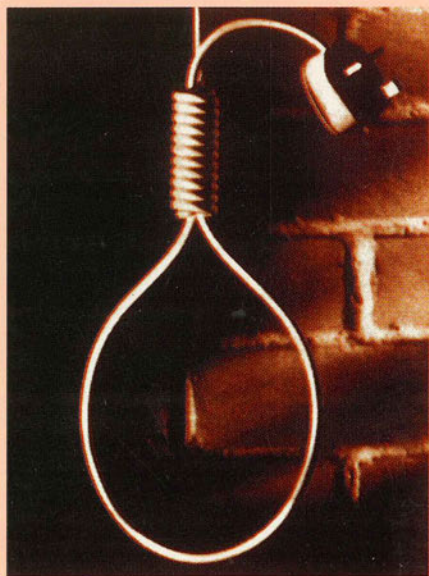


Luis Bramont-Arias Torres

El Delito Informático en el Código Penal Peruano



BIBLIOTECA DE DERECHO CONTEMPORANEO • Vol. 6



PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU



FONDO EDITORIAL 1997

La utilización cada vez más frecuente de las computadoras en los distintos ámbitos de la sociedad moderna, ha propiciado el surgimiento de una nueva forma de delincuencia: el «delito informático».

En el presente trabajo se realiza un análisis de los aspectos político-criminales de la criminalidad informática, haciendo especial incapié en la necesaria reacción del Derecho Penal ante este fenómeno criminal. Se estudia el concepto de delito informático, su relación con otras figuras delictivas clásicas —estafa, daños, falsificación de documentos, propiedad intelectual y hurto de uso—, para finalmente analizar dicha criminalidad recogida en el Código Penal peruano como un agravante del delito de hurto.

Este trabajo constituye un aporte al análisis de una nueva forma de criminalidad, a la luz de nuestro ordenamiento jurídico penal.

Luis Alberto Bramont-Arias Torres realizó estudios de postgrado en la Universidad Autónoma de Barcelona y en la Pontificia Universidad Católica del Perú. Es profesor de Derecho Penal —parte general y especial—, Derecho Procesal Penal y Criminología en la Pontificia Universidad Católica del Perú, Universidad San Martín de Porres, Universidad de Lima y Universidad Femenina del Sagrado Corazón.

Autores: [Faint text]
El Delito Infructivo
en el Código Penal
Peruano

BIBLIOTECA DE DERECHO CONTEMPORANEO

DIRECTOR FERNANDO DE TRAZEGNIES GRANDA

EDITOR RESPONSABLE GORKI GONZALES MANTILLA

Luis Alberto Bramont-Arias Torres

El Delito Informático en el Código Penal Peruano



PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FONDO EDITORIAL 1997

BIBLIOTECA DE DERECHO CONTEMPORANEO

Volumen 6

Copyright © 1997 por el Fondo Editorial de la Pontificia
Universidad Católica del Perú

Av. Universitaria cuadra 18, San Miguel. Lima-Perú

Telfs. 462-6390 y 462-2540, anexo 220

Derechos Reservados

ISBN 9972-42-040-X (obra completa)

ISBN 9972-42-043-4

Prohibida la reproducción de este libro por cualquier medio,
total o parcialmente, sin permiso expreso de los editores.

Diseño: *Edwin Núñez Ibáñez*

Primera edición: abril 1997

Tiraje: 1,000 ejemplares

Impreso en el Perú

ÍNDICE

INTRODUCCIÓN	11
--------------------	----

CAPÍTULO I

ASPECTOS POLÍTICO-CRIMINALES DE LA CRIMINALIDAD INFORMÁTICA	17
--	----

1. El delito informático como reto a una
concepción clásica del Derecho Penal 17
2. La criminalidad informática como nueva
forma de delincuencia: aspectos
criminológicos de este fenómeno 19
3. El delincuente informático 22
4. La víctima 24

CAPÍTULO II

CONCEPTO DEL DELITO INFORMÁTICO	27
---------------------------------------	----

1. Definición del delito informático 27
2. Relación con otras figuras delictivas 28
 - 2.1. Delito de estafa 28

2.1.1. Engaño, astucia, ardid u otra forma fraudulenta	31
2.1.2. Error	34
2.1.3. Acto de disposición patrimonial	37
2.1.4. Perjuicio	38
2.2. Delito de daños	39
2.3. Delito de falsedad documental.....	42
2.4. Delito contra la propiedad intelectual.....	46
2.5. Delito de hurto de uso	48

CAPÍTULO III

BIEN JURÍDICO PROTEGIDO EN EL DELITO INFORMÁTICO	51
--	----

1. Consideraciones generales	51
2. El patrimonio	51
3. El orden económico.....	55
4. El derecho a la intimidad de las personas	57
5. Toma de posición	58

CAPÍTULO IV

EL DELITO INFORMÁTICO EN EL CÓDIGO PENAL

PERUANO: ARTÍCULO 186, INCISO 3º, 2º PÁRRAFO	61
--	----

1. El patrimonio como bien jurídico protegido.....	61
2. Análisis del tipo objetivo	61
2.1. Comportamiento típico: remisión al tipo básico del delito de hurto (art. 185 CP)	61
2.2. Características particulares del delito de hurto desde el punto de vista de la criminalidad informática	65

2.2.1. El objeto material del delito	65
2.2.2. Comportamiento típico	67
2.2.3. Formas de ejecución de la conducta típica	68
a) Utilización de sistemas de transferencia electrónica de fondos	68
b) Utilización de sistemas telemáticos	69
c) Violación del empleo de claves secretas	70
2.3. Determinación de la relación de causalidad: definición del resultado	71
2.4. Sujeto activo	73
2.5. Sujeto pasivo	74
3. Análisis del tipo subjetivo. Dolo y elemento subjetivo del tipo	75
4. Grados de ejecución del delito. Consumación y tentativa	76
CONCLUSIONES	79
BIBLIOGRAFÍA	81

INTRODUCCIÓN

CASO N^o 1.- BARCELONA, 1989: Se detiene a tres jóvenes por extraer de varios cajeros automáticos una cantidad de dinero superior a tres millones de pesetas, por medio de maniobras de manipulación y falsificación informática (valiéndose de cartillas de ahorro falsificadas, provistas de bandas magnéticas también manipuladas con la ayuda de una computadora personal y una impresora). Mediante una pequeña computadora, los sujetos habían entrado en los sistemas informatizados de la entidad financiera, introduciendo en ellos números de cuentas ficticios, saldos irreales y claves bancarias que después codificaban en las bandas magnéticas de las cartillas falsificadas). Posteriormente, con estas cartillas extraían dinero de los cajeros automáticos que la entidad bancaria tenía distribuidos por la ciudad, para lo cual aprovechaban el corto lapso en el que los cajeros quedaban desconectados de la red principal (dato que conocía uno de los sujetos, empleado en una empresa de revisión y mantenimiento de cajeros automáticos)⁽¹⁾.

1 GUTIÉRREZ FRANCÉS. *Fraude informático y estafa*. Ed. Ministerio de Justicia, Centro de Publicaciones, Madrid, 1991, p. 27.

CASO N° 2.- Washington, 1977: Las autoridades del Distrito de Columbia anuncian que cuatro individuos han llevado a cabo un importante fraude informático, a través de manipulaciones de datos efectuadas desde un terminal de computadora de cierta entidad bancaria local. Tras seleccionar cuentas de ahorro que no habían registrado movimiento alguno durante un largo período de tiempo, habían transferido sus fondos a otras cuentas ficticias, abiertas por el grupo bajo nombres falsos, y de las cuales retiraron las correspondientes sumas con posterioridad. (Uno de los individuos había estado empleado en la institución afectada)⁽²⁾.

CASO N° 3.- El autor trabajaba como empleado técnico en la Sección de Asignaciones Familiares de una Oficina de Trabajo en el estado federado de Baviera. Tras falsificar las iniciales de otro empleado técnico, transfirió ilegalmente asignaciones familiares «por hijo», por un monto de entre 5,000 y 10,000 marcos alemanes, a diversas cuentas bancarias suyas o de miembros de su familia. La computadora efectuó las transferencias de acuerdo con sus instrucciones. En un período aproximado de diez meses, realizó veintinueve manipulaciones de ese tipo, mediante las cuales él y sus abuelos —de más de 80 años— se beneficiaron con más de 250,000 marcos. En 1973 fue condenado a la pena privativa de libertad de tres años por abuso de confianza continuado y falsificación de documentos en el ejercicio de un cargo público⁽³⁾.

CASO N° 4.- El autor era programador en una gran socie-

2 GUTIÉRREZ FRANCÉS. O.u.c, p. 23.

3 TIEDEMANN. *Poder económico y delito*. 1ª ed., Ed. Ariel, Barcelona, 1985, p. 124.

dad anónima alemana. Sirviéndose de un programa en el cual figuraban los datos de los salarios pagados por la empresa, introdujo informaciones sobre sueldos de personas ficticias y, como cuenta bancaria a la cual debían ser giradas tales remuneraciones, indicó su propia cuenta. Esta manipulación que podría efectuarse con éxito en numerosas empresas, habría sido detectada en la firma afectada, pues la computadora emitía formularios de sueldos, listas de control, resúmenes contables y balances, los cuales eran controlados y evaluados cuidadosamente por la misma empresa. Para evitar pues que la manipulación fuese advertida en esos controles, el autor modificó el programa de pagos de salarios de modo que no se emitieran formularios ni figuraran los sueldos de los empleados ficticios en las listas de control. Y, mediante otra manipulación en el programa que emitía los resúmenes contables y los balances de la empresa, logró finalmente que los importes escamoteados se dedujeran del impuesto sobre los salarios que se debía a la oficina tributaria respectiva y que, de este modo, no se observaran las diferencias resultantes. Hasta el descubrimiento el autor se apropió de 193,000 marcos. Fue condenado a la pena privativa de libertad de dos años por defraudación y abuso de confianza⁽⁴⁾.

En los casos anteriormente señalados puede comprobarse cómo el empleo de computadoras permite la ejecución de diferentes ilícitos penales, circunstancia que no es más que consecuencia del continuo y progresivo desarrollo del campo de la informática, aplicada en la actualidad a todos los aspectos de la vida cotidiana.

4 TIEDEMANN. O.u.c., pp. 124-125.

Así, la utilización de computadoras en la industria, el comercio, la administración pública, pero sobre todo en el sector de bancos y seguros, lleva también a la aparición de nuevas formas de delincuencia, representativas del ingenio y la habilidad de estos nuevos «delincuentes de computadoras». De esta manera, el mundo de la informática se convierte, por un lado, en un campo amplio y lleno de posibilidades para el futuro progreso, medio de avance en el desarrollo de la sociedad moderna; pero, por otro lado, se convierte en un factor de «riesgo», en cuanto fuente de nuevas formas de criminalidad, entre las que cabe citar la manipulación de computadoras, la destrucción o alteración de datos, la alteración de programas, etc.

Esta verdadera invasión de la computadora en todos los ámbitos de las relaciones socioeconómicas ha motivado que muchos hablen ya de una auténtica «era informática». En efecto, pocas dimensiones de nuestra vida no se ven afectadas, dirigidas o controladas por la computadora, ya sea de manera directa o indirecta; incluso, en determinados casos, las computadoras no sólo son utilizadas como medios de archivo y procesamiento de información, sino que además se les concede la capacidad de adoptar automáticamente decisiones⁽⁵⁾. Es por esta razón que en numerosas empresas los secretos comerciales más importantes estén almacenados en computadoras.

Por todas estas razones, analizaremos en el presente trabajo el delito informático, pero antes debemos indi-

5 En este sentido: SIEBER. «Criminalidad informática: Peligro y prevención». En: *Delincuencia informática*. Ed. PPU, Barcelona, 1992, p. 13.

car, ya el inicio, que dichos ilícitos son independientes de la conformación de los sistemas económicos, en la medida que se presentan allí donde se emplee una computadora.

Efectivamente, en la actualidad nos encontramos frente a conductas de personas que no pertenecen exclusivamente a sectores económicos privilegiados, con un elevado soporte financiero; el empleo cotidiano de la computadora ha propiciado el desbordamiento de este marco elitista inicial, como así lo ponen de manifiesto conductas cada vez más frecuentes e insignificantes como el regalo de computadoras que muchos padres hacen a sus hijos en la etapa escolar, su utilización en universidades, donde se ofrecen inclusive cursos y se programan carreras profesionales como ingeniería de sistemas.

En el presente trabajo se analiza el delito informático a partir de una serie de casos reales extraídos de la jurisprudencia. En el primer capítulo, se establecen los aspectos político criminales de la criminalidad informática, haciendo especial hincapié en la necesaria reacción del Derecho Penal ante este fenómeno, caracterizado por el empleo abusivo de la tecnología. Esto provoca también que tanto el delincuente informático como sus víctimas gocen de unas particularidades específicas que los distinguen del resto de los demás implicados en fenómenos criminales tradicionales.

En el capítulo segundo se precisa el concepto del delito informático y su relación con otras figuras delictivas tradicionales, como el delito de estafa, daños, falsedad

documental, delitos contra la propiedad intelectual y el delito de hurto de uso.

Por su parte en el capítulo tercero se precisa el contenido del bien jurídico protegido, a partir del análisis de las diversas posiciones doctrinales mantenidas a este respecto. Desde este punto de vista, se estudia el patrimonio, el orden económico y la intimidad como posibles bienes objeto de protección frente a las manipulaciones informáticas.

Por último, en el capítulo cuarto se analiza ya en concreto cómo está recogida en nuestro Código Penal la figura de la criminalidad informática, la cual está tipificada como un agravante del delito de hurto (artículo 186, 3º, segundo párrafo CP).

ASPECTOS POLÍTICO-CRIMINALES DE LA CRIMINALIDAD INFORMÁTICA

1. El delito informático como reto a una concepción clásica del Derecho Penal

El fenómeno informático es una realidad incuestionable y parece que también irreversible, la informática se ha instalado entre nosotros. El principal problema se traduce en buscar fórmulas efectivas de control, respecto a las cuales el Derecho ha de tener un marcado protagonismo, en su papel de regulador de las relaciones y mecanismos sociales para el mantenimiento de un orden social.

Nadie duda que el fenómeno informático produce en distintas ramas del ordenamiento jurídico (Derecho Civil, Derecho Procesal, Derecho Mercantil, etc.) un cierto trastorno a la hora de enfrentar tales hechos.

Tal es la problemática generada por este fenómeno que ha motivado en la actualidad la necesidad de recurrir al Derecho Penal a fin de disuadir del uso abusivo

al que lleva el empleo de computadoras, lo cual se ha plasmado ya en varias legislaciones extranjeras. No obstante, ante estas situaciones no puede olvidarse el principio del Derecho Penal como ultima ratio, lo cual significa que la intervención penal sólo está justificada cuando otras ramas del ordenamiento jurídico ya no pueden resolver los problemas que genera el fenómeno informático en la sociedad, de ahí que el Derecho Penal actúe como última instancia de control social.

En un primer momento, las figuras delictivas tradicionales, en particular los delitos patrimoniales, han tenido que hacer frente a esta nueva forma de criminalidad, pero, como veremos más adelante, éstas no ofrecen una delimitación típica completa frente a las nuevas conductas delictivas, razón por la cual en muchas legislaciones se tiende a crear tipos penales especiales, referidos al delito informático; entre éstas se encuentra nuestro Código Penal del 91, donde, no obstante, aún resulta difícil precisar jurídicamente tales conductas.

En términos generales, el fenómeno informático se puede analizar desde dos perspectivas:

- a) Delitos patrimoniales contra el sistema informático, donde el objeto de las conductas ilícitas es el soporte informático *-hardware-* y sus componentes lógicos *-software-*.
- b) Los delitos cometidos por medio del sistema informático, es decir, como instrumento que facilita, asegura o agrava los efectos de ilícitos tradicionales⁽¹⁾.

1 En este sentido: GUTIÉRREZ FRANCÉS. *Fraude informático y estafa*.

Nuestro marco de trabajo en la presente investigación va a desenvolverse básicamente dentro del segundo aspecto, esto es, en torno a aquellos ilícitos penales cometidos empleando el sistema informático.

Es indudable que la computadora puede ser el medio para la comisión de diversos ilícitos penales (por ejemplo, un delito de lesiones contra la persona a la que se le agrede arrojándole una computadora). Pero aquí analizaremos los supuestos en que la computadora es utilizada en su función propia, en cuanto permite el procesamiento de datos, la confección o utilización de programas para ello, como medio de comisión de delitos.

2. La criminalidad informática como nueva forma de delincuencia: aspectos criminológicos de este fenómeno

La criminalidad informática es de reciente aparición. Comenzó a manifestarse con los llamados «computer hackers», personas especialmente hábiles en el manejo de la informática, quienes, en un inicio, hicieron sonar la alarma en orden a la necesidad de reforzar la seguridad en los sistemas informatizados. A esto se une el continuo desarrollo tecnológico de los diversos países, el cual se ve potenciado cada vez más gracias al incremento de redes internacionales de comunicación electrónica de datos; la posibilidad de introducirse en tales redes, desde puntos muy remotos de países extranjeros, agrava

Ed. Ministerio de Justicia, Centro de Publicaciones, Madrid, 1991, pp. 44-45; GONZÁLEZ RUS. «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos». En: *Revista de la Facultad de Derecho*. Universidad Complutense de Madrid, Monográfico sobre Informática y Derecho, nº 12, pp. 107-164.

los problemas de descubrimiento y persecución de estas conductas⁽²⁾.

En el fenómeno informático es necesario resaltar los siguientes aspectos criminológicos:

2.1. Un primer aspecto es el riesgo que gira en torno a la «información» que los nuevos sistemas informáticos potencian, desarrollan y revalúan. No constituye ninguna novedad afirmar que actualmente las computadoras almacenan una gran información, del más variado contenido. El peligro surge con la utilización abusiva de la información relativa a los ciudadanos, circunstancia que en muchos casos puede colisionar con el sistema de garantías fundamentales del ciudadano, propio de un Estado de Derecho.

Desde este punto de vista, «información» significa «poder», en la medida en que aumenta la capacidad de control sobre los individuos⁽³⁾. La informática es una nueva forma de «poder», el cual puede estar concentrado u difuminado en una sociedad, confiado a la iniciativa privada o reservado al monopolio estatal.

Así, la informática multiplica el poder de quien se vale de la información, pero, al mismo tiempo, crea y acentúa las desigualdades y pone en entredicho los derechos y garantías individuales que debe existir en un Estado social y democrático de Derecho.

2 GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., p. 137.

3 Véase al respecto: GUTIÉRREZ FRANCÉS, *Fraude informático*. Op. cit., pp. 43, 63 y 67; JIJENA LEIVA. *Chile, la protección penal de la intimidad y el delito informático*. Editorial Jurídica de Chile, Santiago de Chile, 1992, pp. 45-46.

- 2.2. En la mayoría de los casos, la comisión de un delito informático se detecta de manera casual. Y cuando ello ocurre, sobre todo si la víctima resulta ser una persona jurídica, no se presenta la correspondiente denuncia debido tanto a la publicidad que puede generarse y manchar su reputación, como a la misma desconfianza existente en la eficacia de los órganos jurisdiccionales. Así, la denuncia de la ejecución, realizada dolosamente, por ejemplo, de una transferencia de dinero de una cuenta corriente a otra en una institución bancaria de reconocido prestigio, unida a la publicidad que pudiera hacerse del caso, puede motivar a muchos clientes de dicha institución al cierre de sus cuentas o bien disuade a otros futuros clientes de la apertura de nuevas cuentas por la desconfianza que provoca su sistema de seguridad.
- 2.3. Es importante también indicar que este tipo de delincuencia informática normalmente produce un gran daño a la víctima, sobre todo de carácter económico. Esto trae como consecuencia lo siguiente:
- 2.3.1. Si denuncian los agraviados por estos delitos, no es con la finalidad de recuperar el dinero por el daño causado, sobre todo si se tiene en cuenta que en el proceso judicial, el monto de la reparación suele ser inferior al efectivo daño causado, y porque, al ser condenado este sujeto a una pena privativa de libertad, deja de trabajar, por lo que, con mayor razón carecerá del dinero necesario para reparar el daño causado. De ahí que el motivo de la denuncia de estos hechos, ante todo, es castigar al sujeto con una pena.

2.3.2. Por otro lado, y por lo que respecta al daño o perjuicio ocasionados por estos delincuentes, estos son de tal magnitud que crean una mayor alarma en los miembros de la sociedad.

3. El delincuente informático⁽⁴⁾

La sociedad ha confeccionado su propio estereotipo del autor de la delincuencia informática: adolescente, de clase social media, inofensivo, con ausencia de toda conciencia de estar obrando mal, inteligente, casi siempre varón. Es una persona con un coeficiente intelectual próximo a la genialidad y con gran dominio del complejo mundo de las computadoras.

Si se mantiene este estereotipo, quedarían fuera de la delincuencia informática muchos comportamientos realizados por personas que no cumplen las características anteriormente indicadas, y que, no obstante, son frecuentes dentro de este ámbito, como puede ser el caso en el que X le sustrae la tarjeta del cajero automático a B, encontrando la clave anotada en un papel, o simplemente, la obtiene usando la violencia. En tales casos, X puede no saber nada de informática, pero de igual forma se vale de medios informáticos para sustraerle el dinero a B.

Este supuesto es diferente de aquél en el que una persona desactiva la alarma de una institución bancaria, logrando después sustraer el dinero; o de aquél otro donde la persona ingresa a la base de datos del banco y transfiere dinero de otras personas a su cuenta corrien-

4 Véase al respecto: GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., pp. 74-76.

te. En todos estos casos, el sujeto ha de tener un cierto conocimiento de informática para realizar tales actos, lo cual significa que cualquier persona no hubiese podido realizar la conducta descrita.

De ahí que en la actualidad se afirme que la delincuencia informática no es algo exclusivo de personas especialistas en informática, quienes, por otro lado, no tienen porqué ser necesariamente personas de gran inteligencia.

De otro lado, hay que reconocer que los primeros delitos informáticos recayeron en sistemas de gran importancia: la NASA, y el Departamento de Defensa de los Estados Unidos. Dado estos actos y los avances de la tecnología, cada vez se da más importancia al tema de la «seguridad» dentro de los sistemas informáticos, lo cual hace más difícil el acceso a los distintos programas.

Sin embargo, últimamente también se habla de un delincuente profesional dentro del ámbito informático, en la medida que los comportamientos de estas personas están relacionados con el crimen organizado, relativo sobre todo al espionaje internacional.

Por otro lado, en la práctica se comprueba como la delincuencia informática es realizada por personas vinculadas de algún modo a las empresas, es decir, por sujetos que tienen acceso a la unidad central de procesamiento de datos —*hackers*—. Puesto que dichas personas, por su propio trabajo, llegan a conocer de manera completa el sistema informático, tienen mayor facilidad para burlar la seguridad implantada.

4. La víctima

Cada vez hay más autores que plantean que hay que considerar el papel de la víctima en el Derecho Penal, circunstancia que ha sido posible a través del desarrollo de la Criminología, sobre todo de la Victimología. Entiéndase por víctima a la persona afectada por el comportamiento del autor del delito.

Desde antiguo, se ha destacado cómo en el Derecho Penal hay una interrelación entre delincuente y víctima. Así, en la estafa es muy frecuente que el delincuente se aproveche del afán de lucro del estafado, como sucede, por ejemplo, en la venta a bajo precio de un billete premiado de la lotería.

En los últimos tiempos se ha destacado que la víctima asume, desde el principio, el riesgo como medio de aumentar la seducción de la oferta en un sistema de alta competitividad —así, en el caso de los supermercados o tiendas semejantes, en que todo está al alcance táctil autónomo de los clientes. Es por ello que esta asunción del riesgo hay que tenerla en cuenta también desde una perspectiva penal.

En base a esto, algunos autores pretenden encontrar en el comportamiento de la víctima una categoría de carácter dogmático que actúe como un principio a tener en cuenta dentro de la sistemática del delito.

De ahí surge el concepto de *autorresponsabilidad*. Significa que la víctima ha de tomar todas las precauciones que sean del caso para evitar que sea su comportamiento la causa del delito, en otros términos, quien no

toma las precauciones correspondientes a su responsabilidad respecto de sus bienes jurídicos carecerá de protección frente a estos.

La existencia de autorresponsabilidad implicaría la imposibilidad de atribuir ese hecho al tipo legal; estaríamos ante una causa de atipicidad. Siguiendo esta idea, la víctima que deja un saco, su cartera o su malecón sumamente costosos en el asiento trasero de su carro descapotable mientras va a hacer unas compras, los cuales ya no encuentra al regresar, sería autorresponsable de ese hecho.

En el ámbito de los delitos informáticos también es posible aplicar este razonamiento: normalmente las empresas, con el desarrollo continuo de la sociedad en una economía de mercado, siempre tienden a que su oferta llegue al público; el instrumento para conseguir esto son las computadoras, las cuales facilitan y aceleran este proceso. Es por esto que las víctimas más frecuentes de los delitos informáticos son personas jurídicas con un cierto potencial económico. Esta característica es algo que corresponde con las notas propias de la delincuencia de cuello blanco o socioeconómica, donde también se encuadra la delincuencia informática.

EL CONCEPTO DE DELITO INFORMÁTICO

1. Definición del delito informático

No existe un concepto de delito informático —*computer crime* o *computerkriminalität*— que sea aceptado por el Derecho Penal de manera unánime debido a que la delincuencia informática comprende una serie de comportamientos que es difícil reducir o agrupar en una sola definición.

De manera general, se puede definir el delito informático como aquél en el que para su comisión se emplea un sistema automático de procesamiento de datos o de transmisión de datos⁽¹⁾.

En nuestra legislación esta figura se encuentra descrita en el artículo 186, inciso 3º, segundo párrafo del

1 En este sentido: TIEDEMANN. *Poder económico y delito*. 1ª ed., Ed. Ariel, Barcelona, 1985, pp. 121-122; SALT. «Delitos informáticos de carácter económico». En: *Delitos no convencionales*. Editores del Puerto, Buenos Aires, 1994, pp. 225-226.

Código Penal. Este hecho merece ser resaltado puesto que en otros países se habla de delito informático en un sentido de *lege ferenda* ya que carecen de una tipificación expresa de estos comportamientos.

2. Relación con otras figuras delictivas

La aparición de estas nuevas conductas merece, no obstante, determinar si las figuras delictivas tradicionales contenidas en el Código Penal son suficientes para dar acogida al delito informático.

2.1. Delito de estafa

Entre las conductas defraudatorias mediante computadora y las defraudaciones en general —dentro de las cuales se encuentra la estafa— existe una afinidad o proximidad en los conceptos. Pero al examinar más exhaustivamente los elementos típicos de la estafa, se acaba concluyendo que el fraude informático y el delito de estafa prácticamente sólo tienen en común el perjuicio patrimonial que provocan⁽²⁾.

El fraude informático se indentifica con manipulaciones informáticas lesivas para el patrimonio —siguiendo la distinción germana *computer manipulationen*; dentro de éstas se distinguen⁽³⁾:

- a) La fase *input* o entrada de datos en la cual se introducen datos falsos o se modifican los reales añadiendo otros, o bien se omiten o suprimen datos.

2 GUTIÉRREZ FRANCÉS. *Fraude informático y estafa*. Ministerio de Justicia, Centro de Publicaciones, Madrid, 1992, p. 30.

3 Véase en este sentido: SIEBER. «Criminalidad informática: Peligro y prevención». Op. cit., pp. 15-21; MÖHRENSCHLAGER. «Tendencias de

- b) Las manipulaciones en el programa que contiene las órdenes precisas para el tratamiento informático.
- c) La fase *output* o salida de datos, donde no se afecta el tratamiento informático, sino la salida de los datos procesados al exterior, cuando van a ser visualizados en la pantalla, se van a imprimir o registrar.
- d) Las manipulaciones a distancia, en las cuales se opera desde una computadora fuera de las instalaciones informáticas afectadas, a las que se accede tecleando el código secreto de acceso, con la ayuda de un *modem* y de las líneas telefónicas.

El delito de estafa, según el artículo 196 CP, se define como el perjuicio patrimonial ajeno, causado mediante engaño, astucia, ardid u otra forma fraudulenta, induciendo o manteniendo en error al agraviado, procurándose el estafador un provecho económico para sí o para un tercero.

De esta definición se pueden deducir los elementos que configuran este delito, los cuales están en relación de antecedente a consecuente⁽⁴⁾; estos elementos son: engaño, error, disposición patrimonial, perjuicio –tipicidad objetiva–, dolo y ánimo de lucro –tipicidad subjeti-

política jurídica en la lucha contra la delincuencia relacionada con la informática». En: *Delincuencia informática*. Op. cit., pp. 53-56; el mismo: «El nuevo Derecho Penal informático en Alemania». En: O.u.c., pp. 109-117; TIEDEMANN. *Poder económico y delito*. Op. cit., pp. 123-126; GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., pp. 115-116.

4 BUSTOS RAMÍREZ. *Manual de Derecho Penal. Parte especial*. 2ª ed., Ed. Ariel, Barcelona, 1991, p. 190. Otros autores entienden que los elementos de la estafa tienen que estar en relación de causalidad,

va. El Código Penal no hace referencia expresa a la disposición patrimonial como elemento del tipo de estafa, pero este elemento está implícito en el artículo 196 CP, puesto que la forma en la que se perjudica al sujeto pasivo es mediante un acto de disposición de su patrimonio; aparte de esto, en torno a la facultad de disponer que tiene el sujeto de su patrimonio gira el bien jurídico protegido.

Sujeto activo puede ser cualquier persona⁽⁵⁾. Sujeto pasivo del delito es la persona que sufre el perjuicio patrimonial. Generalmente, la persona que padece el perjuicio es la engañada; pero puede suceder que la persona engañada sea diferente de la que sufre el perjuicio, en este caso, sujeto pasivo del delito será la que sufre el

así: ANTÓN ONECA. *Estafa*. Nueva Enciclopedia Jurídica IX, p. 61; BAJO FERNÁNDEZ. *Manual de Derecho Penal. Parte especial (Delitos patrimoniales y económicos)*. 1ª ed. Ed. Ceura, Madrid, 1987, p. 175; el mismo: «El delito de estafa». En: *Comentarios a la legislación penal*. Ed. EDERSA, Madrid, 1985, p. 1176. Si bien, también hay quienes sostienen que el criterio acertado a emplear es el de la imputación objetiva, así: GÓMEZ BENÍTEZ. *Función y contenido del error en el tipo de estafa*. ADP, 1985 (38), pp. 337-338; MUÑOZ CONDE. *Derecho Penal. Parte especial*. 9ª ed., Ed. Tirant lo Blanch, Valencia, 1993, p. 278.

- 5 GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., pp. 324-325. Indica que normalmente el sujeto realizará por si mismo el delito. Sin embargo, la propia dinámica del comportamiento típico de estafa favorece la realización de este delito en autoría mediata particularmente como consecuencia de las características y complejidad de los procesos de producción, distribución y consumo, en cuyo seno se desarrollan buena parte de las conductas defraudatorias modernas. Por ejemplo, el fabricante A proyecta una estafa sobre los consumidores, y la ejecuta utilizando a la comerciante B como «instrumento» de sus maniobras fraudulentas. El comerciante B, que desconoce la falsedad de lo que se transmite a sus clientes acerca de los productos objeto del fraude, es quien realmente contacta con los consumidores y les presenta una realidad falseada que les induce a realizar traspasos

perjuicio, y la persona engañada será el sujeto pasivo de la acción.

Es preciso analizar, aunque sea de manera breve, cada uno de los elementos de la estafa para comprobar si estos son aplicables al delito informático:

2.1.1. Engaño, astucia, ardid u otra forma fraudulenta

Se ha definido este elemento, acertadamente, a través de la siguiente metáfora: «El estafador alarga la mano, no para coger los bienes como ocurre con el ladrón, sino para que la víctima se los ponga a su alcance».

El engaño consiste en una simulación o disimulación —entendida como desfiguración de lo verdadero capaz de inducir a error a una o varias personas⁽⁶⁾—. Un ejemplo de simulación es la falsa atribución de influencia, que no se tiene, o de bienes inexistentes; en cambio, habría disimulación en la no indicación de un defecto en la calidad de un bien.

patrimoniales perjudiciales. En este caso, el autor de la estafa es A, quien realiza la conducta descrita en el tipo utilizando a B como instrumento. No llega a tener contacto directo con los consumidores, de modo que físicamente no utiliza el engaño típico. Sin embargo, realiza instrumentalmente el tipo logrando la misma infracción de la norma y la ofensa al bien jurídico. El comerciante B, en cambio, actúa con error de tipo —pues desconoce la falsedad de sus manifestaciones, y su conducta es atípica tanto si su error es vencible como en caso de error invencible.

La dinámica comisiva de la estafa propicia, igualmente, los supuestos de coautoría.

6 ANTÓN ONECA. *Estafa*. Op. cit., p. 61; MUÑOZ CONDE. *Derecho Penal. Parte especial*. Op. cit., p. 276. De manera similar: BUSTOS RAMÍREZ. *Manual de Derecho Penal. Parte especial*. Op. cit., p. 190. Dice que el engaño supone una determinada maquinación o simulación por parte del sujeto, el que tiene que tener la aptitud suficiente para inducir a error al otro.

Un punto importante es la aptitud o capacidad del engaño para producir el error. A este respecto, hay que tener en consideración las circunstancias personales del sujeto, si se trata de un niño, campesino o analfabeto, etc.; y además la apariencia de verdad que revisten los hechos falsos; por eso se señalan que estos deben ser idóneos, relevantes y adecuados para producir un error que genere el fraude⁽⁷⁾. Por ello, debe adoptarse un criterio objetivo-subjetivo para determinar el engaño, según el cual habrá que considerar si el engaño reviste apariencia de seriedad y realidad suficiente para defraudar a personas de mediana perspicacia y diligencia —parte objetiva—; y además, en cada caso particular, será preciso tener en cuenta la idoneidad del engaño en función de las condiciones personales del sujeto pasivo —parte subjetiva⁽⁸⁾.

De otro lado, el engaño en la estafa ha de ser anterior al error y a la disposición patrimonial, de modo que si ésta se produce antes del engaño tampoco habrá estafa. Por ejemplo, si Adolfo ha pagado con anterioridad una mercadería de determinada calidad y posteriormente su proveedor —que a consecuencia de un hurto ha quedado sin esta clase de mercadería—, mediante engaño, le entrega una de calidad inferior, no podría plantearse estafa, sino sólo un engaño civil⁽⁹⁾.

El punto medular de la delincuencia informática es la

7 BUSTOS RAMÍREZ. O.u.c., pp. 190-191.

8 Así: BAJO FERNÁNDEZ. *Manual de Derecho Penal. Parte especial*. Op. cit., pp. 169-170; el mismo: *El delito de estafa*. Op. cit., pp. 1166-1168; BUSTOS RAMÍREZ. O.u.c., p. 191.

9 BUSTOS RAMÍREZ. O.u.c., p. 191; ANTÓN ONECA. *Estafa*. Op. cit., p. 63.

manipulación de la computadora. La conducta consiste en modificaciones de datos, practicados especialmente por empleados de las empresas perjudicadas, con el fin de obtener un enriquecimiento personal, por ejemplo, en el pago de sueldos, en pagos injustificados de subsidios, manipulaciones en el balance, etc.

En la manipulación de la computadora se puede decir que estamos ante el engaño que se requiere en la estafa. El engaño, como se entiende en la estafa, está referido de manera directa a una persona física, aunque últimamente algunos autores indican que puede estar dirigido a una persona jurídica. Sin embargo la cuestión estriba en si la introducción de datos falsos en una máquina equivale al engaño —deception— sobre una persona. La opinión unánime de la doctrina, la cual seguimos, rechaza tal identificación, puesto que en un extremo se encuentra el delincuente informático, pero en el otro una computadora. En realidad, para que exista engaño es requisito la participación de dos personas.

Es indudable que en algunas conductas de manipulación fraudulenta sí se podrá configurar el delito de estafa, por ejemplo, cuando el delincuente informático engaña mediante una computadora a otra persona que se encuentra en el otro terminal; en este caso, al haber dos personas podrá sustentarse el engaño, en donde el medio empleado para conseguirlo es una computadora.

También en la actualidad se puede plantear el engaño a una persona jurídica, como en el caso en que se solicita un préstamo al banco, falseándose la situación económica real, o en el que ante una compañía de segu-

ros se miente sobre el verdadero estado de salud de la persona.

Desde el punto de vista del Derecho Penal, se niega la posibilidad de engañar a una máquina. En este sentido, la computadora es sólo una máquina, un instrumento creado por el hombre.

Algunos autores sostienen que en la manipulación informática no es la computadora el afectado por el engaño, ni engañado es tampoco el responsable del departamento informático de la empresa o banco, quien presume que el proceso informático transcurre con normalidad, sino la persona –por lo general jurídica– que instala el sistema informático y que lo programa –u ordena programar– para que desempeñe determinadas tareas⁽¹⁰⁾.

2.1.2. Error

Existe cuando se produce un falso conocimiento de la realidad, que es producto del engaño y que, a su vez, motiva la disposición patrimonial perjudicial⁽¹¹⁾.

También hay autores que consideran que incluir el estado de error entre los elementos típicos de la estafa, como estado psíquico determinante del acto de disposición, no es político-criminalmente acertado. De ahí que la función del error en el tipo objetivo del delito de estafa sería la de restringir las conductas típicas, es decir,

10 GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., pp. 410 y ss.

11 GLADYS ROMERO. *Los elementos del tipo de estafa*. Ed. Lerner, Buenos Aires, 1985, p. 171. Afirma que el error en la estafa juega un doble papel: el error como efecto de la conducta engañosa y el error como causa de la disposición patrimonial.

delimitar restrictivamente las acciones prohibidas como atentatorias contra el bien jurídico protegido⁽¹²⁾.

El Código Penal equipara la conducta consistente en producir el error —conforme al artículo 196 CP— y la de mantener un estado de error por parte del sujeto activo al indicar: «...*induciendo o manteniendo en error al agraviado...*». El mantenimiento del error tiene como presupuesto que otro lo haya provocado, o bien una mala apreciación del agraviado; en estos casos, el comportamiento del sujeto activo se castiga cuando fortifica o impide el cese del error mediante el engaño.

Diferente situación es la simple utilización del error existente con anterioridad, hecho que no configura estafa. Es el caso en que el error proviene de creencias del sujeto; por ejemplo, el caso de curanderos o adivinos que lucran a causa de la superstición del cliente, quien, antes de acudir a la consulta, ya creían en sus mágicos poderes⁽¹³⁾.

No habrá problema de error en aquellos casos en que faltaban las condiciones personales, por cualquier razón, para tomar conocimiento de esa realidad; por ejemplo, aprovecharse de alguien que ignoraba absolutamente un tema por pertenecer a otra cultura, de un niño o de un enfermo mental; en estos casos simplemente habrá hurto y no será necesaria la prueba del engaño ni del error⁽¹⁴⁾.

12 GÓMEZ BENÍTEZ. *Función y contenido del error en el tipo de estafa*. Op. cit., pp. 339 y 344. En la misma línea: GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., pp. 297, 300-304, 362 y ss.

13 ANTÓN ONECA. *Estafa*. Op. cit., p. 65.

14 BUSTOS RAMÍREZ. *Manual de Derecho Penal. Parte especial*. Op. cit.,

Si el error es generado, no por engaño, sino por exclusiva ignorancia, tampoco hay estafa, el solo aprovechamiento de la ignorancia de otro no constituye estafa; por ejemplo, no comete estafa quien compra a un campesino un montón de piedras brillantes a un bajo precio, ignorante el vendedor que se trata de piedras preciosas y sabedor el comprador de ello⁽¹⁵⁾.

En el delito de estafa se requieren dos personas, lo cual se deduce de la descripción del tipo en el artículo 196 CP, donde se indica «induciendo o manteniendo en error al agraviado mediante engaño». Además, el error es entendido como el estado psíquico que padece el agraviado como consecuencia del engaño. Por estas razones es que en la manipulación de computadoras tal como está concebido y establecido el Código Penal no es posible sustentar que existe un engaño. De otro lado, no puede sostenerse que la computadora incurre en un error, dado que actúa conforme a los mandatos o datos de las instrucciones manipuladas⁽¹⁶⁾.

Por tanto, no hay estafa en los casos de manipulación

p. 191; BAJO FERNÁNDEZ. *Manual de Derecho Penal. Parte especial*. Op. cit., p. 172; GLADYS ROMERO. *Los elementos del tipo de estafa*. Op. cit., p. 166. Al respecto: ANTÓN ONECA. *Estafa*. Op. cit., p. 65, afirma que, cuando el sujeto pasivo del delito es un incapaz, el requisito de la capacidad deberá determinarse en vista de la exigencia de esta figura de delito y, conforme a ellas, lo decisivo será si el sujeto pasivo tenía en el caso concreto el grado de madurez y sanidad mental necesarios para conocer los hechos brindados a su conocimiento, y tomar resoluciones de acuerdo a ese conocimiento; GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., p. 365.

15 BUSTOS RAMÍREZ. O.u.c., p. 192.

16 En este sentido: BAJO FERNÁNDEZ; PÉREZ MANZANO. *Manual de Derecho Penal. Parte especial. Delitos patrimoniales y económicos*. 2ª ed., Ed. Centro de Estudios Ramón Areces, Madrid, 1993, p. 300; GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., pp. 410 y ss.

de máquinas automáticas, pues no se puede hablar ni de error ni de engaño; sólo podrá plantearse hurto en el caso que se obtenga un bien mueble, pero será un hecho impune cuando se trate de una prestación de servicios. Un problema semejante tiene lugar con la manipulación de computadoras a través de la introducción y alteración de programas⁽¹⁷⁾.

2.1.3. Acto de disposición patrimonial

El error debe llevar a la víctima a realizar una disposición patrimonial. Es decir, debe haber un acto voluntario, aunque con un vicio del consentimiento, provocado por el engaño y el error⁽¹⁸⁾. Si la persona que dispone del bien hizo su prestación libremente, sin que su consentimiento estuviera viciado por error, y la conducta engañosa del agente es posterior, dirigida a apropiarse del bien o a ocultar su apropiación, no habrá estafa, sino apropiación ilícita (artículo 190 CP)⁽¹⁹⁾.

Es unánime la doctrina al afirmar que el error, el engaño y la disposición patrimonial tienen que recaer sobre la misma persona, la cual no tiene porqué ser necesariamente el perjudicado; por ejemplo, si el depositario entrega el bien a quien dice venir en nombre del dueño, éste —es decir, el dueño— será el perjudicado y sujeto pasivo, a pesar de que el depositario es el engañado. En estos casos, donde el sujeto que realiza la disposición es diferente del sujeto perjudicado se habla de

17 BUSTOS RAMÍREZ. *Manual de Derecho Penal. Parte especial*. Op. cit., p. 192; ANTÓN ONECA. *Estafa*. Op. cit., p. 66. GLADYS ROMERO. *Los elementos del tipo de estafa*. Op. cit., p. 189.

18 BUSTOS RAMÍREZ. O.u.c., p. 192.

19 ANTÓN ONECA. *Estafa*. Op. cit., p. 65.

«estafa en triángulo». Esto es, «la estafa en triángulo» se produce cuando el autor engaña a una persona con la finalidad de que ésta le entregue un bien perteneciente a un tercero⁽²⁰⁾.

Si no hay disposición patrimonial, aunque se produzca el engaño, el error o el perjuicio, no hay estafa: la disposición patrimonial es el elemento básico de la estafa. Por ejemplo, si mediante engaño, el dueño entrega la llave de su casa a un ladrón, creyendo erróneamente que hay un escape de gas, y el ladrón aprovecha esta situación para desvalijar la casa, habrá hurto o robo, según corresponda⁽²¹⁾.

El acto de disposición ha de realizarlo la persona engañada, quien se encuentra en una situación de error, de ahí, que siempre se entienda en la estafa que el acto de disposición es un acto humano, es decir, realizado por una persona. En el caso de las manipulaciones informáticas fraudulentas el acto de disposición lo realiza la computadora, con lo cual se rompe el esquema planteado en el delito de estafa.

2.1.4. Perjuicio

La disposición patrimonial tiene que producir un perjuicio estimable económicamente, pues la estafa es un delito contra el patrimonio. Perjudicado puede ser

20 BUSTOS RAMÍREZ. *Manual de Derecho Penal. Parte especial*. Op. cit., p. 193; ANTÓN ONECA. *Estafa*. Op. cit., p. 66; MUÑOZ CONDE. *Derecho Penal. Parte especial*. Op. cit., p. 279; GLADYS ROMERO. *Los elementos del tipo de estafa*. Op. cit., pp. 204-205; GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., p. 439.

21 BUSTOS RAMÍREZ. O.u.c., p. 193.

cualquier persona, no necesariamente la víctima del engaño⁽²²⁾.

Este elemento de la estafa no ofrece mayor problema para comprenderlo dentro de la manipulación de una computadora, puesto que en ambos casos normalmente se causa un perjuicio a la persona.

Como conclusión, en la legislación peruana, la casi totalidad de supuestos de manipulación de computadoras no puede acogerse dentro del delito de estafa. La única manera sería creando un tipo especial defraudatorio donde se prescindiera de los elementos básicos de la estafa —el engaño a una persona y la subsiguiente provocación del error— tal como sucedió en Alemania con la creación del parágrafo 263 a) del Código Penal alemán (*StGB-Computerbetrug*)⁽²³⁾.

2.2. Delito de daños

El delito de daños se encuentra tipificado en el artículo 205 del Código Penal. El comportamiento consiste en dañar, destruir o inutilizar un bien. Se puede reali-

22 BUSTOS RAMÍREZ. O.u.c., p. 193; ANTÓN ONECA. *Estafa*. Op. cit., p. 67.

23 El parágrafo 263 a) del Código Penal alemán establece:

«I. El que, con intención de obtener para sí o para un tercero un beneficio patrimonial ilegal, lesiona el patrimonio de otro manipulando el resultado de un proceso de datos mediante la alteración de un programa, el empleo de datos falsos o incompletos, o el empleo no autorizado de datos o mediante cualquier otro modo de acción no autorizado sobre el desarrollo del proceso de datos, será castigado con pena privativa de libertad de hasta cinco años o con multa.

II. La tentativa es punible.

III. Cuando revista especial gravedad la pena privativa de libertad será de uno a diez años.»

zar tanto por acción como por omisión impropia, por ejemplo, dejando morir a un animal de hambre.

Por *dañar*, se entiende toda disminución del valor patrimonial de un bien, comprometiendo primordialmente la materia con que ha sido hecha. *Destruir*, significa hacer desaparecer el valor económico de un bien afectando tanto la materia como la función que tenía por destino. *Inutilizar*, consiste en provocar la pérdida de la capacidad del bien para ejercer la función que le compete, sin que haya lesión en la sustancia material.

Sujeto activo puede ser cualquier persona, exceptuando al propietario único del bien; por tanto, no hay inconveniente en admitir como posible sujeto activo en este delito también al copropietario del bien. Sujeto pasivo es el propietario del bien, pero no el mero poseedor, que en todo caso será un perjudicado.

No es necesario que se trate de una destrucción total y efectiva del bien: basta dañarla, es decir, disminuir irreparablemente su calidad o la posibilidad de utilizarla; por ejemplo, hacer derramar por el suelo el vino de los toneles, aunque fuera posible recogerlo⁽²⁴⁾, dejar manco a un animal, hacer muchas perforaciones en un árbol, aunque éste no se seque.

De otro lado, en los bienes compuestos —aquellos en los cuales varios elementos componen un todo— puede

24 En contra: MUÑOZ CONDE. *Derecho Penal. Parte especial*. Op. cit., p. 363, quien manifiesta que el dejar abierta la espita de un tonel de vino no es constitutivo de delito de daños, al no alterarse con ello su esencia o sustancia, aunque sí se produzca un perjuicio patrimonial al propietario; pero sí puede incluirse en el delito de daños el echar a perder el vino añadiéndole sustancias tóxicas.

existir daño por la simple alteración de la estructura, de la colocación o del funcionamiento de las distintas piezas; por ejemplo, desarmar un carro o algunas partes importantes de él constituyen daño, siempre que la reposición implique un considerable esfuerzo o gasto.

El consentimiento del sujeto pasivo es causa de atipicidad, debido a que nos encontramos ante un bien jurídico microsociedad de carácter disponible⁽²⁵⁾.

La descripción del tipo del delito de daños no exige la causación de un perjuicio real, ya que es posible que, tras la destrucción o inutilización del bien, éste acreciente el patrimonio del titular⁽²⁶⁾.

En el sistema informático, el delito de daños existirá si usuarios, carentes de autorización, alteran o destruyen archivos o bancos de datos a propósito.

Es importante precisar que, si los daños se producen de manera negligente, quedarán impunes dado que el delito de daños sólo puede cometerse de manera dolosa.

Estos hechos se conocen como «sabotaje», hechos que resultan ser favorecidos gracias a la concentración de información en un mínimo espacio. La destrucción total de programas y datos puede poner en peligro la estabilidad de una empresa e incluso de la economía nacional⁽²⁷⁾.

25 SUAY HERNÁNDEZ. *Los elementos básicos de los delitos y faltas de daños*. Ed. PPU, Barcelona, 1991, p. 39.

26 SUAY HERNÁNDEZ. O.u.c., p. 24.

27 SALT. *Delitos informáticos de carácter económico*. Op. cit., pp. 229-230. Donde diferencia dos grupos de sabotaje informático: 1. El referido a todo tipo de conductas dirigidas a causar destrozos físicos,

El *modus operandi* de estos actos se viene perfeccionando con el tiempo⁽²⁸⁾; en primer lugar, se realizaban con la causación de incendios, posteriormente, con la introducción de los denominados «programas-crash», virus, *time bombs* —la actividad destructiva comienza luego de un plazo—, cancer *routine* —los programas destructivos tienen la particularidad de que se reproducen por si mismos— que borran grandes cantidades de datos en un cortísimo espacio de tiempo.

Es indudable que estos comportamientos producen un daño en el patrimonio de las personas, por lo que no hay inconveniente en sancionar penalmente dichas conductas. Pero es necesario indicar que con el delito de daños sólo se protege un determinado grupo de conductas que están comprendidas en el delito informático, quedando fuera otras, como por ejemplo, el acceso a una información reservada sin dañar la base de datos. De ahí que el delito de daños será de aplicación siempre que la conducta del autor del hecho limite la capacidad de funcionamiento de la base de datos.

2.3. Delito de falsedad documental

El delito de falsedad documental se encuentra tipificado en el artículo 427 del Código Penal. La conducta consiste en hacer, en todo o en parte, un docu-

es decir, destinadas a la destrucción física del *hardware* y el *software* de un sistema, por ejemplo, por incendio, introduciendo piezas de aluminio dentro de la computadora para producir cortocircuitos, etc.

2. Los métodos dirigidos a causar daños lógicos, es decir, aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos en un sistema informático.

28 Véase: SIEBER. «Criminalidad informática: Peligro y prevención». Op. cit., p. 25.

mento falso o adulterar uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho.

Por tanto, el comportamiento se puede realizar de dos maneras:

1. Hacer, en todo o en parte, un documento falso: esto es, la realización de un documento falso. El sujeto activo puede ser, en principio, cualquiera, con excepción del autor del documento en los supuestos de realización de un documento enteramente falso, puesto que en éste último caso estará haciendo un documento mentiroso, esto es, ideológicamente falso, ya que el documento en sí será siempre genuino, en el sentido de que en el documento se establece lo que efectivamente el autor ha puesto, no respondería de este delito, aunque sí, por ejemplo, de estafa, de concurrir los demás elementos típicos en este delito⁽²⁹⁾. Por realizar un documento falso se entiende la creación de un documento que no existía anteriormente, en donde se hacen constar derechos, obligaciones o hechos que no corresponden con el contenido cierto que el documento debería constar. Sin embargo, es necesario precisar que no puede identificarse realizar un documento enteramente falso a la realización de un documento sólo en parte falso, puesto que, esta última conducta estaría ya abarcada por la segunda modalidad típica comprendida en el artículo de análisis. Es decir, quien altera sólo en parte el contenido de un docu-

29 SOLER. *Derecho Penal argentino*. T. V, Editora Argentina, Buenos Aires, 1976, p. 321; GARCÍA CANTIZANO. *Falsedades documentales*. Ed. Tirant lo Blanch, Valencia, 1994, p. 274.

mento también está realizando un documento en parte falso.

2. Adulterar uno verdadero: a diferencia del comportamiento anterior, aquí es necesaria la previa existencia de un documento verdadero. El comportamiento se realiza cuando se adultera, altera dicho documento. Por ejemplo, la alteración de la fecha o cantidad en un contrato o en una letra de cambio.

El objeto material del delito es el documento. Se entiende por documento toda declaración materializada procedente de una persona que figura como su autor, cuyo contenido tiene eficacia probatoria en el ámbito del tráfico jurídico.

De la definición planteada se puede deducir que los elementos básicos de todo documento son:

- a) La mención del autor, circunstancia que conecta directamente con la «autenticidad» del documento (documento auténtico es aquél que procede de la persona que figura en él como su autor).
- b) El «contenido» que consiste en la constitución de un derecho u obligación o simplemente en cualquier hecho para el cual el documento esté destinado a probar (en relación con esto se habla de veracidad del documento, de tal forma que documento verdadero o verídico sería aquél cuyo contenido coincide con el objeto cierto para cuya constatación el documento ha sido realizado)⁽³⁰⁾.

30 Véase a este respecto: GARCÍA CANTIZANO. *Falsedades documentales*. Op. cit., pp. 146 y ss.

- c) La «forma», lo que nos lleva a la interesante problemática que en la actualidad se suscita en torno a la posibilidad de incluir el documento informático como objeto material de este delito.

Para que exista documento, por tanto, es preciso la materialización de un pensamiento humano, entendida como la existencia de un soporte corporal estable, reconocible visualmente, atribuible a una persona, individualizable en cuanto su autor. Esto sí se puede predicar de los datos y programas de las computadoras⁽³¹⁾, en tanto la información se encuentre contenida en discos, siempre y cuando sea posible tener acceso a ésta. De ahí, que el documento informático goce, al igual que el documento tradicional, de suficiente capacidad como medio probatorio, característica principal en función de la cual se justifica la tipificación de conductas tales como la falsedad documental⁽³²⁾.

Sin embargo, desde el punto de vista práctico, plantea problemas la posibilidad de determinar al autor del documento informático, dado que se exige normalmente que el documento sea la expresión de un pensamiento humano, situación que a veces es difícil reconocer por cuanto incluso existen computadoras capaces de crear nuevos mensajes a partir de los datos introducidos por el sujeto. En estos casos, la cuestión sería determinar hasta dónde llega la autonomía de la máquina para crear su propia fuente de información.

31 GARCÍA CANTIZANO. O.u.c., pp. 178-179. En sentido contrario: GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., p. 165.

32 Véase a este respecto: GARCÍA CANTIZANO. O.u.c., pp. 163 y ss.

Por tanto, esta modalidad delictiva puede aplicarse al delincuente informático siempre y cuando se supere la concepción tradicional de documento, anclada básicamente en un papel escrito, y se acepten nuevas formas de expresión documental, sobre la base de diskettes, CD, discos duros, en cuanto sistemas actuales de expresión de información. De ahí que en algunas legislaciones, como la alemana⁽³³⁾ para cubrir esta laguna se crea un nuevo tipo penal, en el mismo capítulo dedicado a la falsedad documental (Capítulo 23) relativo a la falsificación de datos computarizados —parágrafo 267 del StGB, *Fälschung beweiserheblicher Dater*⁽³⁴⁾—, con el fin de adaptar las características particulares de la información de una computadora a nuevas modalidades de falsificación.

2.4. Delito contra la propiedad intelectual

El delito contra la propiedad intelectual está tipificado en el artículo 216 del Código Penal. El comportamiento consiste en copiar, reproducir, exhibir o difundir al público, en todo o en parte, por impresión, grabación, fonograma, videograma, fijación u otro medio, una obra o producción literaria, artística, científica o

33 Véase: MÖHRENSCHLAGER. *Tendencias de política jurídica en la lucha contra la delincuencia relacionada con la informática*. Op. cit., pp. 57-59.

34 El parágrafo 267 del Código Penal alemán establece:

«I. El que para engañar en el tráfico jurídico almacena datos falsos o modifica datos relevantes para pruebas, de tal forma que, al percibirlos, constituirían un documento falso o falsificado, o el que utiliza datos almacenados o modificados de esta forma, será castigado con pena privativa de libertad de hasta cinco años o con multa.

II. La tentativa es punible.

III. El parágrafo 267.3 es aplicable».

técnica, sin la autorización escrita del autor o productor o titular de los derechos.

Según esto, el sujeto se aprovecha de la creación intelectual de una persona, reproduciéndola, por lo que se afecta tanto al derecho del autor sobre su obra, como a los posibles titulares de este derecho, si es que ha sido cedido a otra persona.

A esta conducta los autores asimilan lo que se conoce como «piratería de *software*» frente a la copia lícita. Esto hechos han alcanzado en la realidad una especial gravedad dada la frecuencia con la que abundan copias piratas de todo tipo de programas de computadoras. Incluso, en nuestro país ello ha obligado a la creación de una fiscalía especializada en la persecución de todas las conductas relativas a la defraudación del derecho de autor. Estas conductas representan un considerable perjuicio económico al autor, quien deja de percibir sus correspondientes derechos por la información y venta del *software*, que es elaborado con un considerable esfuerzo, en el cual, a menudo se encierra un valioso *know how* comercial⁽³⁵⁾.

Por tanto, el delito contra la propiedad intelectual sólo comprendería un grupo de comportamientos incluidos en el delito informático, básicamente los referidos a la defraudación del derecho de autor por su creación científica en el campo del *software*.

35 TIEDEMANN. *Poder económico y delito*. Op. cit., pp. 126-127; SALT. *Delitos informáticos de carácter económico*. Op. cit., pp. 241-244.

2.5. Delito de hurto de uso

El delito de hurto de uso —o *furtum usus*— se incluye en el artículo 187 del Código Penal ante la frecuencia con la que se sustraen automóviles sin ánimo de apropiación. De ahí que el legislador se ha visto en la necesidad de elevar a la categoría de delito de hurto unas conductas que, en cuanto simples usos indebidos de un bien mueble ajeno, no encajan en la descripción típica del delito de hurto del artículo 185 CP.

Sujeto activo puede ser cualquier persona, excepción hecha del propietario, por disposición expresa del artículo 187 CP —«...un bien mueble ajeno...». Sujeto pasivo puede ser cualquier persona, física o jurídica, que sea el titular legítimo de la facultad de uso.

El comportamiento consiste en sustraer un bien mueble ajeno con el fin de hacer uso de él de manera momentánea, para, posteriormente, devolverlo. Por *sustraer* se entiende que el sujeto realiza actos materiales que desplazan el bien del lugar donde se encuentra. Se entiende que no hay consentimiento del sujeto pasivo, ni tampoco se emplea ningún engaño para desplazar el bien mueble —habría en este caso delito de estafa. De ahí que no se pueda comprender en este delito el caso del chófer que emplea el auto más allá de lo establecido por el dueño, como sucedería si, por ejemplo, se le dice que lleve a X a la universidad y que lo espere, pero, en vez de esperar, se va a Ancón a comer un cebiche; en el ejemplo, el chófer se limita sólo a hacer un uso excesivo del automóvil, lo que constituye un ilícito civil.

Tras la sustracción, el sujeto ha de usar el bien du-

rante un tiempo —el texto del artículo 187 CP dice «uso momentáneo»—, hecho que deberá determinarse en cada caso particular.

No es suficiente que el sujeto tenga el fin de usar el bien, en la realidad, ha debido usarlo. Esto se deduce de la propia disposición del artículo, al indicarse que ha de devolverse el bien; es decir, se devuelve después de usarlo. La devolución no tiene que producirse necesariamente en el mismo lugar de donde se sustrajo, basta con que se abandone el bien en otro lugar cualquiera. En este aspecto queda patente el hecho de que el sujeto sólo tenía la intención de usar el bien y no de apropiarlo. Así sucede, por ejemplo, con quien se lleva un auto ajeno para divertirse un fin de semana o para trasladar sus cosas, ya que está de mudanza, y luego lo deja abandonado.

En cuanto a la delincuencia informática, el delito de hurto de uso se le denomina hurto de tiempo, lo que se da con la utilización indebida de las instalaciones de cómputos por parte de empleados desleales o de extraños, lo cuales pueden producir pérdidas considerables, especialmente en los sistemas de procesamiento de datos a distancia.

En cuanto a si este comportamiento encaja dentro del artículo 187 del CP, en primer lugar, es cierto que el autor hace uso de las instalaciones de computo; pero donde existe el inconveniente para aplicar el referido delito es en la exigencia del artículo 187 del CP de una sustracción, entendida ésta como el traslado físico de un bien mueble de un lugar a otro, exigencia que no se cumple en la conducta de uso de instalaciones de com-

puto. Por tanto, el delito de hurto de uso del artículo 187 CP es inaplicable en esta clase de conductas al no encajar en el tipo penal.

BIEN JURÍDICO PROTEGIDO EN EL DELITO INFORMÁTICO

1. Consideraciones generales

Es innegable que el bien jurídico protegido es punto de referencia obligado para la determinación del tipo penal del delito informático, puesto que determina el marco dentro del cual pueden realizarse las conductas delictivas.

No hay unanimidad en orden al contenido del bien jurídico protegido en el delito informático. La mayoría de legislaciones establecen que estos delitos afectan al patrimonio, pero, de *lege ferenda*, también hay autores que afirman que el bien jurídico protegido es bien el orden económico, bien la intimidad de las personas.

No obstante, las principales posiciones sostenidas por la doctrina a este respecto son las siguientes:

2. El patrimonio

El Título V del Libro II del Código Penal se refiere a

los delitos contra el patrimonio. En otros códigos penales, estos delitos se agrupan en un mismo capítulo bajo la rúbrica de: «Delitos contra la propiedad». Nuestro legislador, en el Código Penal actual, manteniendo la misma rúbrica del Código Penal de 1924, ha sido consciente de todas las dificultades que conlleva el empleo del término «propiedad», en la medida en que tal concepto no abarca todos los comportamientos típicos acogidos bajo el Título V, de ahí que en la actualidad, tanto en el ámbito penal como en el civil, se utilice en cuanto término más apropiado el de «patrimonio».

El *patrimonio*, en cuanto a su concepto, tampoco presenta, no obstante, un contenido claro capaz de resolver todos los problemas que plantean estos delitos; es por esto que se han mantenido diferentes posiciones que tratan de esclarecer su significado. Sin embargo, no constituye objeto de esta investigación el realizar una exposición exhaustiva de las distintas tesis doctrinales mantenidas al respecto, puesto que nos saldríamos de los límites fijados para ésta. De ahí que plantearemos la tesis que sostiene la doctrina mayoritaria y con la cual estamos de acuerdo.

Dicha teoría es la de *concepción mixta o jurídico-económica del patrimonio*. Desde esta concepción, el patrimonio está constituido por la suma de los valores económicos puestos a disposición de una persona, bajo la protección del ordenamiento jurídico.

Un aspecto digno de ser resaltado es el grado de reconocimiento jurídico requerido en los bienes de contenido económico para constituir el patrimonio. En base a esto, los bienes ilícitos forman también parte del concepto de

patrimonio⁽¹⁾, dado que, al adquirirse un bien ilícito, éste pasa a formar parte del patrimonio de su adquirente; esto es, se daría una relación fáctica que entraña un valor económico, siempre y cuando no sea frente al propietario.

Por tanto, el bien jurídico protegido en este título es el patrimonio, interpretado según una concepción mixta o jurídico-económica del patrimonio⁽²⁾.

1 De la misma opinión: MUÑOZ CONDE. *Derecho Penal. Parte especial*. 9ª ed., Ed. Tirant lo Blanch, Valencia, 1993, p. 213, siempre que no sea frente al propietario; VALLE MUÑÍZ. *El delito de estafa. Delimitación jurídico-penal con el fraude civil*. Ed. Bosch, Barcelona, 1987, pp. 86-87; BAJO FERNÁNDEZ. *Manual de Derecho Penal. Parte especial (Delitos patrimoniales y económicos)*. 1ª ed., Ed. Ceura, Madrid, 1987, p. 183. En contra: GLADYS ROMERO. *Los elementos del tipo de estafa*. Ed. Lerner, Buenos Aires, 1985, p. 302. Quien manifiesta que los bienes cuya tenencia es ilícita no forman parte del patrimonio, sin que ese sujeto tenga derecho a lucro. Por tanto, si se dispone de tales bienes o servicios no existirá perjuicio. Conforme al Código Penal español, el disponente sólo será víctima de una tentativa inidónea de estafa por inidoneidad del objeto sobre el que recae la acción. Por ejemplo, el supuesto del estafador que pretende estafar al ladrón o a otro estafador; el de la prostituta que presta un servicio y no se le paga. En el mismo sentido: HUERTA TOCILDO. *Protección penal del patrimonio inmobiliario*. 1ª ed., Ed. Civitas, Madrid, 1980, p. 42.

2 Las otras teorías planteadas respecto al concepto de «patrimonio» son:

1. *Concepción jurídica del patrimonio*: según ésta teoría, sólo son derechos patrimoniales aquellos reconocidos como derechos patrimoniales subjetivos por el Derecho privado o público. En la actualidad esta posición ha caído en desuso.

De entre las muchas críticas que se le objetan a esta posición, destaca aquella que afirma la dificultad de definir qué se entiende por derechos patrimoniales subjetivos, puesto que este concepto, según el punto de vista desde el que se analice, puede ser amplio o restringido. Así, si se interpreta ampliamente, supondrá que la lesión de un derecho sin valor económico o mediante alguna contraprestación de valor económico puede considerarse como un daño patrimonial. Si se acoge desde un punto de vista restrictivo, se excluirán como posibles lesiones al

Quienes sostienen que el patrimonio, así interpretado, es el verdadero bien jurídico protegido en el delito informático tienen como fundamento básico el hecho que ofrece la realidad en la comisión de estas conductas, mediante la cuales, casi siempre se ocasiona un perjuicio cuantificable económicamente.

Desde este punto de vista, se estaría afectando a un bien jurídico individual, como es el patrimonio, con independencia de la cuantía del perjuicio y de la capacidad económica de la empresa afectada, que sería, por lo tanto, el único sujeto pasivo afectado por la conducta.

patrimonio aquellas que recaigan sobre bienes con un valor económico pero que no estén jurídicamente concretados en derechos subjetivos, lo cual origina evidentes lagunas de punibilidad.

2. *Concepción económica estricta del patrimonio*: el patrimonio está constituido por la suma de valores económicos pertenecientes a una persona, sin importar que estos gocen de reconocimiento jurídico.

En un primer análisis, pueden ya apreciarse los inconvenientes de esta posición: en un primer lugar, por su visión puramente objetiva, no da importancia a las circunstancias de cada caso individual, como por ejemplo, las necesidades y fines que tiene el «bien» para la persona afectada por su lesión; en segundo lugar, por ser tan amplia, la concepción de patrimonio abarcaría incluso aquellos bienes poseídos antijurídicamente, lo cual contradice uno de los principios rectores del Derecho, esto es, el Derecho sólo protege aquellos bienes jurídicamente reconocidos por él.

3. *Concepción patrimonial personal*: posición mantenida por Otto. Según esta tesis, el concepto de patrimonio depende de la opinión del sujeto pasivo de la infracción. Para Otto lo que se pretende es asegurar y posibilitar el desarrollo de la personalidad del individuo. El patrimonio es una garantía objetiva para el desarrollo subjetivo, destacando principalmente el valor de uso de las cosas sobre el valor económico.

En esta posición se concede una sobrevaloración al momento subjetivo de la infracción, lo cual puede llevar a soluciones injustas, puesto que no existe ningún parámetro objetivo de valoración.

Véase a este respecto: HUERTA TOCILDO. *Protección penal del*

3. El orden económico

Los autores reconocen el surgimiento y la importancia de una nueva rama jurídica que han denominado como Derecho Penal Económico, respecto a la cual, no obstante, no puede decirse que hay un concepto único, —ante todo por falta de precisión—, que sirva para marcar los límites conceptuales de un objeto de estudio en si reacio a una definición dogmática; incluso hay discrepancia en la denominación de la materia⁽³⁾.

Siguiendo a Bajo Fernández⁽⁴⁾, se define el Derecho Penal Económico como «el conjunto de normas jurídico-penales que protegen el orden económico»; para este autor, su objeto de protección sería el «orden económico», el cual, a su vez, puede analizarse desde dos perspectivas. La primera, en sentido estricto, según la cual el Derecho Penal Económico se entendería como regulación jurídica del intervencionismo estatal —es el Derecho de la economía dirigida por el Estado—. Y la segunda, en

patrimonio inmobiliario, primera edición, Ed. Civitas, Madrid, 1980, pp. 29 y ss; BAJO FERNÁNDEZ. «La reforma del Código Penal de 1983». En: *Comentarios a la legislación penal*. (Coord. Manuel Cobo del Rosal), tomo V, volumen 2, Ed. Edersa, Madrid, 1985, pp. 1163 y ss.; el mismo: *Manual de Derecho Penal. Parte especial (Delitos patrimoniales y económicos)*, 1ª ed., Ed. Ceura, Madrid, 1987, pp. 166 y ss.; BUSTOS RAMÍREZ. *Manual de Derecho Penal. Parte especial*. 2ª ed., Ed. Ariel, Barcelona, p. 161; DE LA MATA BARRANCO. *Tutela penal de la propiedad y delitos de apropiación. El dinero como objeto material de los delitos de hurto y apropiación ilícita*. Ed. PPU, Barcelona, 1994, pp. 65-69; OTTO. *Grundkurs Strafrecht. Die einzelnen Delikte*. Dritte Auflage, Walter de Gruyter Verlag, Berlin/New York, 1991, p. 129.

3 VIRGOLINI. *Delito de cuello blanco, punto de inflexión en la teoría criminológica*. DP, 1989, pp. 353-354.

4 BAJO FERNÁNDEZ. *Manual de Derecho Penal. Parte especial*. Op. cit., pp. 394-395.

sentido amplio, para la cual el Derecho Penal Económico sería la regulación jurídica de la producción, distribución y consumo de bienes y servicios. Desde esta perspectiva, contendría aquellas infracciones que, afectando a un bien jurídico patrimonial individual, lesionan o ponen en peligro, en segundo término, la regulación jurídica de la producción, distribución y consumo de bienes y servicios⁽⁵⁾.

Quienes mantienen esta tesis en el ámbito de la delincuencia informática han de partir del hecho de que con estas conductas se afecta, no ya el patrimonio particular de una empresa, sino en realidad, todo el orden económico establecido en una concreta sociedad, por lo que los perjudicados no serían sólo la empresa, sino toda la colectividad imbuida en el mundo de las relaciones

5 TIEDEMANN. *Poder económico y delito*. 1ª ed., Ed. Ariel, Barcelona, 1985, p. 12; el mismo: *Objetivos, propósitos y métodos de la investigación criminológica europea en el ámbito de los delitos económicos*. DP, 1977, p. 156; el mismo: *Lecciones de Derecho Penal Económico*. Ed. PPU, Barcelona, 1993, pp. 31-32. En este sentido, plantea que los delitos socioeconómicos pueden clasificarse de dos formas: los delitos económicos en un sentido restringido, que abarcan dos áreas: a) las transgresiones en el ámbito del Derecho Administrativo Económico, o sea, contra la actividad interventora y reguladora del Estado en la economía; y b) las infracciones en el campo de los demás bienes jurídicos colectivos o supraindividuales de la vida económica, los cuales, por necesidad conceptual, trascienden los bienes jurídicos individuales (delitos económicos en un sentido restringido).

Y los delitos socioeconómicos en un sentido amplio, que coinciden con los delitos patrimoniales clásicos: estafa, extorsión, defraudación, cohecho, etc., los cuales, a su vez, tienen dos direcciones: a) cuando se dirigen contra patrimonios supraindividuales, como en los casos de obtención fraudulenta de subvenciones o créditos estatales, y, b) cuando constituyen abuso de medidas e instrumentos de la vida económica, como en los casos de libramientos indebidos o balances falsos.

socioeconómicas⁽⁶⁾. Estaríamos ante un bien jurídico de carácter macrosocial.

4. El derecho a la intimidad de las personas⁽⁷⁾

El derecho a la intimidad está reconocido constitucionalmente como un derecho fundamental de la persona en el artículo 2, 7º Co.

A este respecto, no puede olvidarse cómo en la actualidad se tiende a la concentración de una gran masa de información relativa a todos los aspectos posibles de la persona, cuyo acceso es restringido a un grupo reducido, el cual, mediante la manipulación informática de tales datos puede llegar a tener un excesivo control sobre el individuo.

En el Código Penal peruano tal utilización indebida de información tendría su tipificación expresa en el artículo 157 CP, donde se ha querido reforzar expresamente la protección de la intimidad de la persona frente al manejo indiscriminado de datos, tanto cuando ello se ha realizado por personas naturales como el Estado.

La frase conocida de que la información es poder, ha llevado a varios Estados a la creación de organismos especiales encargados del control del empleo correcto de toda la información que el Estado pueda tener almacenada respecto a la intimidad de la persona.

6 Véase a este respecto: SIEBER. «Criminalidad informática: Peligro y prevención». En: *Delincuencia y prevención*. Ed. PPU, Barcelona, 1992, p. 27.

7 Véase al respecto: JIJENA LEIVA. *Chile, la protección penal de la intimidad y el delito informático*. Editorial Jurídica de Chile, Santiago de Chile, 1992, pp. 44-45.

5. Toma de posición

Es innegable el hecho de que los diferentes comportamientos incluidos dentro del delito informático pueden afectar a múltiples bienes jurídicos; de hecho, ha quedado demostrado como la intimidad, el patrimonio, el orden económico resultan lesionados mediante manipulación informática de datos. Pero no sólo ellos, también es posible hablar de la seguridad nacional, la seguridad del flujo transnacional de datos, etc.

De manera indiscriminada, pues, se alude a bienes jurídicos de naturaleza individual como macrosocial. Todo ello nos obliga a afirmar que en realidad no existe un bien jurídico protegido en el delito informático, porque en verdad no hay, como tal un «delito» informático. Este no es más que una forma o método de ejecución de conductas delictivas que afectan a bienes jurídicos que ya gozan de una específica protección por el Derecho Penal.

Así, sería más correcto hablar de criminalidad informática en cuanto nueva forma de comisión de delitos ya tradicionales, como pueden ser la estafa, el hurto, el delito de traición a la patria, espionaje, nacida al amparo del rápido desarrollo tecnológico habido en los últimos tiempos⁽⁸⁾.

Este avance es a la vez la causa de que la actual estructura de los delitos tradicionales, por llamarlos de alguna forma, no sea suficiente para acoger esta crimina-

8 En el mismo sentido: GUTIÉRREZ FRANCÉS. *Fraude informático y estafa*. Ed, Ministerio de Justicia, Centro de Publicaciones, Madrid, 1991, pp. 61-63.

lidad de la computadora, la cual se presenta cada vez de una manera refinada y sutil. De ahí, los graves problemas de lagunas de punibilidad que la manipulación informática provoca, los cuales representan un nuevo reto para el Derecho Penal del siglo XXI.

EL DELITO INFORMÁTICO EN EL CÓDIGO PENAL PERUANO: ARTÍCULO 186, INCISO 3º, 2º PÁRRAFO

1. El patrimonio como bien jurídico protegido

La criminalidad informática en el Código Penal peruano se encuentra recogida de manera expresa como un agravante del delito de hurto en el artículo 186, inciso 3º, segundo párrafo. De esta manera, el legislador penal opta por tipificar esta modalidad delictiva como una forma de ataque contra el patrimonio, por cuanto éste se configura en el bien jurídico protegido en el delito de hurto, entendiéndose el patrimonio en un sentido jurídico-económico. Por tanto, cabe concluir que se protege un bien jurídico individual.

Si bien, es posible que en algunos casos las referidas conductas afecten, además del patrimonio, a la intimidad de las personas, al orden económico, etc.

2. Análisis del tipo objetivo

2.1. Comportamiento típico: remisión al tipo básico del delito de hurto (artículo 185 CP)

La conducta descrita en el artículo 186, 3º CP está configurada como una agravante del delito de hurto, justificada en función del medio empleado por el sujeto activo del delito, esto es, un sistema de transferencia electrónica de fondos, la telemática o la violación de claves secretas.

Por tanto, para su aplicación se exigirá la concurrencia de los mismos elementos que son imprescindibles para configurar el delito de hurto. No obstante, es necesario precisar que algunos de estos elementos van a tener que interpretarse de manera diferente a la tradicional para poder aplicar el referido tipo penal.

El comportamiento consiste en apoderarse ilegítimamente de un bien mueble, total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra, empleando la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas.

Por *apoderarse* se entiende toda acción de poner bajo su dominio y disposición inmediata un bien que antes se encontraba en la esfera de custodia de otra persona⁽¹⁾. Cuando se da el apoderamiento, el sujeto tiene la posibilidad inmediata de realizar actos de disposición sobre el bien, posibilidad de la que carecía antes de este comportamiento al encontrarse dicho bien en la esfera de dominio del poseedor⁽²⁾.

-
- 1 ROY FREYRE. *Derecho Penal peruano*. T. III, Ed. Instituto Peruano de Ciencias Penales, Lima, 1983, pp. 45-46.
 - 2 SOLER. *Derecho Penal argentino*. T.IV, Editora Argentina, Buenos Aires, 1976, pp. 161-168.

Este apoderamiento tiene que realizarse mediante sustracción. Por *sustracción* se entiende toda acción que realiza el sujeto tendente a desplazar el bien del lugar donde se encuentra —«...sustrayéndolo del lugar donde se encuentra ...»; de tal manera que, la obtención de un bien mediante otra forma no se considerará hurto, así, por ejemplo, el coger las gallinas del vecino que se han pasado a otra finca solas⁽³⁾. No se requiere una aprehensión manual o contacto material del autor con el bien, puesto que puede realizarse la sustracción por otros medios, por ejemplo, valiéndose de otra persona —caso de autoría mediata—, de animales o de procedimientos mecánicos⁽⁴⁾.

Este comportamiento no se puede realizar con violencia sobre las personas ni con intimidación, puesto que en estos casos estaríamos ante el delito de robo.

El objeto material sobre el que recae este delito es un bien mueble. Por *bien mueble*, tanto la doctrina como la jurisprudencia, entienden todo objeto del mundo exterior con valor económico, que sea sus-

3 VIVES ANTÓN. *Derecho Penal. Parte especial*. 3ª ed., Ed. Tirant lo Blanch, Valencia, 1990, p. 804. Señala que la sustracción no ha de ser entendida exclusivamente como el alejamiento o desplazamiento del bien mueble, sino que puede llevarse a cabo mediante la ocultación de la misma, allí donde la ocultación baste para separar el bien de la esfera de custodia de su titular e incorporarla al agente. Pareciera que dicha opinión no es aplicable en nuestra legislación tal como está tipificado el delito de hurto.

4 RODRÍGUEZ DEVESA. *Derecho Penal español. Parte especial*. 15ª ed., Ed. Dykinson, Madrid, 1992, p. 418-419; VIVES ANTÓN, *Derecho Penal. Parte especial*. Op. cit., p. 805.

ceptible de apoderamiento material y de desplazamiento⁽⁵⁾. El párrafo segundo del artículo 185 CP equipara a bien mueble —es decir, asimila o comprende como bienes muebles a los efectos del delito de hurto, aunque no son en esencia bienes muebles— la energía eléctrica, el gas, el agua y cualquier otra energía o elemento que tenga valor económico, así como el espectro electromagnético⁽⁶⁾.

El objeto material sobre el que recae el delito ha de ser, por tanto, un bien mueble. No se admiten como objeto material del delito los bienes inmateriales ni los que no tengan un valor económico⁽⁷⁾. A este respecto, se cita el ejemplo de la destrucción de papeles o documentos que no tienen un valor estimable; en estos casos, podría hablarse de un cierto valor referido a la significación del documento en el tráfico jurídico⁽⁸⁾.

Por tanto, el concepto de bien mueble en el delito de

5 MUÑOZ CONDE. *Derecho Penal. Parte especial*. 9ª ed., Ed. Tirant lo Blanch, Valencia, 1993, p. 219; BUSTOS RAMÍREZ. *Manual de Derecho Penal. Parte especial*. 2ª ed., Ed. Ariel, Barcelona, 1991, p. 165.

6 A este respecto: PEÑA CABRERA. *Tratado de Derecho Penal. Parte especial II*. Ed. Ediciones Jurídicas, Lima, 1993, p. 35. Define el espectro electromagnético relacionándolo con las ondas de radiofrecuencia y microondas, que define como «Las ondas de radiofrecuencia son las que se usan en los sistemas de radio y televisión: son generadas por medio de dispositivos electrónicos, principalmente circuitos oscilantes (estaciones). Y las microondas se usan en otros sistemas de comunicación, generado también con dispositivos electrónicos. Es lo que conocemos como UHF (frecuencia ultra altas)».

7 En contra: SUAY HERNÁNDEZ. *Los elementos básicos de los delitos y faltas de daños*. Ed. PPU, Barcelona, p. 151. Quien afirma que los objetos materiales no valubles económicamente también pueden ser objeto material del delito de daños, dado que se protege la propiedad sin referencia a su contenido económico.

8 MUÑOZ CONDE. *Derecho Penal. Parte especial*. Op. cit., p. 366.

hurto es un concepto funcional y autónomo del Derecho Penal, que no coincide con el concepto civil del mismo.

Este bien mueble tiene que ser total o parcialmente ajeno. Por *ajeno* se entiende todo lo que no pertenece a una persona, en este caso, todo lo que no es propiedad del sujeto activo del delito. Por eso, no puede haber hurto de la *res nullius* –las cosas que no pertenecen a nadie y que cualquiera puede apropiarse, así el aire– o de la *res derelictae* –las cosas abandonadas por su dueño para que se apodere de ellas el primero que las encuentre–. No se comprenden los bienes que se encuentran perdidos, puesto que, en caso de apropiación de éstos, se configura el delito de apropiación ilícita (artículo 192 CP).

Finalmente, cabe indicar que sólo se considerará delito cuando la acción recaiga sobre un bien cuyo valor sobrepasa las cuatro remuneraciones mínimas vitales, en caso contrario, estaremos ante una falta contra el patrimonio. Si al momento de cometer el delito, el bien sobrepasaba esta cantidad y, en la investigación o antes de la sentencia, el bien ya no alcanza la cantidad indicada, habrá que seguirse el procedimiento por faltas.

2.2. Características particulares del delito de hurto desde el punto de vista de la criminalidad informática

2.2.1. El objeto material del delito

Con carácter general ya se ha indicado que el objeto material en el delito de hurto ha de ser un bien mueble;

y por tal interpreta la doctrina un bien corporal o material, aprehensible, tangible, entre otras cosas porque sólo así es posible su sustracción.

Pero, si se parte de la base de que en el uso de computadoras en realidad se trabaja con datos archivados y se maneja únicamente información, se suscita un grave problema a la hora de poder definir a dicha información con las mismas características que tradicionalmente se exigen en el bien mueble a los efectos del delito de hurto.

Es preciso señalar, sin embargo, que este problema no se plantea en el ámbito del Derecho Civil donde se acoge una cláusula general en el artículo 886, 10^º CC, que define como bien mueble todos aquellos bienes no comprendidos en el artículo 885, relativo a los bienes inmuebles. Pero el Derecho Penal parte de conceptos autónomos, de ahí que no pueda aplicarse con carácter automático la solución civilista a este problema.

Es evidente que la información en sí misma no es algo tangible; esto no impide que pueda llegar a adquirir corporeidad en aquellos casos en los que se archiva o grava en medios tangibles como puede ser una cinta, un disco, *diskette*, etc., en cuyo caso no plantearía problema alguno puesto que ya habría un concreto bien mueble corpóreo susceptible de ser aprehendido.

Intentando solucionar este problema no faltan autores que consideran como bien mueble al dinero contable, escritural o documental –Giralgeld, Buchgeld⁽⁹⁾–. Desde

9 Véase: SIEBER. «Criminalidad informática: Peligro y prevención». En: *Delincuencia informática*. Ed. PPU, Barcelona, 1992, p. 39.

este punto de vista, cuando la conducta consista en la manipulación de dinero contable por medio de computadora será pues factible estimar la comisión de un delito de hurto en la medida en que se ha adquirido un derecho de crédito, o se ha suprimido un débito, aunque no haya un bien corporal ni una aprehensión material sobre él⁽¹⁰⁾.

Esta tesis es admisible pero sólo respecto a una concreta modalidad de criminalidad informática prevista en el artículo 186, 3º CP, más concretamente, la consistente en el empleo del sistema de transferencia electrónica de fondos, no así para el resto, cuya definición, al ser más amplia, exige también una ampliación de los estrictos límites marcados por un concepto materialista de bien mueble. En base a esto, no habría inconveniente en admitir, a la información computarizada, como bien mueble, y por lo tanto, objeto material del delito de hurto, en cuanto sea susceptible de gozar de un determinado valor económico en el mercado.

2.2.2. Comportamiento típico

En el delito de hurto, el comportamiento típico consiste en apoderarse de un bien mueble mediante sustracción del lugar en el que se encuentra. Por lo tanto, y según esta descripción, sería preciso la concurrencia de un desplazamiento físico del bien mueble.

En el ámbito de la criminalidad informática es posible, sin embargo, sustraer información sin necesidad de

10 GUTIÉRREZ FRANCÉS. *Fraude informático y estafa*. Ed. Ministerio de Justicia, Centro de Publicaciones, Madrid, 1991, p. 157.

proceder a un desplazamiento físico o material. Es por ello, que la noción de desplazamiento físico se ha espiritualizado, bastando con que el bien quede de alguna forma bajo el control del sujeto activo. Sin embargo en la sustracción de información, el apoderamiento puede realizarse con una simple lectura o memorización de datos, de cuya utilización, por lo demás, no queda excluido el titular. De ahí, que muchos autores consideren que en este delito, lo que se lesiona es el derecho al secreto de los datos almacenados, el derecho a un exclusivo control, o un hipotético derecho a negar el acceso a terceros fuera de los que él decida⁽¹¹⁾.

2.2.3. Formas de ejecución de la conducta típica

Ya hemos indicado que la criminalidad informática está contemplada en el Código Penal como un agravante del delito de hurto, establecido en función del medio empleado en su comisión. Según esto, por lo tanto, se caracteriza por ser una forma particular de ejecución del delito de hurto, la cual puede, sin embargo, revestir tres posibilidades: la utilización del sistema de transferencia electrónica de fondos, de la telemática, en general, y la violación del empleo de claves secretas.

a) Utilización de sistemas de transferencia electrónica de fondos

La transferencia electrónica de fondos queda definida como aquella que es iniciada a través de una terminal electrónica, instrumento telefónico o compu-

11 GUTIÉRREZ FRANCÉS. O.u.c., p. 134.

12 GUTIÉRREZ FRANCÉS. O.u.c., p. 147.

tadora, para autorizar un crédito —o un débito— contra una cuenta o institución financiera⁽¹²⁾. Según esta definición, este sistema está referido a la colocación de sumas de dinero de una cuenta a otra, ya sea dentro de la misma entidad financiera, ya a una cuenta de otra entidad financiera, o entidad de otro tipo ya sea pública o privada.

Esta transferencia se manifiesta, por lo tanto, en el reflejo de un asiento contable⁽¹³⁾.

b) Utilización de sistemas telemáticos

La telemática, técnicamente, se define como la informática a distancia (por ejemplo, el uso de dos o más computadoras, radios, teléfonos, fax), entendiéndose por «informática» el tratamiento de información. Por tanto, el empleo de la telemática, en el ámbito de la criminalidad informática, comprende la utilización de cualquier equipo automático de procesamiento de datos, de ahí que la anterior conducta esté ya incluida en esta última, así por ejemplo, el llamado «hurto de información», que se produciría mediante la sustracción de información de una empresa con la finalidad de obtener un beneficio económico.

Si en estos casos, la sustracción se produce con la intención de demostrar una simple habilidad, podría constituirse un delito de hurto de uso (artículo 187 CP). Si se destruyen los datos contenidos en el sistema, habría un delito de daños (artículo 205 CP).

13 GUTIERREZ FRANCÉS, o.u.c., p. 125.

14 GUTIÉRREZ FRANCÉS, o.u.c., p. 131.

En Estados Unidos, la sustracción de información —*information theft*— incluye todos aquellos supuestos en los que se accede a un sistema informático con la finalidad de conocer, copiar o apropiarse de información ajena, bien en forma de datos, de programas, fórmulas o similares⁽¹⁴⁾.

c) Violación del empleo de claves secretas⁽¹⁵⁾

En la violación de claves secretas se protege la obtención de claves tanto por medios informáticos como utilizando otros medios, distintos a los informáticos, para su posterior empleo accediendo a estos sistemas.

Con la violación de claves secretas se alude, fundamentalmente, al uso indebido de las claves en los cajeros automáticos, pero no exclusivamente se incluyen estos casos, sino también la violación de la clave secreta de un sistema de alarma de una institución bancaria o de una empresa, o la alteración del crédito concedido en una tarjeta telefónica.

Es indudable que en la práctica las conductas más frecuentes son los casos de violación de claves de los cajeros automáticos. De ahí, que los bancos aseguran estos actos mediante la utilización de tarjetas con bandas magnéticas y el empleo de un número personal y desconocido.

15 Véase a este respecto: SIEBER. «Documentación para una aproximación al delito informático». En: *Delincuencia informática*. Op. cit., pp. 70-72. Recopila interesantes casos de la jurisprudencia alemana. TIEDEMANN. *Poder económico y delito*. 1ª ed., Ed. Ariel, Barcelona, 1985, pp. 134-137.

Si el autor del delito, para averiguar el número de la clave secreta de la tarjeta, no emplea un medio informático, sino, por ejemplo, acude al uso de la violencia o de la amenaza sobre el sujeto pasivo, no será de aplicación la presente modalidad, ya que se habrá cometido, en realidad, un delito de robo.

2.3. Determinación de la relación de causalidad: definición del resultado

El empleo de la informática se caracteriza, sobre todo, por la ausencia total de fronteras en orden a su utilización, de tal manera que no existen límites territoriales a la hora de proceder a su uso. Así, por ejemplo, es relativamente frecuente que en el ámbito del sistema bancario se produzca continuamente una transferencia de información entre sucursales situadas en diferentes partes del mundo, ya sea pertenecientes a una misma o a diferentes entidades bancarias.

Por otro lado, las conductas de manipulación informática se caracterizan por ser comportamientos pocos arriesgados, susceptibles de ser ejecutados desde su propio domicilio, incluso a muchos kilómetros de distancia o más allá de las fronteras del país donde se producirán los efectos. Existe una separación temporal entre el hecho ilícito y su resultado⁽¹⁶⁾.

Esta situación es la causa de importantes problemas relativos a la determinación de la relación de causalidad entre la conducta del sujeto y el resultado —perjuicio económico— que ésta ocasiona, por cuanto, es posible que

16 GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., p. 79.

la manipulación haya tenido lugar a través de un *modem* situado en Puno, mediante el cual se ha tenido acceso a la base de datos de una sucursal bancaria ubicada en Rio de Janeiro, que ha permitido realizar una transferencia de fondos a una cuenta en un banco suizo.

Esta complejidad, propia del sistema informático, si bien desde el punto de vista teórico no ofrece mayores problemas de determinación de la relación causa-efecto, en el ámbito práctico, esto es, en el de la prueba, origina graves complicaciones difíciles de resolver *a priori*⁽¹⁷⁾.

Esto nos lleva al problema del descubrimiento de dichos hechos, debido entre otras razones a la complejidad técnica de los sistemas informáticos, al desconocimiento de las altas tecnologías por los propios directivos de la empresa, la insuficiencia de medidas de seguridad. A esto se añade otro problema respecto a la prueba de estas conductas en un proceso penal que no es más que la falta de preparación de los magistrados en este tipo de cuestiones técnicas. Se fuerza de esta manera la intervención de peritos en informática⁽¹⁸⁾.

Unido a esta cuestión, se encuentra también el problema de la determinación de la ley aplicable, que vendrá resuelto, según lo dispuesto en el artículo 5 CP, por el principio de ubicuidad, esto es, se aplicará la ley vigente en el lugar de comisión del delito, o bien la del lugar donde se producen sus efectos.

17 Véase: SIEBER. «Documentación para una aproximación al delito informático». Op. cit., pp. 94-95.

18 GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., pp. 80-81.

2.4. Sujeto activo

En principio, sujeto activo de este delito podrá ser cualquier persona, sin necesidad de que ésta tenga unas condiciones particulares en orden a sus conocimientos de informática y manejo de computadoras.

No obstante, no puede olvidarse el hecho de que estamos ante un delito de hurto, aunque agravado, lo cual obliga a desestimar como posible autor al propietario del bien mueble.

Sin embargo, es posible diferenciar dos grupos de casos, según el autor del delito:

- 1º) Aquellos en los que el sujeto actúa sobre un sistema informático ajeno, esto es, directamente sobre los elementos lógicos o sobre el soporte físico, o por comunicación electrónica, desde otra computadora y a distancia. En estos casos el agente es un tercero, extraño al sistema afectado, aunque frecuentemente se tratará de un empleado o de alguien vinculado a la entidad titular de los datos electrónicos.
- 2º) Aquellos en que es el propio titular del sistema afectado quien lleva a cabo la manipulación fraudulenta en perjuicio de terceros —entidad bancaria, compañía de seguros, empresa, administración tributaria⁽¹⁹⁾.

Por otro lado, en estos supuestos, lo normal es que el empresario, directivo o comerciante, por ejemplo, que se sirve en su actividad de un equipo informático cuyo funcionamiento técnico desconoce, necesite de personal es-

19 GUTIÉRREZ FRANCÉS. O.u.c., pp. 328-329.

pecializado para materializar sus órdenes, decisiones o actos dispositivos a través de las máquinas.

Cuando el experto en programación realiza la manipulación informática en ejecución de las órdenes o instrucciones recibidas, desconociendo el propósito fraudulento que con ellas se persigue, su papel es de mero instrumento, y si bien realiza la parte objetiva del tipo, actúa con error de tipo, esto es, sin dolo; sería un supuesto de autoría mediata.

Los niveles crecientes de especialización y la división de funciones entre las distintas personas que pueden intervenir a lo largo de un mismo proceso electrónico, nos hace suponer que no será difícil la presencia de varios autores mediatos en un hecho delictivo.

2.5. Sujeto pasivo

Por sujeto pasivo se entiende al titular del bien jurídico protegido, en este caso, sería el titular del patrimonio que resulta afectado mediante la manipulación informática.

Podrá ser tanto una persona natural o jurídica, aunque en la práctica generalmente suelen ser grandes empresas financieras, dada la gran concentración de capital que ellas tienen.

No obstante, no puede olvidarse que, con independencia de quien sea su titular y del volumen del perjuicio causado, siempre se considera a un titular del bien patrimonio, por cuanto estamos ante un bien jurídico individual, no colectivo.

3. Análisis del tipo subjetivo. Dolo y elemento subjetivo del tipo

Se requiere el dolo y, además, un elemento subjetivo del tipo, el ánimo de lucro, que comprende la intención de apropiación del bien (disponer del bien como propietario) y la de obtener un beneficio o provecho⁽²⁰⁾.

Es necesario recalcar el contenido del elemento subjetivo del tipo que consiste en la finalidad de obtener un provecho económico, de ahí que en los casos en que falte dicha finalidad, como por ejemplo, se quiera causar un daño a una empresa, por diversión o por demostrar su destreza, no podrá aplicarse el artículo que analizamos por ser los hechos atípicos⁽²¹⁾.

No obstante, podría analizarse si tales hechos configuran un posible delito de daños (artículo 205 CP).

Sin embargo, el contenido de este elemento subjetivo del tipo está siendo objeto de una nueva interpretación en los Estados Unidos, donde se equipara a la intención de privar a otro definitivamente de su propiedad. Pero, hay que señalar que quien sustrae datos de un sistema informático, en cambio, no busca necesariamente privar de ellos a su titular, ya que puede resultar suficiente para su proyecto criminal el conocerlos. En ciertos casos, incluso, resulta más ventajoso para el delincuente que la víctima continúe sirviéndose de la información copiada, sin advertir la infracción⁽²²⁾.

20 BUSTOS RAMÍREZ. *Manual de Derecho Penal. Parte especial*. Op. cit. p. 166; MUÑOZ CONDE. *Derecho Penal. Parte especial*. Op. cit., pp. 220-221; ROY FREYRE. *Derecho Penal peruano*. T.III. Op. cit., pp. 54-55.

21 GUTIÉRREZ FRANCÉS. *Fraude informático*. Op. cit., p. 132.

22 GUTIÉRREZ FRANCÉS. O.u.c., p. 134.

En Ohio se ha reelaborado el elemento subjetivo, «ánimo de lucro», añadiendo a su significación tradicional ya mencionada, el ánimo de usar de un bien sin dar consideración –compensación– a su titular⁽²³⁾.

4. Grados de ejecución del delito. Consumación y tentativa

Según lo dispuesto en el artículo 185 CP, donde se acogen los elementos básicos para la aplicación de la agravante del artículo 186, 3º CP, ha de admitirse la consumación del delito en el momento en que el sujeto activo tiene la disponibilidad del bien mueble. Por tanto, no basta para que pueda entenderse consumado el hurto, que el sujeto activo haya tomado el bien, sino que es preciso que haya tenido un mínimo de disponibilidad sobre él.

Pero de nuevo surgen problemas de interpretación a la hora de fijar los criterios que han de emplearse para establecer cuándo tuvo el sujeto, por mínima que sea, la disponibilidad del bien.

Para la consumación no se requiere en ningún momento que el sujeto activo se haya efectivamente lucrado con su acción; basta con la intención de obtener un provecho económico ilícito.

En algunos estados de Estados Unidos es suficiente para la consumación de estos delitos el mero acceso no autorizado a una computadora o sistema informático. Las sanciones penales se imponen con independencia de la intención que mueva al agente, y al margen de los

23 GUTIÉRREZ FRANCÉS. O.u.c., p. 135.

perjuicios económicos que puedan producirse. Se comprende la aproximación, intrusión o comunicación de datos recogidos o almacenados en una computadora o sistema informático, o de otro modo, hacer uso de cualquier recurso de los mismos⁽²⁴⁾.

Sin embargo, es necesario hacer referencia a algunos supuestos especiales que plantean ciertas modalidades específicas en orden a su consumación.

Así, por ejemplo, en los casos de violación de clave secreta, en los que el sujeto, tras usar ilegítimamente una tarjeta electrónica, la devuelve, no puede afirmarse la existencia de un ánimo de apoderamiento de la tarjeta. El objeto material del delito, en este caso, vendría constituido por el dinero, y quedaría consumado con el acceso a la cuenta a través de la violación de la clave secreta, siendo indiferente el hecho de que con posterioridad se devuelva o no la tarjeta.

Por el contrario, cuando la modalidad delictiva consista en el empleo de la telemática, en general, el delito girará en torno al acceso del sistema informático o red o cadena informática con el ánimo de causar un perjuicio económico, de suerte que la consumación tiene lugar con el simple acceso —siempre que concurren los demás elementos, y en especial la intención de obtener un lucro—, sin que sea precisa la apropiación efectiva de los fondos u otros bienes⁽²⁵⁾.

24 GUTIÉRREZ FRANCÉS. O.u.c., pp. 138-139.

25 GUTIÉRREZ FRANCÉS. O.u.c., p. 129. Señala como en los Estados Unidos esta posición provoca una ampliación del ámbito de lo punible, con el riesgo de trasladar el problema a la prueba de la intención de defraudar en el autor.

Por otro lado, es posible consumir una lesión patrimonial a través de una manipulación informática fraudulenta sin que en momento alguno tenga lugar una aprehensión física, esto es, un apoderamiento material del dinero —contable— afectado; esto tendría lugar con relación a la transferencia electrónica de fondos, donde basta con un simple asiento contable de una cuenta a otra, por cuanto esto representa ya la disponibilidad de los fondos transferidos, sin necesidad de que el sujeto haya tomado físicamente el dinero.

CONCLUSIONES

1. El desarrollo tecnológico ha sido tan importante en los últimos tiempos, que la interpretación tradicional de las clásicas figuras delictivas del Derecho Penal han quedado completamente obsoletas ante este nuevo fenómeno representado por la criminalidad informática.
2. Ante esta situación, el legislador se sitúa ante una doble opción, o crear nuevos tipos penales donde se criminalicen específicamente estas conductas, como delitos autónomos, o bien, introducirlas como modalidades de comisión dentro de las conductas delictivas ya tipificadas. Esta última posición es la asumida específicamente por el Código Penal peruano.
3. No existe un bien jurídico protegido en el delito informático, porque en verdad no hay, como tal un «delito» informático. Este no es más que una forma o método de ejecución de conductas delictivas que afectan a bienes jurídicos que ya gozan de una específica protección por el Derecho Penal.

4. Así, sería más correcto hablar de criminalidad informática en cuanto nueva forma de comisión de delitos ya tradicionales, como pueden ser la estafa, el hurto, el delito de traición a la patria, espionaje, nacida al amparo del rápido desarrollo tecnológico habido en los últimos tiempos.
5. En cuanto al objeto material del delito, se exige una ampliación de los estrictos límites marcados por un concepto materialista de bien mueble. En base a esto, no habría inconveniente en admitir, a la información computarizada, como bien mueble, y por lo tanto, objeto material del delito de hurto, en tanto en cuanto sea susceptible de gozar de un determinado valor económico en el mercado.
6. En el ámbito de la criminalidad informática es posible sustraer información sin necesidad de proceder a un desplazamiento físico o material del bien mueble. Es por ello, que la noción de desplazamiento físico se ha espiritualizado, bastando con que el bien quede de alguna forma bajo el control del sujeto activo.

BIBLIOGRAFÍA

ANTÓN ONECA. *Estafa*. NEJ IX.

BAJO FERNÁNDEZ. *Manual de Derecho Penal. Parte especial (Delitos patrimoniales y económicos)*. 1ª ed., Ed. Ceura, Madrid, 1987.

La reforma del Código Penal de 1983, en Comentarios a la legislación penal. (Coord. Manuel Cobo del Rosal), tomo V, volumen 2, Ed. Edersa, Madrid, 1985.

Manual de Derecho Penal. Parte especial (Delitos patrimoniales y económicos). 1ª ed., Ed. Ceura, Madrid, 1987.

BAJO FERNÁNDEZ; PÉREZ MANAZAN., *Manual de Derecho Penal. Parte especial. Delitos patrimoniales y económicos*. 2ª ed., Ed. Centro de Estudios Ramón Areces, Madrid, 1993.

BRAMONT-ARIAS TORRES. *Manual de Derecho Penal. Parte especial*. Ed. San Marcos, Lima, 1994.

- BUSTOS RAMÍREZ. *Manual de Derecho Penal. Parte especial*. 2ª ed. Ed. Ariel, Barcelona, 1991.
- DE LA MATA BARRANCO. *Tutela penal de la propiedad y delitos de apropiación. El dinero como objeto material de los delitos de hurto y apropiación ilícita*. Ed. PPU, Barcelona, 1994.
- GARCÍA CANTIZANO. *Falsedades documentales*, Ed. Tirant lo Blanch, Valencia, 1994.
- GÓMEZ BENÍTEZ. *Función y contenido del error en el tipo de estafa*. ADP 1985 (38).
- GONZALES RUS. *Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos*. Revista de la Facultad de Derecho de la Universidad Complutense de Madrid, Monográfico sobre Informática y Derecho, nº 12.
- GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, Ed. Ministerio de Justicia. Centro de Publicaciones, Madrid, 1991
- HUERTA TOCILDO. *Protección penal del patrimonio inmobiliario*. 1ª ed., Ed. Civitas, Madrid, 1980.
- JIJENA LEIVA. *Chile, la protección penal de la intimidad y el delito informático*. Ed. Jurídica de Chile, Santiago de Chile, 1992.

- MIR PUIG (Cord.). *Delincuencia informática*. Ed. PPU, Barcelona, 1992.
- OTTO. *Grundkurs Strafrecht. Die einzelnen Delikte*. Dritte Auflage, Walter de Gruyter Verlag, Berlin/New York, 1991.
- PEÑA CABRERA. *Tratado de Derecho Penal. Parte especial II*. Ed. Ediciones Jurídicas, Lima, 1993
- RODRÍGUEZ DEVESA. *Derecho Penal español. Parte especial*. 15ª ed., Ed. Dykinson, Madrid, 1992.
- ROMERO. *Los elementos del tipo de estafa*. Ed. Lerner, Buenos Aires, 1985.
- ROY FREYRE. *Derecho Penal peruano*, T. III, Ed. Instituto Peruano de Ciencias Penales, Lima, 1983.
- SOLER. *Derecho Penal argentino*. T. V, Editora Argentina, Buenos Aires, 1976.
- SUAY HERNÁNDEZ. *Los elementos básicos de los delitos y faltas de daños*. Ed. PPU, Barcelona, 1991.
- TIEDEMANN. *Poder económico y delito*. 1ª ed., Ed. Ariel, Barcelona, 1985.
- Objetivos, propósitos y métodos de la investigación criminológica europea en el ámbito de los delitos económicos*. DP, 1977.

Lecciones de Derecho Penal Económico. Ed. PPU, Ba

VALLE MUÑÍZ. *El delito de estafa. Delimitación jurídico-penal con el fraude civil*. Ed. Bosch, Barcelona, 1987.

VIRGOLINI. *Delito de cuello blanco, punto de inflexión en la teoría criminológica*. DP, 1989.

VIVES ANTÓN. *Derecho Penal. Parte especial*. 3ª ed., Ed. Tirant lo Blanch, Valencia, 1990.

*El Delito Informático en el Código
Penal Peruano*, se terminó de imprimir
en el mes de abril de 1997 en los
talleres gráficos de Editorial e Imprenta
DESA S.A. (Reg. Ind.16521),
General Varela 1577,
Lima, 5, Perú.

PUBLICACIONES RECIENTES

TEOFILO ALTAMIRANO

Migración: El fenómeno del siglo. 1996. 302 p.

ROSENDO CHAVEZ

Recursos de agua. 1996. 422 p.

GUILLERMO DAÑINO

La pagoda blanca. 1996. 136 p.

GUILLERMO DESCALZI

Educación y autorrealización. 1996. 246 p.

MANUEL MARZAL

Historia de la antropología social. 1996. 388 p.

HECTOR NOEJOVICH

Los albores de la economía americana. 1996. 584 p.

ALEJANDRO ORTIZ R.

José María Arguedas. Recuerdos de una amistad. 1996. 312 p.

MARIO POLIA

Despierta, remedio, cuenta: Adivinos y médicos del Ande. 1996.
892 p.

JORGE ROJAS

Políticas comerciales y cambiarias en el Perú 1960-1995. 1996.
292 p.

EDUARDO VILLANUEVA

Internet. Breve guía de navegación en el ciberespacio. 1996. 206 p.

Biblioteca de Derecho Contemporáneo

Volúmenes publicados:

**EL DERECHO EN LA SOCIEDAD
POSTMODERNA.**

René Ortiz Caballero.

**LAS REGLAS DEL AMOR EN PROBETAS
DE LABORATORIO (Reproducción Humana
Asistida y Derecho).**

Marcial Rubio Correa.

**LAS DOCTRINAS TRADICIONALES FRENTE
A LA CONTRATACION COMPUTARIZADA.**

Mario Castillo Freyre.

**EL PRINCIPIO PRECAUTORIO
Y SU APLICACION A LOS ENSAYOS
NUCLEARES SUBTERRÁNEOS FRANCESES
EN EL PACIFICO SUR.**

Elvira Méndez Chang.

**LA CONSIDERACION JURIDICA
DEL EMBRION IN VITRO.**

Gorki Gonzales Mantilla.

**EL DELITO INFORMATICO EN EL CODIGO
PENAL PERUANO.**

Luis Alberto Bramont-Arias Torres.

**HACIA UNA CONCEPCION JURIDICA
UNITARIA DE LA MUERTE.**

Juan Morales Godo.

De próxima aparición:

**LA REVOLUCION DEL DERECHO DE SEGUROS
Y DEL DERECHO LABORAL (Genética y Derecho:
El Proyecto Genoma Humano).**

Pinkas Flint Blanck.

FONDO EDITORIAL

Av. Universitaria, cuadra 18 s/n,
San Miguel.

Apartado 1761. Lima - Perú.

Tels. 462-2540 anexo 220 y 462-6390.

