradas o falsificadas.

(28) El art. 640 ter. Codice Penale sanciona el fraude informático, el cual de acuerdo con la legislación italiana se puede producir alterando o modificando el funcionamiento del sistema informático o telemático, alterando de cualquier forma sus datos, informaciones o programas, permitiendo para sí o un tercero un injusto a través del daño. Crf. PALIERO, Carlo Enrico, Codice Penale e Normativa Complementare, Rafelo Cortina Editore, 1998 (en adelante citado como Codice Penale y el número de artículo).

(29) El Código Penal italiano sanciona con multa de hasta un millón de liras la alteración, modificación, cancelación en todo o en parte, así como impedir o entorpecer el funcionamiento de un programa de cómputo, como propiedad privada y se procede solo a instancia de la parte ofendida.

utilización de datos incorrectos o incompletos, por medio de la utilización no autorizada de datos o sino por medio de la influencia sobre la salida de los datos, será sancionado con pena privativa de libertad de hasta cinco años o con multa.

(2) Son aplicables los incisos 2 a 7 del artículo 263.[30]

§ 263 Estafa...

(2) La tentativa es punible.

(3) En casos especialmente graves la pena privativa de libertad será de seis meses hasta diez años. Un caso especialmente grave por regla general ocurre, cuando el Autor:

1. Actúa profesionalmente o como miembro de una banda, y ésta ha sido constituida para la comisión continua de falsificaciones de documento o de estafas.

2. Provoca una pérdida económica de grandes magnitudes y actúa con la intención, de provocar un peligro para una gran cantidad de personas en el sentido de pérdida de valor económico a través de la acción continua de estafar.

3. Provoca a otra persona un estado de miseria.

4. Abusa de capacidad o posición como empleado público, o

5. Manipula un caso de seguros, a través del cual él o un tercero con esa intención destruye total o parcialmente una cosa con valor económico en el sentido de la ley de incendios o por medio de su incendio o el hundimiento de un barco o su encayamiento.[31]

Mientras que en el art. 420 protege los bienes de utlidad pública y protege tanto el programa como los datos contenidos en una base, sancionando en tal caso con prisión de trece a ocho años. Ver art. 392 Codice Penale.

(30) Se acompaña la trducción de dichos incisos para mayor claridad del rector.

(31) El inciso 4, hace referencia al delito de robo en relación con cosas que se encuentran protegidas especialmente contra robos, así como al robo en la

§ 269 Falsificación de datos de considerable valor probatorio[32]

(1) Quien para engañar en el comercio, almacena o modifica datos de considerable valor probatorio, los que de acuerdo con su percepción hicieran existir un documento no auténtico o falsificado, o utiliza este tipo de datos almacenados o modificados, será sancionado con pena privativa de libertad de hasta cinco años o con multa.

(2) La tentativa es punible.

(3) Son aplicables el inciso tercero y cuarto del artículo 267.[33]

§ 267 Falsificación de documento.

(3) En casos especialmente graves la pena privativa de libertad será de seis meses hasta diez años. Un caso especialmente grave por regla general ocurre, cuando el autor:

1. Actúa profesionalmente o como miembro de una banda, y ésta ha sido constituida para la comisión continua de estafas o falsificaciones de documento.

2. Provoca una pérdida económica de grandes magnitudes.

3. A través de una gran cantidad de documentos no auténticos o falsificados pone en peligro la seguridad en el comercio, o

4. Abusa de su capacidad o posición de funcionario público.

---

casa de habitación y/o familia y la utilización no autorizada de un vehículo. Los incisos 6 y 7 hacen referencia a normas que contemplan la posibilidad de imponer una pena de multa y ampliación de la caducidad de la acción y el inciso 5 es exactamente igual al inciso 4 del art. 267 que se traduce más adelante.

(32) El artículo 491-bis del Codice Penale contiene una definición del documento electrónico, a diferencia de Strafgesetzbuch (StGB), el cual no contempla dicho concepto: "por documento electrónico se entiende cualquier soporte electrónico que contiene datos o información de eficacia probatoria o programas específicamente destinados a elaborarlos".

(33) Se acompaña la traducción de dichos incisos para mayor claridad del rector.

(4) Con pena privativa de libertad de un año hasta diez años, en casos menos graves con pena privativa de libertad de seis meses hasta cinco años será sancionado, quien actúa profesionalmente en la falsificación de documentos como miembro de una Banda, la cual ha sido constituida para la comisión continuada de delitos sancionados en los artículos 263 a 264 ó 267 a 269.[34]

§ 270 Engaño en el comercio por medio del procesamiento de datos. En el engaño en el Comercio se incluye igualmente la influencia en un procesamiento de datos en el comercio.

§ 303 a Modificación de datos.

(1) Quien ilegalmente (§ 202 a inciso 2) borre, suprima, inutilice o modifique datos, será sancionado con pena privativa de libertad de hasta dos años o con multa.

(2) La tentativa es punible.

§ 303 b Sabotaje de computadoras.

(1) Quien debido a que perturba un procesamiento[35] de datos con un significado esencial para una Empresa o una Compañía ajenas a la Administración Pública,

1. Él comete un delito de acuerdo con el artículo 303 inciso 1.

2. Un centro de procesamiento de datos o un almacenador de datos, deteriore, haga inservible, elimine o modifique, será sancionado pena privativa de libertad de hasta cinco años o con multa.

(2) La tentativa es punible.

---

(34) Artículo 263 estafa, 263 a estafa por computadora (el tipo completo se traduce más adelante), 264 estafa de subvención, 264 a estafa en la inversión de capital, 267 falsificación de documento, 268 falsificación de gravaciones técnicas y 269 falsificación de datos de considerable valor probatorio.

(35) El Codice Penale, en el art. 615 ter, sanciona el acceso abusivo a un sistema informático o telemático con una pena de uno a cinco años, dependiendo de si media la afectación de un servicio público, si se produce utilizando violencia sobre la persona o cosa, si del hecho se derive la destrucción,

E) SINTESIS

Como puede apreciarse, existen en la República Federal de Alemania, varios tipos penales que de una u otra manera protegen el procesamiento electrónico de datos, su manipulación, programas, bases de datos, e información. Particularmente importantes, resultan las regulaciones del Codice Penale, con el propósito de obtener una idea clara del camino a seguir. No se propone en nuestro caso, una copia directa de las normas citadas, y por el contrario, se propone la introducción en nuestra legislación, de normas que hagan posible un adecuado tratamiento del problema, sobre todo, teniendo presente el Legislador, que en esta materia, día con día se avanza en el plano tecnológico y se requiere de normas que brinden una correcta protección. En este sentido, se hace la observación a manera de conclusión de que el delito electrónico responde por lo general a tres características, que deben ser tomadas en cuenta como fundamentales, si se pretende elaborar una legislación apropiada:

a) Los delitos electrónicos, no responden en cuanto a su comisión, tentativa, consumación y agotamiento, con los delitos convencionales. Es perfectamente posible realizar una conducta de este tipo a distancia, por vías y canales electrónicos, traspasando las fronteras naturales, incluso continentales, utilizando la comuni-

---

tanto del sistema como de los datos, o si quien lo comete se encuentra en una posición de garante del sistema en relación con su resguardo o custodia. En el art. 615 quater, se sanciona la retención y difusión abusiva del código de acceso a un sistema informático o telemático (en este caso la pena puede ser desde uno hasta dos años o incluso desde 10 hasta 20 millones de Liras, en el caso de que se produzca un daño a un sistema utilizado por el Estado o un alto ente público esencial en el servicio público o de necesidad pública, o bien si es cometido por un empleado público, encargado del servicio con abuso de su cargo, violación inherente a sus funciones, circunstancias reguladas en los incisos 1 y 2 del párrafo 4°, art. 617 quater. Por su parte, el art. 615 quinquies con pena de hasta dos años o con multa de hasta 20 millones de Liras, a quien difunda programas tendientes a producir daño o interrumpir el funcionamiento de un sistema informático o telemático. Otras regulaciones en la materia se encuentran en los numerales 617 quinquies y sexies, así como en los art. 621 y 623 del Codice Penale, en relación con la intercepción y difusión de comunicaciones telemáticas e informáticas, de igual forma se sanciona su alteración y/o falsificación. El mero daño del sistema informático o telemático es sancionado por el art. 635 Codice Penale.

cación por satélite, etc. Se pueden programar rutinas a plazo, suspenderse, hacerse intermitentes, etc., es decir, la gama de posibilidades es muy amplia.

b) Existe una enorme facilidad para encubrir el hecho cometido, pues se puede actuar a través de seudónimos, usurpar cuentas ajenas, utilizar códigos de acceso no previstos. Por lo general no existen, desde el punto de vista probatorio, más elementos que los registros electrónicos. Los rastreos e intervenciones en las comunicaciones, son indispensables si se quiere combatir este tipo de criminalidad, además de que la acción inmediata de las autoridades debe estar prevista, puesto que un autor puede desplazarse muy fácilmente de un lugar a otro, sin ser sorprendido, por lo que la demora en trámites judiciales puede hacer ilusoria su captura.

c) Es muy fácil eliminar toda clase de pruebas de los delitos cometidos, por lo tanto, las reglas en cuanto a la apreciación de la prueba en este campo, requieren de una adecuada amplitud, no desde el punto de vista jurídico sino mental, así como su tratamiento, pues debe preveerse la incorporación de todo tipo de elementos probatorios.(36) No obstante, la naturaleza de la materia electrónica, hace necesario preveer como conducta punible de manera individual, el borrado de las huellas de una intromisión o comisión de un delito electrónico, hecho que cometido de manera dolosa, hace presumir la comisión del delito original o al menos su participación en él. El problema entonces es, cómo hacer coincidir esa presunción, por lo demás lógica, con el principio de inocencia consagrado en el art. 39 de nuestra Constitución Politica. Vuelvo en este punto al inicio. No se pretende brindar una solución al problema, es de por sí imposible en un corto análisis como éste, solo pretendo llamar la atención acerca de la ausencia normativa en este campo. Tiene la palabra el legislador.

(36) Situación que al menos de manera general se encuentra prevista en el art. 182 del Código Procesal Penal, al otorgar libertad probatoria en materia penal.