Informe de Investigación

Título: Delitos informáticos
Subtítulo: -

Rama del Derecho: Derecho Penal	**Descriptor:** Derecho Penal Especial
Tipo de investigación: Compuesta	**Palabras clave:** Delitos informáticos
Fuentes: Jurisprudencia, cuadro estadístico	**Fecha de elaboración:** 10-2009

Índice de contenido de la Investigación

1 Resumen

El presente informe se acompaña de jurisprudencia dsobre el delito de fraude informático. Sobre algunas características que se han tomado en cuenta para resolver su condenatoria o desestimar su existencia. Además se incluye un cuadro estadístico del Poder Judicial sobre los casos que ingresaron recurso de Casación por delito en el año 2007. Se complementa este informe con investigaciones previamente elaboradas por el equipo del CijulenLínea.

2 Doctrina

En el cuadro 27 [1] a continuación se observa el resumen estadístico del número de casos que llegan a Casación por delito. No se encuentra disponible información similar en materia penal juvenil, tampoco más reciente.

NÚMERO DE RECURSOS DE CASACIÓN ENTRADOS EN LA SALA TERCERA SEGÚN TIPO DE DELITO DURANTE EL 2007

Abandono incapaces	1	Homicidio simple	36
Abuso de autoridad	2	Homicidio tentativa	53
Abuso sexuales menores de edad	45	Hurto agravado	14
Abuso sexuales mayores de edad	2	Hurto simple	4
Abusos deshonestos agravados	1	Hurto simple (tentativa de)	1
Administración fraudulenta	12	Incendio	2
Agresión calificada	1	Infracción ley de armas	2
Agresión con arma	5	Infracción ley Migración	1
Amenazas agravadas	4	Injurias, calumnias, difamación por la prensa	17
Amenazas personales	2	Lesiones	3
Apropiación indebida	2	Lesiones culposas	7
Asociación ilícita	2	Lesiones graves	56
Cohecho	1	Lesiones gravísimas	4
Concusión	8	Lesiones leves	5
Contrabando	1	Peculado	10
Corrupción agravada	2	Penalidad del corruptor	1
Daños	4	Piratería	1
Daños agravados	1	Pornografía, difusión de	2
Denuncia calumniosa	4	Portación de arma	3
Desobediencia	2	Aportación de arma prohibida	1
Desobediencia a la autoridad	1	Privación de libertad	4
Difamación	2	Privación de libertad agravada	8
Drogas suministro	2	Receptación	1
Drogas, tenencia de	11	Retención indebida	3
Drogas, tráfico de	3	Resistencia agravada	10
Drogas, tráfico internacional	4	Robo agravado	263
Drogas, venta de	13	Robo simple	45
Ejercicio ilegal de la profesión	2	Robo simple, tentativa	3
Estafa	35	Robo agravado, tentativa	38
Estafa mediante cheque	3	Robo (tentativa de)	2
Estelionato	13	Secuestro	4
Extorsión	7	Suministro drogas	1
Extorsión (tentativa de)	1	Sustracción de menor o incapaz	1
Evasión	2	Tentativa de estafa	1
Falsedad ideológica	40	Trata de personas	3
Falsificación de documento	9	Uso de documento falso	22
Falsificación de moneda	1	Usurpación	3
Falso testimonio	2	Violación	21
Favorecimiento personal	2	Violación agravada	4
Favorecimiento real	1	Violación calificada	1
Fraude de simulación	14	Violación, tentativa de	3
Fraude informático	3	Violación de domicilio	3
Homicidio calificado	38		
Homicidio culposo	34	TOTAL	**1012**

Elaborado por: Sección de Estadística, Departamento de Planificación

Anuario de estadísticas judiciales 2007

3 Jurisprudencia

Res: 2007-01500[2]

Delito informático: Concepto en sentido amplio y distinción con el delito de peculado

Texto del extracto

“V. Dentro de su cuarto reclamo , alega “ aplicación indebida de las normas relativas al dolo y su incidencia con la calificación legal ” (cfr . Folio 7763). Según el criterio del recurrente, la conducta tenida por probada en el caso de los imputados Sequeira y Cascante, encaja en la figura del delito informático, figura penal que no estaba en vigencia para el momento de los hechos, razón por la cual debió declararse la atipicidad de la conducta, esto por cuanto “ quedó total y absolutamente probado que la desviación de los dineros ocurridos en la Tesorería Nacional lo fue utilizando medios informáticos, independientemente de la no probación (sic) de las funciones de los imputados Sequeira y Cascante, estos utilizaron todos los medios mecánicos-informáticos que se requerían para poder hacer los (sic) desviación, NO EXISTÍA OTRA FORMA DE HACERLO que no fuera por este medio … Justifica el Tribunal que no existió el delito informático porque la figura del 352 (sic) que regula el Peculado tiene los verbos SUSTRAER O DISTRAER y por consiguiente, teniendo Sequeira y Cascante la administración y custodia de los dineros “electrónicos” entonces su conducta no es atípica .”(cfr . Folio 7764). Siendo que el a quo condenó a los imputados por un delito que no se encontraba vigente para la fecha en la que acontecieron, solicita se dicte la absolutoria a favor de Sequeira y Cascante, y de todos los demás imputados, por atipicidad de la conducta. El reclamo es improcedente . Esta disconformidad con la calificación legal, ya había sido planteada ante el Tribunal por parte de la defensa técnica de algunos imputados. Ante esta situación, el a quo indicó en su sentencia: “ La defensa de los imputados alegó en sus conclusiones que la conducta de los imputados encuadra en el delito de Fraude Informático previsto en el numeral 217 Bis del Código Penal. Que como dicha norma no estaba vigente en el momento de los hechos, las acciones cometidas por los imputados eran atípicas. El Tribunal no comparte dicha apreciación. El artículo 217 Bis del Código Penal que contempla el delito de Fraude Informático, y que entró en vigencia el 24 de octubre de 2001, con posterioridad a estos hechos, dispone: “ Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema”. Con respecto a este tipo penal ya la Sala Tercera se ha encargado de delinear el delito informático. En el Voto 2006-148 dijo: “ En sentido amplio, el delito informático es cualquier ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como medio o como fin; como medio en el caso del fraude informático, y como fin, en el sabotaje informático (artículo 229 bis del Código Penal)…Si bien para la comisión de un delito informático se requiere un ordenador, ello no implica que siempre que en la comisión del hecho delictivo esté presente un computador, estaremos en presencia de un delito informático. Para mostrar un caso obvio, si se violenta un cajero automático para sustraer el dinero que guarda, no se cometerá un delito informático. De acuerdo a la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en influir en el procesamiento o el resultado de los datos de un sistema de

cómputo, a través de varias conductas que han de incidir en el proceso de los datos del sistema. Influir en el procesamiento o resultado de los datos será manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema. Por ejemplo, en el proceso de pagar el salario a los empleados habrá una serie de pasos a seguir, que si alguno se altera fraudulentamente, incidirá en el resto del proceso." El Tribunal tiene claro que el medio por el cual se cometieron los delitos, lo fue un sistema informático, se utilizaron las computadoras de la Tesorería Nacional para a través del Sistema de Pagos TEF y posteriormente el de Créditos Directos, digitar los pagos ilícitos logrando sustraer el dinero mediante el desvío a cuentas clientes que no correspondían. Todo ello por medio del sistema SINPE que es un sistema informático. Ahora bien, para el Tribunal en primer término, la conducta cometida por los imputados no era impune al momento de su comisión por el hecho de que el delito de Fraude Informático no estuviera vigente, ya que la misma encuadra en la acción de sustraer dispuesta en el tipo penal del artículo 352(sic). El numeral 352 (sic) (vigente en ese momento) describe como acción típica la de SUSTRAER O DISTRAER, por parte del Funcionario Público, dinero o bienes cuya administración, percepción o custodia se tienen por razón de su cargo. La acción de sustraer como ya se expuso contiene cualquier forma de apoderamiento, entre ellas la utilización de medios informáticos. Es una norma que además de proteger el bien jurídico patrimonio, también protegido en el delito de Fraude Informático, protege un bien jurídico adicional, que es la probidad en el manejo de los bienes públicos de parte de los funcionarios encargados… En el presente caso, precisamente los instrumentos informáticos fueron utilizados para influir en el procesamiento de datos y lograr sustraer el dinero de la Tesorería Nacional , dinero que estaba bajo la percepción y administración de los imputados Sequeira Castillo y Cascante Prada . El delito de fraude informático funciona como medio para cometer el delito fin, en este caso el Peculado, la sustracción de fondos públicos por parte de quienes los tenía a su cargo, lo que violenta un bien jurídico adicional al patrimonio, que es la PROBIDAD EN EL EJERCICIO DE LA FUNCION PUBLICA , EL CUIDO CON RESPONSABILIDAD DE LOS BIENES PUBLICOS . El delito de Peculado puede cometerse de varias maneras, dentro de ellas por medios informáticos, ya que la norma no excluye dentro del concepto de sustracción, tal posibilidad. De allí que estamos ante un concurso aparente de normas, en el cual prevalece la norma especial que protege además del patrimonio, un bien jurídico adicional que no contiene el delito de Fraude Informático, que es la PROBIDAD en el ejercicio de la función pública. Además, la norma del 352 (sic) contiene integramente (sic) a la del 217 bis (si la consideraramos (sic) aplicable por favorecer al reo), por proteger el patrimonio, pero además tener otros elementos del tipo que son especializantes , que protegen la probidad, como lo es la calidad de funcionario público, la administración, percepción y custodia de los bienes públicos... De manera que cuando se realizaron los hechos, la conducta si estaba sancionada penalmente, no siendo de recibo la tesis de la defensa." (cfr . Folios 7642 a 7645) . Como se aprecia, la forma en la cual el a quo descartó la existencia de atipicidad es acertada, ya que la conducta desplegada por los imputados y acusada por el Ministerio Público, encuadra de manera integral en el tipo penal de peculado, pues se tuvo por demostrado que Sequeira Castillo y Cascante Prada utilizaron las funciones de administración de los bienes que estaban en recaudo de la hacienda pública, para sustraer grandes cantidades de dinero. Además, como bien apuntó el Tribunal, el delito de peculado protege no sólo el erario público, sino también el deber de probidad en la función pública, bien jurídico tutelado, el cual forma parte del tipo objetivo en mención, todo lo cual se ajusta a la descripción de la situación por la cual se le impuso la sanción a los imputados Sequeira Castillo y Cascante Prada . Igualmente, es acertada la observación hecha por el a quo, cuando consideró que la utilización del medio informático, en este caso particular, fue la circunstancia a través de la cual se realizó la sustracción, y que su uso no genera per se la calificación que pretende el impugnante. Es por ello que, avala esta Sala la argumentación plasmada por el Tribunal en sentencia, considerando que el delito que se tuvo por probado, dentro de los límites de la verdad forense, fue el de peculado, encontrándose en la

plataforma fáctica descrita por los juzgadores, todos los elementos objetivos y subjetivos del tipo penal de peculado. Tomando en cuenta lo anterior, se declara sin lugar el reclamo de fondo planteado por el recurrente."

Res: 2007-00592 [3]

Delito informático: definición y alcances. Substracción y posterior utilización de tarjeta en cajero automático no lo configura

Texto del extracto

" III . […] En segundo lugar, el punto relativo al uso de tarjetas de débito y sus claves de identificación ya ha sido objeto de análisis por parte de la Sala. Así , en el fallo No. 763-06, de 9:20 horas de 18 de agosto de 2006, se expuso: " A juicio de esta Sala, la conducta tenida por probada – sustracción de la tarjeta de débito, obtención de la clave de ingreso, y uso de la tarjeta para conseguir en el cajero automático, dinero de la cuenta de la ofendida –, no es propia de dicha ilicitud [fraude informático], en vista de que [la acusada] Barrantes Barrantes no manipuló los datos del sistema, ni influyó en su procesamiento. Como se señaló en un caso similar: "En sentido amplio, el delito informático es cualquier ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como medio o como fin; como medio en el caso del fraude informático, y como fin, en el sabotaje informático (artículo 229 bis del Código Penal)... Si bien para la comisión de un delito informático se requiere un ordenador, ello no implica que siempre que en la comisión del hecho delictivo esté presente un computador, estaremos en presencia de un delito informático. Para mostrar un caso obvio, si se violenta un cajero automático para sustraer el dinero que guarda, no se cometerá un delito informático. De acuerdo (sic) a la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en influir en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas que han de incidir en el proceso de los datos del sistema. Influir en el procesamiento o resultado de los datos será manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema. Por ejemplo, en el proceso de pagar el salario a los empleados habrá una serie de pasos a seguir, que si alguno se altera fraudulentamente, incidirá en el resto del proceso. El usuario aparece al final de ese proceso, y en términos generales, no lo puede modificar. Para hacerlo, requiere el ingreso al sistema, y usualmente debe poseer ciertos conocimientos. Las personas que cometen delitos informáticos presentan algunas características que no tiene el común de las personas, como la destreza en el manejo de los sistemas informáticos, o una posición estratégica que le facilita el manejo de información restringida, o, en muchos casos, ambas ventajas. Por estos aspectos son considerados "delitos de cuello blanco". Esto por cuanto, además de la tecnicidad en el manejo de los sistemas, éstos se encuentran protegidos por mecanismos de defensa cuya vulneración requiere, usualmente, de conocimientos técnicos: "Esta predisposición de medios defensivos en forma general y la limitación que se puso a los delitos electrónicos nos permite inducir en forma clara que para ingresar a cualquier sistema sin la debida autorización (para el caso la simple intrusión resultaría el delito subsidiario de otros más graves como hacking o robo de información,

por citar algunos) implica necesariamente vencer una resistencia predispuesta del sistema colocada allí expresamente por razones de seguridad, - según expresan los programadores y constructores -." (Derecho Penal Informático, Gabriel Cámpoli , Investigaciones Jurídicas S.A., 2003, página 28). " (Sala Tercera, sentencia # 148-2006). Como se observa, el delito de fraude informático requiere algún manejo de los datos, o los programas, que afecta el proceso de los datos del sistema. Por su parte, la conducta tenida por acreditada, en el caso en estudio, es el apoderamiento ilegítimo de dinero ajeno, utilizando la tarjeta original, por medio de un ordenador, pero sin modificación, ni alteración de la información que éste contenía, de modo que indujera a error en el procesamiento o el resultado de los datos del sistema. La acción realizada es la misma que hubiera hecho la titular de la tarjeta de débito, para obtener el dinero, por lo cual la conducta tenida por cierta no se adecua al tipo penal considerado por el Tribunal. [...] Sobre la figura del hurto agravado : sostiene la recurrente, que se está en presencia del delito de hurto agravado, por el uso de la tarjeta de débito, como llave. Se tuvo por demostrado, que la imputada sustrajo la tarjeta de débito del Banco Popular, a la ofendida Bermúdez Quesada, logró que le proporcionara la clave o pin de dicha tarjeta, y con ese dato en su poder, usó la tarjeta y la clave para lograr que el cajero automático le suministrara el dinero que la perjudicada tenía en su cuenta, logrando obtener la suma de trescientos ochenta y cuatro mil colones, mediante tres transacciones (folio 77). El artículo 208 del Código Penal sanciona a quien se apoderare ilegítimamente de una cosa mueble, de un valor superior a la mitad del salario base, el cual para la fecha de los hechos estaba fijado en 136.600 .° ° (ciento treinta y seis mil seiscientos colones) (correspondiendo a 68.300.°° la mitad). La encartada se apoderó ilegítimamente, sin autorización, de cierta suma de dinero propiedad de la quejosa, usando para ello la tarjeta de débito sustraída , así como la clave que la víctima le había suministrado mediante engaño. La tarjeta fue el instrumento que permitió el acceso al dinero de la ofendida, la llave que liberó las defensas que lo protegían. Es por ello que la figura del hurto se agrava, de conformidad con el inciso 3 del artículo 209 del Código Penal, el que precisamente sanciona con mayor rigor a quien vulnera las barreras que el dueño o poseedor del bien ha establecido en su resguardo. Según la vigésima segunda edición del diccionario de la Real Academia Española de la Lengua , entre las acepciones del término llave , se contempla "instrumento, comúnmente metálico, que, introducido en una cerradura, permite activar el mecanismo que la abre y la cierra" . Define cerradura como "mecanismo de metal que se fija en puertas, tapas de cofres, arcas, cajones, etc., y sirve para cerrarlos por medio de uno o más pestillos que se hacen jugar con la llave; cierre". Como definición de cierre , contempla " Aquello que sirve para cerrar" . En el caso de los cajeros automáticos, el dinero se encuentra guardado dentro del aparato, y la entrega del dinero se produce tras la introducción de la tarjeta en la máquina, y el ingreso de la clave. Es decir, la tarjeta constituye la llave que introducida en la máquina, permite activar el mecanismo que dispensa el dinero. Es claro que la tarjeta cumple la misma función que una llave metálica, con ella se acciona tanto la puerta de ingreso, como el cierre del cajero, que una vez abierto, entrega la cantidad de dinero solicitada. Se está entonces en presencia del delito de hurto agravado . No podría hablarse de una estafa , pues, si bien la clave de la tarjeta fue suministrada gracias a una maniobra de la acusada, no hubo disposición patrimonial de parte de la víctima, sino que fue la acción de la acusada, sin conocimiento de la agraviada – sustraer el dinero del cajero – la que despojó a la perjudicada de su patrimonio. Para que se constituya la estafa, debe haber un nexo entre el ardid, el error y la disposición patrimonial, nexo que en este caso no se da: "El fraude, el error y la disposición patrimonial deben estar vinculados subjetiva y objetivamente. Desde el primer punto de vista, el autor debe usar el fraude para inducir, mantener o reforzar el error en la víctima, con el designio de lograr de ella una disposición patrimonial. Se trata de un delito doloso de intención. Desde el punto de vista objetivo, entre el fraude, el error y la disposición patrimonial, debe mediar una relación causal sucesiva. Existe esta relación si entre el fraude y el error y éste y la disposición patrimonial, media, respectivamente, una relación derivativa, sin interferencia de otra serie causal independiente y preponderante. Cuando

esto sucede en el caso concreto, existe fraude, y éste es eficaz" (Ricardo C. Núñez, Manual de Derecho Penal, Parte Especial, Lerner , 1978, página 238). Tampoco puede pensarse en una estafa al cajero automático, pues el artículo 216 del Código Penal, referido a la estafa, sanciona a quien " induciendo a error a otra persona o manteniéndola en él", es decir, el sujeto pasivo debe ser una persona, y no una máquina, como en este caso" . Las reflexiones transcritas son aplicables en el presente caso, pues, conforme se expuso, el a quo tuvo por cierto que Wilfredo Silva Arias logró apoderarse de la tarjeta de débito de la víctima y le dio uso para hacer retiros de dinero en cajeros automáticos, merced a que tuvo conocimiento de la clave de identificación personal del titular de la tarjeta. Ahora bien, conviene destacar que para sancionar el hecho como hurto agravado por el uso de la llave verdadera que fue sustraída, hallada o retenida, no se está acudiendo a analogía de ningún tipo (cual parece entenderlo la defensora y en virtud de que el tribunal se refirió a que la tarjeta era "semejante" a una llave). No se trata de que la tarjeta sea "similar" a una llave, sino que es una llave . Es un mecanismo complejo (en tanto se integra también con el número de clave o " pin ", que ha de digitarse como paso indispensable para cumplir su propósito), pero es, a fin de cuentas, la llave que permite extraer el dinero del cajero automático en que se encuentra."

Res: 2006-00763 [4]

Delito informático: definición y alcances. Substracción y posterior utilización de tarjeta para cajero automático no lo configura

Texto del extracto

"III.- En el motivo por inobservancia de normas sustantivas se reprocha indebida aplicación del artículo 217 bis del Código Penal, e inaplicación del numeral 209. Considera la impugnante, que el hecho tenido por cierto no es constitutivo de la conducta descrita en el numeral 217 bis del Código Penal, que se refiere a una estafa informática, aunque se titule fraude informático. Afirma, que cuando el tipo penal habla de "influir", se refiere a quien de alguna forma altere el normal funcionamiento de un procesamiento, o altere el resultado de los datos de un sistema de cómputo. Indica que en este caso el sujeto activo se limitó a seguir los pasos que realizaría el propietario de la tarjeta, para obtener el dinero, sin que en forma alguna influenciara en el sistema. Sostiene que la actuación del tercero que obtiene dinero de un cajero, será o no legal, no porque esa persona influya en el cajero, sino si tiene o no autorización del propietario de la tarjeta para sacar el dinero. Alega que la acción que se configura es la de hurto agravado, con utilización de "llave", sea la tarjeta. Se acoge el reclamo. Al realizar el análisis jurídico penal, el Tribunal afirma que la encartada hizo uso indebido de la tarjeta – al sustraerla de la cartera de la ofendida – así como de los datos del sistema de cómputo para ingresar a su cuenta, sea la clave o pin de esa tarjeta. Esa acción la considera constitutiva del delito contemplado en el artículo 217 bis del Código Penal, el cual dispone: " Se impondrá prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los

datos del sistema ". A juicio de esta Sala, la conducta tenida por probada – sustracción de la tarjeta de débito, obtención de la clave de ingreso, y uso de la tarjeta para conseguir en el cajero automático, dinero de la cuenta de la ofendida –, no es propia de dicha ilicitud, en vista de que Barrantes Barrantes no manipuló los datos del sistema, ni influyó en su procesamiento. Como se señaló en un caso similar: "En sentido amplio, el delito informático es cualquier ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como medio o como fin; como medio en el caso del fraude informático, y como fin, en el sabotaje informático (artículo 229 bis del Código Penal). "Por una parte, el National Center for Computer Crime Data indica que "el delito informático incluye todos los delitos perpetrados por medio del uso de ordenadores y todos los delitos en que se dañe a los ordenadores o a sus componentes". De igual forma, y siempre con ese carácter de generalidad y amplitud, la Organización para la Cooperación y Desarrollo Económico (OCDE) explica que el "delito informático es toda conducta ilegal, no ética o no autorizada, que involucra un proceso automático de datos y/o la transmisión de datos". Asimismo, William Cashion – estadounidense experto en informática – señala que el "delito informático es cualquier acto inicuo que no puede ser cometido sin un ordenador o que no existiría sin un ordenador o su tecnología" (Delitos informáticos, Carlos Chinchilla Sandí, Farben, 2004, página 27). Si bien para la comisión de un delito informático se requiere un ordenador, ello no implica que siempre que en la comisión del hecho delictivo esté presente un computador, estaremos en presencia de un delito informático. Para mostrar un caso obvio, si se violenta un cajero automático para sustraer el dinero que guarda, no se cometerá un delito informático. De acuerdo a la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en influir en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas que han de incidir en el proceso de los datos del sistema. Influir en el procesamiento o resultado de los datos será manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema. Por ejemplo, en el proceso de pagar el salario a los empleados habrá una serie de pasos a seguir, que si alguno se altera fraudulentamente, incidirá en el resto del proceso. El usuario aparece al final de ese proceso, y en términos generales, no lo puede modificar. Para hacerlo, requiere el ingreso al sistema, y usualmente debe poseer ciertos conocimientos. Las personas que cometen delitos informáticos presentan algunas características que no tiene el común de las personas, como la destreza en el manejo de los sistemas informáticos, o una posición estratégica que le facilita el manejo de información restringida, o, en muchos casos, ambas ventajas. Por estos aspectos son considerados "delitos de cuello blanco". Esto por cuanto, además de la tecnicidad en el manejo de los sistemas, éstos se encuentran protegidos por mecanismos de defensa cuya vulneración requiere, usualmente, de conocimientos técnicos: "Esta predisposición de medios defensivos en forma general y la limitación que se puso a los delitos electrónicos nos permite inducir en forma clara que para ingresar a cualquier sistema sin la debida autorización (para el caso la simple intrusión resultaría el delito subsidiario de otros más graves como hacking o robo de información, por citar algunos) implica necesariamente vencer una resistencia predispuesta del sistema colocada allí expresamente por razones de seguridad, - según expresan los programadores y constructores -." (Derecho Penal Informático, Gabriel Cámpoli, Investigaciones Jurídicas S.A., 2003, página 28). Según indica el doctor Chinchilla Sandí, dentro de esas conductas destacan la manipulación de los datos de entrada: conocido también como sustracción de datos, es el más común en vista de la facilidad para la comisión y la dificultad en el descubrimiento. No requiere de conocimientos técnicos en informática y puede realizarlo cualquier persona que tenga acceso al procesamiento de datos en su fase de adquisición; manipulación de programas: difícil de descubrir pues el sujeto activo ha de tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en introducir nuevos programas o nuevas rutinas. Un método muy usado es el denominado "Caballo de Troya", el cual consiste en implantar instrucciones de computadora en forma subrepticia en un

programa informático para que realice una función no autorizada al mismo tiempo que la normal; manipulación de los datos de salida: se lleva a cabo fijando un objetivo al funcionamiento del sistema informático, como el fraude a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos, lo que se hacía con tarjetas bancarias robadas. Ahora se usa equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y en las tarjetas de crédito" (Sala Tercera, sentencia # 148-2006) . Como se observa, el delito de fraude informático requiere algún manejo de los datos, o los programas, que afecta el proceso de los datos del sistema. Por su parte, la conducta tenida por acreditada, en el caso en estudio, es el apoderamiento ilegítimo de dinero ajeno, utilizando la tarjeta original, por medio de un ordenador, pero sin modificación, ni alteración de la información que éste contenía, de modo que indujera a error en el procesamiento o el resultado de los datos del sistema. La acción realizada es la misma que hubiera hecho la titular de la tarjeta de débito, para obtener el dinero, por lo cual la conducta tenida por cierta no se adecua al tipo penal considerado por el Tribunal. "

Res : 2006-0 0148 [5]

Delito informático: concepto en sentido amplio y distinción entre el fraude informático y el sabotaje informático

Texto del extracto

"VII.- Recurso de la licenciada Ivette Carranza Cambronero, fiscal del Ministerio Público : en el único motivo del recurso, reclama errónea aplicación de la ley sustantiva. Afirma, que los hechos tenidos por acreditados son típicos de una pluralidad de delitos de fraude informático. Considera, que se está ante ilícitos que protegen diferentes bienes jurídicos: el patrimonio en el delito de estafa y la buena fe en los de falsificación y uso de documento. Además, dice, se trata de acciones que se despliegan en diferentes establecimientos en momentos históricos disímiles, por lo que no se rigen por una misma finalidad, ni las diversas acciones resultan dependientes entre sí, sino que cada ilícito resulta agotado en sí mismo, en cada visita a distinto negocio comercial. Arguye, que se trata de un concurso de delitos de fraude informático, previsto en el artículo 217 bis del Código Penal. No se acoge el reclamo: Dos son los aspectos que la recurrente reclama: que se está en presencia de delitos informáticos y que estos concurren materialmente, por lo que no se trata de un delito continuado. A) Sobre el delito de fraude informático: Esta Sala considera que tal acción no es configurativa de dicho ilícito. La norma citada describe: " Se impondrá prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema ". En sentido amplio, el delito informático es cualquier ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como medio o como fin; como medio en el caso del fraude informático, y como fin, en el sabotaje informático (artículo 229 bis del Código Penal). "Por una parte, el National Center for computer Crime Data indica que "el delito informático incluye todos los delitos perpetrados por

medio del uso de ordenadores y todos los delitos en que se dañe a los ordenadores o a sus componentes". De igual forma, y siempre con ese carácter de generalidad y amplitud, la Organización para la Cooperación y Desarrollo Económico (OCDE) explica que el "delito informático es toda conducta ilegal, no ética o no autorizada, que involucra un proceso automático de datos y/o la transmisión de datos". Asimismo, William Cashion – estadounidense experto en informática – señala que el "delito informático es cualquier acto inicuo que no puede ser cometido sin un ordenador o que no existiría sin un ordenador o su tecnología" (Delitos informáticos, Carlos Chinchilla Sandí, Farben, 2004, página 27). Si bien para la comisión de un delito informático se requiere un ordenador, ello no implica que siempre que en la comisión del hecho delictivo esté presente un computador, estaremos en presencia de un delito informático. Para mostrar un caso obvio, si se violenta un cajero automático para sustraer el dinero que guarda, no se cometerá un delito informático. De acuerdo a la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en influir en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas que han de incidir en el proceso de los datos del sistema. Influir en el procesamiento o resultado de los datos será manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema. Por ejemplo, en el proceso de pagar el salario a los empleados habrá una serie de pasos a seguir, que si alguno se altera fraudulentamente, incidirá en el resto del proceso. El usuario aparece al final de ese proceso, y en términos generales, no lo puede modificar. Para hacerlo, requiere el ingreso al sistema, y usualmente debe poseer ciertos conocimientos. Las personas que cometen delitos informáticos presentan algunas características que no tiene el común de las personas, como la destreza en el manejo de los sistemas informáticos, o una posición estratégica que le facilita el manejo de información restringida, o, en muchos casos, ambas ventajas. Por estos aspectos son considerados "delitos de cuello blanco". Esto por cuanto, además de la tecnicidad en el manejo de los sistemas, éstos se encuentran protegidos por mecanismos de defensa cuya vulneración requiere, usualmente, de conocimientos técnicos: "Esta predisposición de medios defensivos en forma general y la limitación que se puso a los delitos electrónicos nos permite inducir en forma clara que para ingresar a cualquier sistema sin la debida autorización (para el caso la simple intrusión resultaría el delito subsidiario de otros más graves como hacking o robo de información, por citar algunos) implica necesariamente vencer una resistencia predispuesta del sistema colocada allí expresamente por razones de seguridad, - según expresan los programadores y constructores -." (Derecho Penal Informático, Gabriel Cámpoli, Investigaciones Jurídicas S.A., 2003, página 28). Según indica el doctor Chinchilla Sandí, dentro de esas conductas destacan la manipulación de los datos de entrada: conocido también como sustracción de datos, es el más común en vista de la facilidad para la comisión y la dificultad en el descubrimiento. No requiere de conocimientos técnicos en informática y puede realizarlo cualquier persona que tenga acceso al procesamiento de datos en su fase de adquisición; manipulación de programas: difícil de descubrir pues el sujeto activo ha de tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en introducir nuevos programas o nuevas rutinas. Un método muy usado es el denominado "Caballo de Troya", el cual consiste en implantar instrucciones de computadora en forma subrepticia en un programa informático para que realice una función no autorizada al mismo tiempo que la normal; manipulación de los datos de salida: se lleva a cabo fijando un objetivo al funcionamiento del sistema informático, como el fraude a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos, lo que se hacía con tarjetas bancarias robadas. Ahora se usa equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y en las tarjetas de crédito. Como se observa, la conducta implica cierto manejo de los datos, los programas, que incide en el proceso de los datos del sistema. Por su parte, la conducta tenida por acreditada en este caso, es el uso ilegítimo de la tarjeta original, por medio de un ordenador (cajero

automático), pero sin modificación ni alteración de la información que éste contenía, que indujera a error en el procesamiento o el resultado de los datos del sistema, así como el uso en diversos establecimientos, de la tarjeta verdadera, por parte de quienes la habían sustraído, haciéndose pasar la co-imputada, por su titular, lo que hizo incurrir en error a los vendedores, quienes hicieron entrega de los bienes que de esa forma se adquirieron. Por tanto, la conducta tenida por cierta no se adecua al tipo en referencia. B) Sobre el delito continuado: las múltiples estafas con la tarjeta sustraída, fueron consideradas por el Tribunal como delito continuado. Es claro que tanto en el concurso material, como en el caso del delito continuado, se produce un pluralidad de acciones típicas. Es por ello que algunos se refieren al delito continuado como “concurso continuado”, o “concurso material aparente”. Puede decirse, que se trata de un concurso material de delitos, en el que concurren aspectos que lo diferencian de éste. Francisco Castillo, en su obra “El concurso de delitos en el derecho penal costarricense”, afirma que el delito continuado es una excepción a las reglas del concurso real en el ámbito de los delitos que afecten bienes jurídicos patrimoniales. En efecto, lo que establece la diferencia entre uno y otro, es que los ilícitos en el delito continuado, han de ser de la misma especie, afectar bienes jurídicos patrimoniales, y que el sujeto activo persiga una misma finalidad, tal como establece el artículo 77 del Código Penal. Es decir, la conducta debe ser homogénea y con un fin unitario, que engloba todos los ilícitos, lo que lleva a valorarla como un solo delito, para efectos de sanción: “Para construir la figuraa del delito continuado, el legislador utiliza un elemento subjetivo, que une entre sí todos los delitos de la continuación: el agente debe perseguir con todos ellos “una misma finalidad”...En la hipótesis se trata, pues, de una ficción: el legislador traslada los efectos de un hecho (delito único) a otro hecho (pluralidad de delitos, en los que el agente persigue una misma finalidad). Pero tampoco la ley considera éstos unidos por la misma finalidad como una total unidad; por el contrario, restringe los efectos de los hechos así unidos, solamente a la consecuencia jurídica, que es la pena. Desde este punto de vista, podermos definir el delito continuado en nuestro derecho como una ficción restringida “quod poenam” (Francisco Castillo, obra citada, página 89). La figura surgió para atemperar la sanción en aquellos casos de reiteración delictiva en corto espacio de tiempo, y de forma semejante, pues se consideró que esas conductas repetidas son más reprochables que una sola, pero tienen menor contenido injusto que la suma de todas. En el caso bajo examen, se observa que los ilícitos perpetrados con la tarjeta de crédito, son homogéneos. En todos se opera de la misma forma, mediante compra, con la tarjeta sustraída, por parte de la co-imputada, quien se hacía pasar por la titular. Las acciones se llevan a cabo el mismo día, en un período de aproximadamente nueve horas, con pocos minutos entre una y otra acci ón , y en un reducido espacio territorial. Hay por tanto cercanía espacial y temporal entre las conductas, así como idéntico modo de operar. Siempre se presentan los tres acusados, en el auto propiedad de la víctima. Todos los ilícitos afectan a la misma persona, la ofendida Quirós Goicoechea, a cuya cuenta se cargan todas las compras. Desde el momento del despojo de las tarjetas, las acciones llevan la misma finalidad, violentándose con ellas los mismos bienes jurídicos, de contenido patrimonial en exclusiva, como en el caso de la estafa, y patrimonial y de otra índole en la falsificación y el uso de documento falso, por ser delitos pluriofensivos. El propósito de los acusados era la adquisición masiva de bienes, designio acordado de antemano. Como se afirma en el fallo: “Se trata en este caso concreto de delitos de la misma especie que lesionaron el mismo bien jurídico y patrimonio de la ofendida en donde los agentes persiguieron una misma finalidad mediante el mismo modus operandi ya descrito” (folio 1005). Por lo tanto, sin lugar el reclamo."

Res: 2004-00269 [6]

Delito informático: "Comunidad virtual" que ofrece por medio de internet servicios de índole sexual que involucra a menores. Validez de la utilización de mensajes recibidos por correo electrónico aportados por destinatario en la investigación y uso de agentes encubiertos

Texto del extracto

" III. [...] En lo que atañe al primer reclamo, debe indicarse que aún cuando el impugnante afirma que en casación no se trató el tema de lo que se había discutido durante el juicio, lo cierto es que el argumento esgrimido por el accionante es el mismo que se planteó en casación, cual es el de que la intervención de sus comunicaciones no se hizo con base en lo establecido en la Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones. Ya esta Sala, mediante sentencia Nº 2003-00457 de las 15:20 horas del 5 de junio de 2003 (visible a folio 276), resolvió expresamente ese punto al conocer el recurso interpuesto en su oportunidad y estimó que la utilización de los mensajes enviados por correo electrónico era válida. Precisamente porque ya se estableció en sede de casación que era válido utilizar la información contenida en los mensajes de correo electrónico es que deviene inadmisible este argumento que se presenta en revisión. Lo anterior acarrea la inadmisibilidad del segundo motivo planteado por Marín Rojas, pues él hace depender su reproche de que se declare la invalidez de la prueba derivada de los mensajes por correo electrónico, lo cual, debido a que el tema fue resuelto en casación, no puede hacerse y ello conlleva a tener el segundo reclamo como manifiestamente infundado. Exactamente lo mismo es lo que sucede con el tercer alegato, ya que lo que propone el accionante es que si es ilegal intervenir sus comunicaciones electrónicas, estas no podían ser utilizadas como prueba y tampoco lo podría ser la información conocida por quienes leyeron los mensajes. Lo que ocurre es que la utilización de los mensajes sí fue válida, tal como se indicó en casación y ello hace evidente que carezca de interés discutir si quienes los leyeron podían o no informar sobre su contenido, pues ya se determinó la validez de que los mismos constituyeran prueba durante el juicio. En cuanto al cuarto motivo, debe decirse que en casación también se indicó que no existe problema alguno en utilizar un agente encubierto para la averiguación de hechos como los que aquí interesan. Asimismo, se indicó que todo lo actuado en relación con los menores agraviados fue orquestado por los justiciables, sin que hubiese inducción alguna por las autoridades. También se explicó que no se había vulnerado de manera alguna la obligación del Estado por salvaguardar el interés superior del niño, pues lo que se hizo fue documentar el desarrollo de las actividades ilícitas de los encartados. Así, queda claro que todos esos puntos fueron resueltos cuando se conoció el recurso de casación. En cuanto al quinto motivo, debe indicarse que el accionante expone él mismo la carencia de sustento de su reclamo, pues de lo que él relata no se deriva la contradicción que alega. Como él dice, el Tribunal indicó que la veracidad del contenido de los correos electrónicos se comenzó a verificar con la entrega del disco compacto. Pero, como se ve, lo que se hizo fue verificar con elementos probatorios información con la que se contaba desde antes y en ese relato el gestionante no expone ninguna contradicción, lo que demuestra la irrelevancia y la carencia de interés del mismo; además, el petente nunca explica de qué manera incide eso sobre la veracidad de los hechos que se tuvieron por acreditados, lo que evidencia la falta de fundamentación del reproche. En cuanto al sexto motivo, el reclamante retoma el tema del agente provocador, problema que fue resuelto desde casación, pues en esa sede se indicó que nunca hubo inducción alguna de las autoridades estatales para que los encartados actuaran como lo hicieron."

Res: 2003-00457[7]

Delito informático: aplicación de la teoría del riesgo permite considerar lícita la información obtenida

Texto del extracto

" V.- [...]. Con respecto a la utilización de mensajes enviados por medio del correo electrónico, aportados por un particular como elementos de convicción, que proporcionan indicios suficientes para iniciar una investigación penal, debe apuntarse que el acceso al correo electrónico de las personas, al igual que otros medios de comunicación, están amparados por el derecho constitucional a la intimidad (artículo 24 de la Carta Magna). Dicha afirmación cobra mayor relevancia, si se tiene en cuenta el creciente volumen de correspondencia que circula de esa manera y las también progresivas capacidades de los particulares y del Estado, para seguir y controlar el texto o contenido enviado por ese medio. Empero, ello no significa que la tutela de la autodeterminación informativa sea irrestricta, pues en circunstancias excepcionales el titular de los datos puede consentir en que se difundan a terceros. Establecido este principio general, adicionalmente debe tomarse en cuenta, que cuando se ofrece una dirección de correos por Internet, dirigida indiscriminadamente a cualquier persona que desee tener contacto con otras personas, se parte del hecho de que se podrá acceder a ella en cualquier momento, desde cualquier lugar y con cualquier objetivo, incluso aquel para el que originalmente se decidió poner esa dirección en la amplia red mundial denominada Internet. Desde esta última perspectiva, quien haga esto acepta la posibilidad de que a dicha dirección pueden llegar mensajes de cualquier criterio, tema y calidad y por supuesto, correos provenientes de quienes investigan sucesos delictivos. Es el titular de la cuenta electrónica quien decide, caso por caso, si opta por responder o no mensajes de procedencia desconocida y eventualmente, iniciar comunicación con otras personas. Con ello, voluntariamente asume el riesgo de que, por las condiciones de anonimato facilitadas por la citada red, la persona con la que se comunique pueda ser o no, quien dice ser. Al dar inicio al intercambio de opiniones, textos, fotografías, vídeos y otros documentos, igual que como sucede con la correspondencia tradicional, quien los remite puede representarse como posible que el destinatario no lo reserve, máxime si como sucedió en la especie, las comunicaciones versaban sobre la estructura organizativa de un grupo criminal encaminado a corromper sexualmente a menores de edad y a intercambiar material pornográfico prohibido. En la especie sometida a examen, no existió una imposición indebida de las comunicaciones privadas de parte de los funcionarios encargados de realizar la investigación penal, pues es cierto que la correspondencia electrónica fue agregada a la denuncia, por la persona que había creado la cuenta virtual de correo. Llegado a este punto, conviene tener presente que en el ámbito de la doctrina y la jurisprudencia comparadas, se ha expuesto la denominada “teoría del riesgo” como excepción a la regla de los “frutos del árbol envenenado” , teoría ésta que como es sabido tiene aplicación, cuando para obtener el material probatorio se violenten derechos fundamentales de forma tan decisiva, que contaminen con la misma invalidez los actos probatorios o procesales derivados de la infracción procesal originaria (regla de exclusión probatoria). Esta teoría del riesgo, que impide considerar como ilícita la prueba obtenida, se fundamenta en que en todas las actividades cotidianas de comunicación entre dos o más personas, quien hace revelaciones extraprocesales y voluntarias ante un particular, respecto a un ilícito o realiza actividades relacionadas con éste, asume el riesgo de que el interlocutor lo delate, de forma que ese conocimiento pueda aprovecharse en las investigaciones originadas o que pueda respaldar. Sí debe aclararse, que carecen de valor

probatorio las manifestaciones vertidas por quien conoció los datos, en virtud de habérseles confiado por existir un deber de secreto profesional o en caso de que un funcionario omita cumplir una serie de garantías procesales de rango constitucional, estatuidas a favor de los justiciables (por ejemplo, una confesión policial sin contar con la presencia de abogado defensor, constituiría una prueba ilegítima). La teoría del riesgo se sustenta en el principio genérico de libertad probatoria y en el consentimiento tácito de quien puede prever que sus expresiones sean conocidas por otros, aunque no sean sus destinatarios originales. Es así como se ha afirmado, que: "... "El Tribunal Supremo español entiende que en esta hipótesis, el derecho a la intimidad es renunciado por el propio ciudadano que exteriorizó sus pensamientos sin coacción. Asimismo, que el derecho no podría prohibir que la exteriorización de propósitos delictivos sea mantenida en reserva por el destinatario de la charla, pues la ley no garantiza el secreto que una persona dice a otra, ya que nada impide que éste revele lo que hablaron, siendo irrelevante la forma en que se documenta ese diálogo..." (Sentencia 11/5/94, citada por Torres Morato: La prueba ilícita penal. Citado por Hairabedián, Maximiliano: Eficacia de la prueba ilícita y sus derivadas en el proceso penal , Editorial Ad-hoc, Argentina, 2.002, pág. 106-107). Así, si en el caso conocido en esta sede se comprobó que los acusados formaron parte de una "comunidad virtual" interesada en intercambiar información con cualquier persona que accediera a la página o los contactara vía correo electrónico (documentos e imágenes), para realizar actividades relativas a la instrumentalización de menores de edad, como parte de material pornográfico o como meros objetos para satisfacer sexualmente al grupo. Se autodenominaron incluso, como "boys lovers" y en los mensajes de correo electrónico aportados, se identificaron expresamente como "pedófilos". Como parte de sus funciones en la organización no gubernamental (O.N.G.), denominada "Casa Alianza", la funcionaria María del Rocío Rodríguez García localizó una página virtual del grupo identificado como "Comunidad Paidos" [...]. a la que pertenecían los imputados, estableció comunicación con ellos con el exclusivo interés de verificar que estaban implicados en actividades delictivas de contenido sexual, en detrimento de personas menores de edad. Tal como señala el Tribunal, a folio 81 de la sentencia: "... dado que dentro de esta página, la cual está abierta al público, aparecen todos los requisitos para suscribirse con el fin de intercambiar correspondencia con otros boylovers, la señora Rodríguez, se inscribe, identificándose como Roger Morales, pañameño, residente en Estados Unidos, de 43 años y de profesión Contador, y creó para tal fin, la cuenta de correo electrónico [...] ...". Fue así como recibió un primer mensaje de Cristian Araya Monge, quien se identificó como "boylover" o "pedófilo", quien a partir de ahí le narró quiénes integraban la agrupación, remitiéndole una serie de documentos para que aprendiera: "... el arte de abusar sexualmente a las personas menores de edad...", a la vez que le envió fotografías pornográficas de menores de edad, en donde aparecen adultos abusando sexualmente de niños entre los 3 o 4 años de edad aproximadamente y otras en las que figuran el propio Araya Monge y el menor de edad O.M., segundo apellido ignorado. (ver folio 82). Con esta información en su poder, María del Rocío interpuso la denuncia penal correspondiente y anexó la documentación indicada. Como dijo el Tribunal de instancia entre folios 130 a 134, no existió una intromisión indebida en las comunicaciones de parte de las autoridades, pues quedó demostrado que uno de los partícipes de la comunicación, a saber, la funcionaria Rodríguez García del grupo privado de cita, proporcionó los mensajes que a través del correo electrónico se habían dirigido a la cuenta creada por ella. Como queda expuesto en esta sentencia, los encartados asumieron - bajo su propio riesgo - la posibilidad de ser descubiertos al manifestar sus acciones delictivas. No lleva razón quien recurre, al argumentar que el proceso penal se impuso de aspectos íntimos de los acusados, pues lo cierto es que al establecer contacto con terceros, aquellos renunciaron a la tutela que ellos mismos podían desplegar en su ámbito de privacidad. Tal como lo ha indicado la jurisprudencia de esta Sala, resulta válido que una persona a quien se dirige una comunicación la aporte al proceso judicial, para que en él se la considere como un elemento de convicción. Así, se ha señalado que: "... El numeral 29 de la Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones establece en

su párrafo segundo lo siguiente: “Cuando el destinatario de una comunicación, mediante la cual se está cometiendo un delito tipificado por la Ley, la registre o la conserve, ésta podrá ser presentada, ante las autoridades judiciales o policiales, para la investigación correspondiente”. Como puede apreciarse, se extrae que el “propietario”, por decirlo de alguna forma, de una comunicación es quien la recibe. Sobre él pesa la responsabilidad de presentarla como elemento para una investigación. Claro está que si la presenta, se convierte en un elemento probatorio que debe ser discutido y al cual debe dársele el valor que corresponda luego de apreciarlo conforme a las máximas del correcto entendimiento humano. Asimismo, contrario a lo que estima el Tribunal, este derecho de registrar la comunicación que ostenta su destinatario no se restringe a los casos en que se investiguen delitos de Narcotráfico y de Secuestro Extorsivo, que son los mencionados en la Ley 7425. Si en ese párrafo se permite el registro en relación con “un delito tipificado por la Ley” y si la ley mencionada no tipifica delitos, entonces debe entenderse que se refiere a todos los delitos descritos y sancionados (es decir, tipificados) en las leyes penales, sea el Código Penal o cualquiera de las especiales ...” . (Sentencia

número 48-2.001, de 11:00 horas del 12 de enero de 2.001). (ii) Utilización de agentes encubiertos y grabaciones de vídeo en delitos de índole sexual: En otro orden de ideas, no existe infracción al debido proceso por utilizar a un agente encubierto para descubrir la forma en que se verificaron las infracciones, por no existir impedimento legal alguno para acudir a esta técnica, máxime cuando resulta útil para esclarecer hechos ejecutados en la clandestinidad, como los que aquí se comprobaron. Luego, si los responsables de la pesquisa determinaron que la reunión (“fiesta”) concertada debía realizarse en un apartamento perteneciente a “Casa Alianza”, al que llegarían los acusados en compañía del agente encubierto y de menores de edad, con el objeto de filmar los actos que ejecutarían utilizando un equipo de vídeo-grabación del que disponía el oficial encubierto, Jonathan Abarca Segura, debe acotarse que no existe ilegalidad alguna que reprochar. Cabe recordar, que para el caso no era necesario efectuar un registro previo del domicilio, de manera que se pudiera verificar la no existencia de droga en el sitio - como bien resolvió el sentenciador – quedando demostrado que los acusados fueron quienes llevaron y suministraron las sustancias ilícitas (confrontar folios 131 a 132). Ahora bien, esta forma de perpetuar las comunicaciones mediante su grabación, se conoce como “grabación ex-professo” o predeterminada, que son: “.... aquellas que se disponen como registro documental periodístico o de investigación, o como mecanismo de prevención y seguridad, o cuando existen, previamente, indicios serios y fundados que permiten sospechar que en un lugar determinado va a ser cometido o se está cometiendo un hecho delictivo, a los efectos de su registro a través de la imagen y de ser posible también de su sonido, para su posterior introducción al proceso penal como medio de acreditación de la plataforma fáctica delictual.(...) Las que derivan de las cámaras ocultas son aquellas que se han provisto de antemano para captar intencionalmente también hechos delictivos, rastros o circunstancias vinculados a él , que pueden ser operadas por particulares (ciudadanos o prensa) o por el propio Estado (fuerzas de seguridad) sin autorización legitimante del órgano judicial, ya sea que la cámara se oculte materialmente en un espacio público del Estado (por ej: en una plaza) o de particulares abierto al público (por ej: restaurant) o en un ámbito privado (morada), o en el cuerpo o efectos del propio cameraman situado en cualquiera de estos lugares...”. (Pascua, Francisco Javier: Escuchas telefónicas, grabaciones de audio subrepticias y filmaciones , Ediciones Jurídicas Cuyo, Argentina, 2.002, págs. 141 a 142). En el caso que ahora se resuelve, la actividad de investigación se limitó a registrar la conducta planificada de antemano por los acusados y ejecutada por ellos con pleno dominio del acontecimiento, sin que pueda sostenerse que las autoridades instigaron la comisión del ilícito o que toleraran la lesión de bienes jurídicos de los menores perjudicados. En realidad, la intervención policial, ejecutando la orden de allanamiento previamente dictada y contando con presencia de juez, fiscal y defensores designados al efecto, se efectuó para impedir que los sucesos llegaran a consecuencias dañosas ulteriores. Obsérvese, que la

argumentación del impugnante se torna contradictoria, al afirmar que no existió infracción alguna porque los menores – aún desconociéndolo - contaban con respaldo policial, pero a su vez sostiene, que los responsables fueron los funcionarios que consintieron en que se realizara el convivio. Con cualquiera de las dos opciones, lo que se pretende es exonerar de responsabilidad a los encartados. Sin embargo, esa posición carece de mérito, porque fueron los propios implicados quienes con sus conductas individuales y con planeamiento de grupo, realizaron los hechos reprochados en el fallo de mérito, sin que en ningún momento se les indujera a cometerlos. Bajo esta tesitura, tampoco existe irrespeto alguno a las garantías de los menores relacionados (“interés superior del niño”), ya que la acción policial se encaminó a documentar en vídeo lo que acontecía, cuidando evidentemente que no se ejecutaran actos contrarios a la voluntad de los menores asistentes al evento.

1 Poder Judicial. Departamento de Planificación y Estadística. Cuadro No. 27. Anuario de estadísticas judiciales 2007. Disponible en: http://200.91.68.19/planificacion/estadistica/judiciales/2007/Presentaci%F3nanuario2007final.htm

2 SALA TERCERA DE LA CORTE SUPREMA DE JUSTICIA. San José, a las quince horas treinta minutos del veinte de diciembre dos mil siete.

3 SALA TERCERA DE LA CORTE SUPREMA DE JUSTICIA. San José, a las quince horas cincuenta y dos minutos del treinta y uno de mayo de dos mil siete.

4 SALA TERCERA DE LA CORTE SUPREMA DE JUSTICIA. San José, a las nueve horas veinte minutos del dieciocho de agosto de dos mil seis.

5 SALA TERCERA DE LA CORTE SUPREMA DE JUSTICIA. San José, a las nueve horas del veinticuatro de febrero de dos mil seis.

6 SALA TERCERA DE LA CORTE SUPREMA DE JUSTICIA. San José, a las ocho horas cuarenta y dos minutos del veintiséis de marzo de dos mil cuatro.

7 SALA TERCERA DE LA CORTE SUPREMA DE JUSTICIA. San José, a las quince horas con veinte minutos del cinco de junio del año dos mil tres.