ANEXO

CRIMINALIDAD MEDIANTE COMPUTADORAS

Klaus Tiedemann
Catedrático de Derecho Penal y Criminología
Friburgo de Brisgovia

1. INTRODUCCION

El desarrollo de la técnica constituye un factor novedoso dentro del polifacético conjunto de factores de la criminalidad económica y de la situación económico-social de una colectividad. Así como la motorización y el aumento del tránsito colocaron ante nuevos problemas al Derecho y la jurisdicción penales, pero especialmente a la política en materia de tránsito y de salud pública, del mismo modo la introducción y difusión de máquinas en la industria, el comercio y la administración pública, pero sobre todo en el sector de bancos y seguros, implica, de manera general, además de una racionalización y de un progreso, la posibilidad y el medio para la comisión de nuevos hechos punibles.

Dicho fenómeno será examinado seguidamente, en particular desde los puntos de vista penal y criminológico. Pero valga destacar por adelantado que la llamada criminalidad mediante computadoras, pese a las diferencias de matices, en lo fundamental es independiente de la conformación de los sistemas económicos, pues ella se presenta donde quiera que se incorporan computadoras. Así, en abril de 1983 la agencia de noticias *«Tanjug»* no sin un cierto orgullo por el estado alcanzado por la técnica en Yugoslavia, informó acerca del caso en que tres empleados del «Banco de Istria» habían programado la computadora de esa entidad para que les girase un millón de dinares a quince cuentas privadas; según las versiones de los autores, fueron impulsados a ese hecho por los informes de diarios italianos sobre esa clase de delincuencia.

En el acápite II presentaremos un breve concepto de «criminalidad mediante computadoras», así como una amplia descripción sistemática de sus modalidades, factores, frecuencia, conocimiento por parte de las autoridades, perjuicios y tipos de autores. En el acápite III trataremos los problemas jurídicos que la mencionada forma de criminalidad ofrece y la consiguiente necesidad de reforma de las disposiciones vigentes. Y en el acápite IV nos ocuparemos del abuso de «cajeros automáticos».

2. CONCEPTO Y MODALIDADES DE LA CRIMINALIDAD MEDIANTE COMPUTADORAS

A. Concepto

Con la expresión «criminalidad mediante computadoras» se alude a todos los comportamientos antijurídicos según la ley penal vigente (o socialmente perjudi-

ciales y por eso a penalizar en el futuro) realizados merced al empleo de un equipo automático de procesamiento de datos. Dicho concepto, pues, abarca, por una parte, el problema de la *amenaza a la esfera privada*, del ciudadano a través de la acumulación, archivo, asociación y divulgación de datos mediante computadoras; de hecho, sin embargo, hasta el momento en Alemania Federal sólo se han conocido pocos casos de violación de derechos personalísimos en razón del aprovechamiento abusivo de datos conservados en una computadora. De cualquier forma, el legislador alemán, en la «Ley Federal de Protección de Datos» del 27 de enero de 1977 y en concordancia con modelos extranjeros, reglamentó de modo general esa cuestión, denominada equívocamente «protección de datos» y reforzó la regulación con normas penales poco precisas. Y, por otra parte, el concepto aludido se refiere a los *daños patrimoniales* producidos por el uso abusivo de datos procesados automáticamente; las consideraciones siguientes se circunscriben a este segundo ámbito.

B. **Modalidades**

En Alemania Fedeal el punto de partida de la discusión acerca de la criminalidad mediante computadoras, consistió en determinar si efectivamente existía dicha forma de delincuencia. Gracias a las investigaciones efectuadas desde hace diez años por el Instituto de Criminología y Derecho Penal Económico de la Universidad de Friburgo, actualmente se puede ofrecer una recopilación bastante completa de asuntos penales tanto de la República Federal de Alemania como del ámbito europeo, para acreditar la existencia de tal criminalidad.

Esos casos de delincuencia mediante computadoras revisten especial importancia no sólo por la creciente automatización de los procesos contables. Antes bien, en la República Federal, tanto los productores como también y muy especialmente los usuarios de computadoras, han descuidado gravemente el aspecto de la seguridad, por lo cual se puede y se debe suponer que la criminalidad en mención se ha difundido notablemente en los últimos años. En especial, pero de ningún modo exclusivamente, el medio bancario ofrece innumeralbes posibilidades para esa delincuencia y los riesgos aumentarían si se concretase el proyecto de introducir un sistema de transferencias sin comprobantes. Además, la práctica actual de centralizar y trasladar los equipos de contabilidad al extranjero, dificulta tanto práctica como legalmente la iniciación y adelantamiento de procesos penales. El primer caso argentino decidido por un tribunal de Buenos Aires con fecha 15 de febrero de 1983 concierne a otro campo: la adulteración de las notas finales en la Facultad de Ciencias Económicas de la Universidad Nacional de Buenos Aires y la errónea expedición de títulos universitarios por el sistema de información electrónica. (Jurisprudencia Argentina No. 5268 del 18 de julio de 1984 p. 13 ss).

Parece imposible realizar un cálculo siquiera aproximado de la cifra desconocida (o «cifra negra») en el ámbito de la criminalidad mediante computadoras. En la mayoría de los procesos penales alemanes, el descubrimiento de los hechos se produjo por pura casualidad además, generalmente cuando se detectan esa clase de actividades, las empresas afectadas –y sobre todo los bancos– no efectúan la denuncia correspondiente pues temen por su buen nombre ante la publicidad a que se verían sometidas y consideran que la reparación del daño resultaría afectada si el responsable es condenado a una pena privativa de libertad, en cuyo caso dejaría de trabajar y de percibir una remuneración.

Los hechos conocidos pueden ser, divididos en cuatro grupos, sin tomar en cuenta el empleo de computadoras para la comisión de hechos económicos punibles de carácter general (v. gr. delitos en balances y delitos fiscales, que han

sido estudiados en Capítulos precedentes). Tales grupos son: *manipulaciones, espionaje, sabotaje y hurto de tiempo.*

1. *Manipulaciones.*

Estas pueden afectar tanto la fase de suministro o alimentación (*«input»)* de datos, como la de su salida *(«output»)* y la de su procesamiento (bajo la forma de manipualciones en el *programa* o en la *consola*). Por el contrario, poco importantes resultan las manipulaciones en el *«hardware»*, al cual pertenecen los elementos mecánicos del equipo de procesamiento de datos.

Como ejemplo de manipulación en el *«input»* se puede mencionar el primer caso que, en Alemania Federal, llegó a conocimiento judicial. Su autor trabajaba como empleado técnico en la «Sección de Asignaciones Familiares» de una «Oficina del Trabajo» en el Estado Federado de Baviera. Tras falsificar las iniciales de otro empleado técnico, transfirió ilegalmente asignaciones familiares por hijo, por un monto 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 mas de 80 años– se beneficiaron con más de 250.000 marcos. En 1973 fue condenado a pena privativa de libertad de tres años por abuso de confianza continuado, falsificación de documentos y falsificación de documentos en el ejercicio de un cargo público. Las manipulaciones fueron descubiertas por casualidad: el director del banco en el cual el autor del hecho tenía sus cuentas, comía regularmente con el superior jerárquico del implicado y en alguna oportunidad le mencionó la posibilidad de enriquecerse por el hecho de tener numerosos hijos.

Como ejemplo de una manipulación en el *programa*, se puede traer a colación un caso ocurrido también en el sur de Alemania. Su autor era programador en una gran sociedad anónima. Sirviéndose de un programa, en el cual figuraban los datos de los salarios de 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. Esa manipulación que podría efectuarse con éxito en numerosas empresa, 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 que la manipulación fuese advertida en esos controles, el autor modificó el programa de pagos de salarios de modo que por los sueldos de los empleados ficticios no se emitieran formularios ni fuguraran en las listas de control. Y mediante otra manipulación en el programa que emitía los resúmenes contables y balances de la empresa, logró finalmente que los importes escamoteados se dedujeran del impuesto sobre salarios que se debía a la oficina tributaria respectiva y que de ese modo no se observaran los montos faltantes. Hasta el descubrimiento, también casual, de sus manipulaciones, el autor se apropió de 193.000 marcos. Fue condenado a pena privativa de libertad de dos años, por defraudación y abuso de confianza («infidelidad», Untreue).

La más espectacular manipulación de *consola* fue realizada en relación con la caída del banco privado *«Herstatt»*. En este caso no se informó (o se hizo tardíamente) a la computadora del banco sobre una cantidad considerable de operaciones a término en divisas. Se evitaron los asientos pulsando una tecla llamada «de interrupción» gracias a lo cual se ocultaron pérdidas y se mantuvieron aparentemente bajos el volumen general de las operaciones a término y la denominada «posición neta». En esa forma no se asentaron (o no se hizo de modo regular) sumas por varios miles de millones de dólares norteamericanos.

Los *sistemas para el procesamiento de datos operados a distancia*, que de manera creciente han sido incorporados durante los últimos años, ofrecen una variante especialmente interesante, con muchas perspectivas de ulteriores desarrollos, para las técnicas de manipulación aquí descritas: si se puede acceder a la computadora, por ejemplo, a través de la red telefónica mediante una terminal que opera a distancia, el autor puede efectuar la manipualción desde su casa con su propia terminal, sin necesidad de introducirse personalmente en la empresa perjudicada. Como ejemplo se puede mencionar la manipualción de un estudiante norteamericano quien, ya en los años 70, desde su apartamento y por medio del teléfono logró alcanzar la computadora central de la *«Pacific Telephone Corporation»* y ordenarle que le enviara gratuitamente mercancías por valor de un millón de dólares. Según los informes del «*New York Times*» de comienzos de septiembre de 1983, con la ayuda de sus computadoras personales –de las cuales hay actualmente más de 600.000 en los EE.UU.– cientos de jóvenes norteamericanos interfieren las grandes computadoras comerciales (véase «Frankfurter Allgemeine Zeitung» del 7 de septiembre de 1983, p. 7).

En estos casos se observan claramente varias características de la criminalidad mediante computadoras: en ésta, a diferencia de lo que ocurre en los delitos patrimoniales clásicos, la acción y el efecto se verifican por separado, lo cual dificulta sobremanera el *descubrimiento del hecho.* A ello se suma el *efecto continuado* de esa forma de delincuencia: si en la primera ocasión se actúa con éxito, éste frecuentemente se vuelve permanente, especialmente en la manipulación de programas y de los llamados «datos básicos» hasta que se descubre el hecho por casualidad o por un control específico. Sin embargo, los controles posteriores prácticamente carecen de sentido, pues resultarían sumamente engorrosos por el número extraordinario de procesos resueltos mediante la computadora y, en última instancia, anularían el efecto de racionalización perseguido con la introducción de dicho aparato. De ahí proviene el hecho de que, frecuentemente, los *perjuicios* ocasionados por la criminalidad mediante computadoras tengan una especial envergadura.

Respecto de la *personalidad de los autores* de estas manipulaciones se puede anotar que casi siempre se trata de principiantes o de autores casuales, quienes, contrariamente al punto de vista sostenido principalmente por la doctrina norteamericana, no son en modo alguno personas con una inteligencia superior a la media. En especial las frecuentes manipulaciones del *«input»* o del *«output»* por parte de empleados técnicos, no suponen conocimientos previos de computación. Por otro lado, el mencionado grupo de jóvenes, quienes por razones casi deportivas intentan penetrar las grandes computadoras comerciales constituye un nuevo tipo criminológico.

De la dimensión del daño y de la forma de comisión del hecho, se derivan también nuevos aspectos para los casos examinados a continuación.

2. Espionaje

En el ámbito del procesamiento de datos el espionaje económico se ve favorecido por el hecho de que las informaciones se encuentran archivadas en un espacio mínimo y pueden ser transferidas sin ningún problema a otro soporte.

Además, en el centro del uso indebido de datos figura siempre el también llamado hurto de *«software»* o empleo indebido de programas de computación, cuya elaboración implica generalmente una considerable inversión de esuferzos y a menudo encierran un valioso *«know how»* comercial. En forma accesoria, se trata principalmente de datos de investigación, archivos referidos a clientes y balances.

El siguiente ejemplo de un hurto de *«software»* tiene especial significación por cuanto actualmente se encuentra a consideración de la Corte Suprema Alemana y probablemente conducirá a una decisión sobre la muy discutida posibilidad de proteger los derechos de propiedad intelectual sobre los programas de computación por parte del Derecho Civil:

El autor (A) de este hecho, empleado sin relación de dependencia en una empresa de cobranzas, había desarrollado en dicha firma y en colaboración con otros empleados, un complicado sistema de programación en el cual se incluyó también un archivo de datos elaborado por la empresa luego de largos años de esfuerzos y único en la República Federal de Alemania. Para poder realizar el trabajo de programación, A tenía acceso libre al centro de cómputos de la empresa, especialmente durante los fines de semana. A fines de 1979 se descubrió por casualidad, merced al control realizado por el nuevo jefe del centro de cómputos, que A el 13 de octubre de ese año había copiado las partes más importantes del programa y de los archivos de la empresa, en un disco magnético que llevara al efecto. Las averiguaciones efectuadas posteriormente por la misma entidad, mostraron que entre tanto A había fundado una empresa propia de provisión de servicios para computadoras, había ofrecidos a diversas firmas competidoras un sistema idéntico en líneas generales y se encontraron indicios de que dicho programa ya se estaba empleando en otros dos centros de cómputos.

El espionaje mediante computadoras no es, utilizado únicamente con propósitos económicos por empresas rivales, sino también con finalidades políticas por estados extranjeros. En un proceso penal realizado en Alemania Federal en los años 70, se supo que las posibilidades de espionaje mediante computadoras fueron advertidas muy tempranamente en los países del Este, en especial por parte de la República Democrática Alemana. De acuerdo con esas informaciones, ya en 1964 se elaboró en Berlín Oriental un «plan con perspectivas de largo alcance» en cuyo marco los futuros agentes recibían primeramente, una formación básica en computación, con el encargo de perfeccionarse luego en la industria procesadora de datos de la República Federal.

3. Sabotaje

Tanto desde la perspectiva de la envergadura del daño como desde la del modo de realizar el hecho, son dignos de considerar los casos de sabotaje en el procesamiento de datos. También éstos resultan favorecidos por la alta compresión de informaciones en un mínimo espacio. La destrucción total de programas y datos –por ejemplo mediante atentados, incendiarios, imanes o «programas borradores» especialmente elaborados–, puede poner en jaque la continuidad de toda una empresa. Los servicios secretos de otros países, los fanáticos políticos y los empleados deseosos de venganza, deben ser considerados como posibles autores.

En un proceso penal efectuado en Alemania Federal a finales de la década del 70, el Ministerio Público acusó a un ingeniero, dependiente de la empresa perjudicada, de haber borrado comentarios importantes y programas de trabajo del archivo de la computadora y, en consecuencia, haber puesto en peligro el cumplimiento de un encargo por valor de un millón de marcos, así como la existencia de la firma. El acusado reconoció haber borrado los comentarios referidos al programa, pero en su defensa adujo que lo había hecho para evitar una sobrecarga al disco que contenía el archivo, que previamente había grabado los programas con sus comentarios en una «cassette» y que si ésta desapareció con posterioridad de ello él no era responsable. Como tal argumento no se pudo rebatir, el acusado fue absuelto el 13 de diciembre de 1979 por fallo del Tribunal de primera instancia, en

el que se dijo: «pese a los importantes puntos oscuros referidos al comportamiento del acusado, se le concede el beneficio de la duda».

Más espectacular fue un atentado con explosivos, efectuado por «células revoluionarias», contra el centro de cómputos de las industrias *«Man»* en Ginsheim-Gustavsburg, como expresión de protesta contra el «armamentismo» y la industria de armamentos. En los EEUU se conocieron atentados terroristas similares en vinculación con el movimiento de protesta por la guerra de Vietnam.

4. Hurto de Tiempo

Este es el último grupo de casos de criminalidad mediante computadoras. La utilización indebida de instalaciones de cómputos por parte de empleados desleales o de extraños, puede producir pérdidas considerables, especialmente en aquellos sistemas de procesamiento de datos a distancia, al efectuarse cómputos con números de *«account»* ajenos.

Como ejemplo de hurto de tiempo, además de las actividades en EEUU mencionadas en el acápite II B 1, sirve también el proceso penal iniciado en uno de los Estados Federados de Alemania, en el cual se acusa a un empleado del mismo Estado de haber fundado una empresa propia de provisión de servicios para computadoras y efectuado los correspondientes cómputos en la computadora de propiedad estatal, sin autorización y bajo una descripción falsa del programa y de la tarea. Se le acusa de abuso de confianza («infidelidad» Untreue»).

3. REGULACION PENAL Y NECESIDAD DE REFORMAS

El concepto de criminalidad mediante computadoras, descrito sintéticamente en los párrafos precedentes, resume criminológicamente una nueva categoría de comportamientos punibles, desde la perspectiva del medio empleado. Esa delincuencia a menudo recae sobre objetos intangibles como dinero en los bancos, secretos comerciales, *«konw how»* y otras informaciones. Por lo tanto, no debe sorprender que las normas penales existentes sólo logren abarcar aquellos comportamientos en forma parcial y más bien casual, aunque con diferentes resultados en los diversos sistemas jurídicos.

Las consideraciones siguientes presentan someramente las figuras penales más relevantes para la comprensión de la criminalidad mediante computadoras y, paralelamente señalan las necesidades de reforma del Derecho Penal sustantivo.

A. Hurto de tiempo

La utilización indebida de instalaciones de cómputos, no está prevista en ninguno de los tipos penales de la normatividad alemana. Así, el llamado «hurto de uso» (§ 248 b del Código Penal) es punible únicamente cuando se realiza sobre vehículos a motor y bicicletas; la figura específica de la sustracción indebida de energía eléctrica (§ 248 c), tampoco resulta aplicable por cuanto en ninguno de los casos relevantes se recurrió a un «aprovechamiento irregular de energía» de un determinado conductor eléctrico; y el abuso de confianza (§ 266) que supone tanto un cierto ámbito para que el autor ejecute el hecho como también un perjuicio patrimonial de la víctima, es aplicable sólo en casos especiales.

Hay que destacar que en el hurto de tiempo la actividad reprochable no consiste tanto en el escaso consumo de energía eléctrica ni en el mínimo desgaste del equipo de cómputos, como y sobre todo en el notable enriquecimiento del autor proveniente del uso indebido de la computadora. La acción implica, pues, la

captación fraudulenta de una ventaja, semejante, pero no idéntica, a la descrita en los § § 248 b y 265 a. El hurto de tiempo, por consiguiente, requiere un nuevo tipo penal que lo encuadre adecuadamente, siempre y cuando se considere necesaria la introducción de esa norma, ya que en la actualidad el uso indebido de otros bienes valiosos, sin apropiación de ellos, tampoco es punible.

B. Sabotaje

Todos los actos de sabotaje relacionados con computadoras quedan, en cambio, abarcados plenamente por la figura del daño material (§ 303) ya que la doctrina y la jurisprudencia prevalientes en Alemania consideran que ese tipo penal se refiere, no sólo al mero perjuicio mecánico en la sustancia de un objeto, sino también a la limitación de su capacidad de funcionamiento.

Conforme a dicha opinión, pues, borrar informaciones de bandas magnéticas constituye «daño», aunque el objeto mismo pueda seguir siendo usado para el fin previsto y lo destruído sea la información que contenía, y aunque la propieda del objeto, bien jurídico protegido por el § 303, no sea el fin específico del hecho.

No es necesaria, por consiguiente, en el Derecho alemán una figura penal específica para el sabotaje en relación con computadoras. Pero si se incorporara una norma penal sobre sabotaje industrial en general (como la del § 179 del «Proyecto alternativo de Código Penal») ella podría y debería referirse también a los actos de sabotaje contra computadoras, programas y demás datos.

C. Hurto de «software» y espionaje

De la valoración jurídica de estos hechos, se derivan los problemas más interesantes tanto para el Derecho Penal como para el Civil.

Según la legislación y jurisprudencia penal alemana, la simple obtención de copias no constituye, incluso desde el punto de vista de la denominada «teoría del valor del objeto» apropiación en el sentido de las figuras del hurto y la apropiación indebida (dejando de lado la problemática sobre la calidad de «cosa» de los programas y datos). Dado que, por otra parte, existe consenso en la doctrina acerca de la restringida posibilidad de proteger los programas de computación mediante el derecho de patentes, la discusión actual se centra entonces sobre la *protección de los derechos de propiedad intelectual respecto de los programas de computación.*

La doctrina dominante al respecto en Alemania Federal, afirma la posibilidad de proteger los derechos de propiedad intelectual, sobre programas de computación, ya que éstos constituyen una «creación intelectual personal» en el sentido del § 2, párrafo II, de la «Ley sobre la Propiedad Intelecutal». El Tribunal Superior Regional (*Oberlandesgericht)* de Karlsruhe adoptó ese punto de vista en la decisión dictada en el ya mencionado caso de hurto de «software» por parte de A (véase acápite II B 2). Está pendiente, de todos modos, la sentencia del Tribunal Supremo Federal. Resultaría conveniente que dicha corporación sostuviera también la posibilidad de proteger los derechos de propiedad intelectual sobre los programas de continuación, ya que de «lege lata» únicamente la propiedad intelectual sobre el «software» goza con seguridad de la protección legal debida; aquella tutela debería impedir igualmente la «adquisición de buena fe» por parte de intermediarios de *«software»* de programas de computación sustraídos.

Las disposiciones penales en materia de competencia que sancionan la revelación de secretos comerciales e industriales (§§ 17, 18 y 20 de la «Ley contra la Competencia Desleal») ofrecen asimismo protección frente al autor y al intermediario de *«software»* que actúen dolosamente. Esas figuras penales se vieron

reforzadas en el proyecto de reforma presentado por el anterior Gobierno Federal, según el cual no sólo resultan punibles la reveleación de secretos comeciales a terceras personas y el aprovechamiento de tales secretos, sino que también lo serían su mera apropiación u obtención indebida mediante el empleo de medios técnicos subrepticios y la elaboración clandestina de una reproducción tangible del secreto. Entre tanto, el nuevo Gobierno Federal no ha considerado necesaria una reforma. Tampoco parece punible de lege lata, la mencionada penetración de computadoras por parte de jóvenes por puro espíritu deportivo o por curiosidad.

D. **Manipulaciones**

Estas originan problemas penales específicos en materia de criminalidad mediante computadoras.

Contrariamente a lo que ocurre, en los sistemas penales de Francia y Suiza, la doctrina alemana dominante considera que el dinero en bancos o escrituras no constituye una «cosa», en el sentido de los §§ 242 y 246 del Código Penal. Por consiguiente, la acreditación o extracción de un importe de una cuenta bancaria o a favor de ella, resultante de un acto indebido y doloso, no constituye hurto ni apropiación indebida. Además, dado que el autor se convierte en propietario de los importes acreditados al serle abonados, las normas penales que protegen el derecho de propiedad no le son aplicables. Los problemas penales de la criminalidad mediante computadoras, por tanto, se concentran alrededor de los hechos punibles contra el patrimonio (en especial la estafa y el abuso de confianza), así como sobre las falsificaciones (de documentos y de reproducciones técnicas).

El tipo penal de la *estafa* (§ 263 del Código Penal alemán), lo mismo que las normas respectivas de las legislaciones española y suiza supone el engaño y el error de una persona (mientras que la norma francesa se conforma con «maquinaciones engañosas» lo cual implica menos problemas al enfrentar la criminalidad mediante computadoras). Por lo tanto, el «error de la computadora» es irrelevante para el Derecho Penal alemán. De todos modos, muchas manipulaciones debidas a la intervención de empleados técnicos, personas con firma autorizada o revisores, pese a la limitación establecida por el requisito del error humano, pueden ser encuadradas dentro del tipo penal de la estafa. Esta posibilidad, sin embargo, depende de las características particulares de cada caso y no debe llevar a engaño, pues ante un considerable número de manipulaciones no puede ser aplicado el § 263. Por ello resulta procedente proponer la incorporación de un tipo penal específico, semejante al de la estafa.

El tipo penal sobre *abuso de confianza* o «infidelidad» (Untreue), § 266 del Código Penal alemán, art. 319 del portugués y desconocida, por lo menos en esa forma, en las legislaciones que siguen la tradición latina, apenas parcialmente puede cubrir las omisiones del mencionado tipo de estafa. En efecto, el § 266 no resulta aplicable, por lo general, a perforadores, programadores, operadores y personas ajenas a la empresa, por cuanto en sus casos falta el requisito exigido por la jurisprudencia alemana en el sentido de que exista una esfera de actuación, es decir, una cierta independencia y responsabilidad propias. La programación de una computadora exige, por cierto, considerables conocimientos técnicos, pero los resultados de los procesos se verifican comúnmente de acuerdo con instrucciones precisas, las cuales no dejan espacio para decisiones independientes. En general, el § 266 es sólo aplicable a los empleados técnicos que elaboran y verifican los datos concernientes al *«input»*. Respecto del personal subalterno técnico, los Tribunales Regionales alemanes suelen aplicar la norma del abuso de confianza cuando ha existido un cierto margen de decisión propia.

El tipo penal sobre *falsificación de documentos* (§ 267) exige que el documento sea «la expresión tangible y probatoria» de un pensamiento humano. Aunque se cuestione este requisito, los datos y programas de las computadoras no son en ninguna forma documentos, por cuanto los datos archivados electromagnéticamente *no son reconocibles visualmente*. Por lo general, además, no permiten individualizar a sus autores y actualmente –en lo que hace a los programas y supervisores pertenecientes a una empresa– no se satisfacen las exigencias legales y probatorias provenientes de la definición de «documento». Por otro lado cuando el documento (público) está firmado por una persona, como en el caso argentino mencionado de delito de falsificación ideológica, no existen problemas de punibilidad.

Debido a que la opinión predominante relacionaba el concepto de documento con el de la expresión de un pensamiento humano, en 1969 se incorporó al Código Penal alemán (§ 268) la figura específica de la *falsificación de reproducciones técnicas*. Sin embargo, de acuerdo también con la opinión mayoritaria, las modificaciones efectuadas en el programa de una computadora no constituyen, por sí mismas grabaciones técnicas. Y en los casos en que las manipulaciones afectan al *«Input», el autor no modifica «el resultado de la grabación mediante interferencias perjudiciales sobre el proceso de grabación» como lo exige el § 268 III. Por ello la norma penal sobre falsificación de reproducciones técnicas tiene muy escaso campo de aplicación respecto de las manipualciones sobre computadoras.*

Se puede afirmar, en síntesis, que en la legislación penal alemana las manipulaciones en el procesamiento automático de datos son sancionadas frecuente aunque no inexorablemente. El «Proyecto de una Segunda Ley contra la Delincuencia Económica», dado a conocer por el anterior Gobierno Federal en junio de 1982 y presentado para su discusión legislativa por el actual en abril de 1983, propone la incorporación de dos nuevas figuras penales: la «estafa mediante computadoras» y la «falsificación de datos archivados». Con la aprobación, aún pendiente, de esas propuestas, quedarín subsanados los actuales vacíos del Código Penal, respecto de las manipulaciones sobre computadoras.

4. ABUSO DE «CAJEROS AUTOMATICOS»

Con una adecuada descripción de la «estafa mediante computadoras», incluída en el mencionado *«Proyecto de una Segunda Ley contra la Delincuencia Económica»*, se podría solucionar también otro problema que se presenta por una aplicación especial de la cibernética en el ámbito bancario: el *abuso de las llamadas tarjetas para «cajeros automáticos» o «bancoautómatas».*

Dichas tarjetas, que desde hace bastante tiempo se utilizan en los EEUU, Japón, Francia y Suiza y que también han sido introducidas en Alemania y en España, otorgan al cliente del banco, cuya tarjeta está grabada magnéticamente en forma similar a como ocurre con la tarjeta del cheque europeo, la posibilidad de, una vez por día, hacerse pagar, por el «cajero automático» una determinada suma de dinero en efectivo.

Para evitar abusos por parte de terceros, todos los sistemas de «cajeros automáticos» en funcionamiento o planeados, preven que el cliente además de introducir la tarjeta en la abertura correspondiente, informe al equipo un número personal y secreto conocido únicamente por él. Y solamente si la cifra grabada magnéticamente en la tarjeta coincide con la informada por el cliente, el «cajero automático» entregará la suma de dinero.

Para impedir que un cliente utilice su tarjeta para extraer dinero varias veces en el mismo día, en uno o en diferentes «bancoautómatas», tanto en Alemania como en otros países se están considerando diversas medidas de seguridad: la más efectiva sería la conexión permanente y directa de todos los «cajeros automáticos» con la central que maneja el estado de cuentas y su movimiento mediante el sistema *«online»*, pero las complicaciones organizativas y sus costos no la hacen viable. Algunos sistemas preven, en consencuencia, que el «cajero automático» grabe en la tarjeta la extracción con la fecha del día y la bloquee para futuras operaciones en el mismo día. Otra estrategia consiste en que los movimientos de cuentas de todos los «cajeros automáticos» sean controlados y evaluados periódicamente por una central y en los casos de retiros repetidos, movimientos llamativos y otras irregularidades, se proceda a informar inmediatamente el bloqueo de la tarjeta involucrada a todos los «cajeros automáticos». La dificultad para aplicar estos sitemas de seguridad en Alemania se origina en el hecho de que los bancos, cajas de ahorro y oficinas de giro postal aspiran a alcanzar un sistema en el que el tiular de la tarjeta pueda efectuar extracciones no sólo en los «cajeros automáticos» de una institución, sino también en los de las demás entidades bancarias. La compatibilización y administración conjunta de las medidas de seguridad de las diversas instituciones, presentan considerables dificultades.

Los frecuentes abusos observados en relación con las aludidas tarjetas, consisten, además de la violación contractual, por retiros repetidos o en descubierto por parte del titular, principalmente en el *abuso de tarjetas extraviadas o sustraídas por terceros*, quienes con triquiñuelas o en cualquier otra forma consiguen conocer el número secreto necesario para efectuar extracciones. Si tales retiros ilegítimos son punibles o no, constituye una cuestión contradictoriamente tratada, por la doctrina alemana.

Sin lugar a dudas, la figura penal de la *estafa* (§ 263) resulta inaplicable, ya que en el empleo indebido de una tarjeta de identificación falta tanto el «egaño» como el «error» de una persona.

La norma penal alemana sobre *«abuso de un autómata»* (§ 265 a) tampoco es generalmente aplicada en aquellos casos, con el discutible argumento de que el tipo penal mencionado se refiere únicamente a los autómatas que prestan un servicio –por ejemplo, un tocadiscos– pero no a los que entregan un objeto; además, el autor no habría actuado con el propósito requerido por el § 265 a de «no abonar un precio» y, finalmente, faltaría el presupuesto legal de las «maquinaciones» ya que no se habría interferido el funcionamiento regular del autómata.

La discusión actual, entonces, radica en determinar si la extracción de dinero mediante una tarjeta ajena satisface el tipo penal del *hurto* (§ 242). En los casos en que la tarjeta sustraída no es devuelta, la respuesta es afirmativa: el hurto se refiere a la tarjeta. Si, por el contrario, el autor la devuelve tras haberla utilizado, resulta cuestionable la aplicación del citado % 242, pues éste exige «la intención de apropiarse». La opinión predominante en Alemania, niega que en esta hipótesis se estructure un hurto de la tarjeta, ya que no hay apropiación de su «sustancia» ni del valor del objeto» (según su tipo y función de acuerdo con su destino regular).

Una reciente corriente de opinión, sin embargo, sostiene que cuando la tarjeta ha sido devuelta hay hurto del dinero, con el argumento de que los bancos están de acuerdo, en que las sumas sean retiradas exclusivamente por los titulares de las tarjetas y del saldo en la cuenta bancaria y que, por consiguiente, sólo a favor de esas personas están los bancos dispuestos a transferir la propiedad del dinero en efectivo. Esta construcción jurídica no deja de ser cuestionable, por cuanto el

consentimiento de las entidades bancarias únicamente se puede referir al uso de la tarjeta legítima de identificación y del número secreto correcto, pero su abuso no es equiparable a la extracción de mercancías de autómatas mediante dinero falsificado. Además, aquel ranozamiento llevaría, en última instancia, a considerar también como hurto todo retiro en descubierto efectuado conscientemente por el titular legítimo de una tarjeta.

Antes bien, un respetable sector de la doctrina penal alemana ha llegado a la conclusión extremamente contraria: el empleo abusivo de la tarjeta de identificación acompañado por *la intención de devolverla inmediatamente a su titular, no es punible* conforme a la normatividad penal alemana vigente.

En el Derecho Penal francés, por el contrario, sin problemas se acepta que hay hurto cuando se usa abusivamente una de tales tarjetas, debido a que allí se tiene un concepto más amplio de «apropiación»; e igualmente se admite la existencia de una *«manoeuvre frauduleuse»* (maniobra fraudulenta) en el sentido de la figura penal de la *«escroquerie»*.

Como los «cajeros automáticos» son dirigidos por computadoras sería comprensible que la legislación alemana regulara el abuso de las tarjetas para dichos autómatas por parte de terceros, dentro del nuevo tipo penal de la «estafa mediante computadoras» contenido en la proyectada «Segunda Ley contra la Delincuencia Económica».

En su conjunto, las novísimas posibilidades de abuso en el marco de las técnicas modernas en materias de pagos y transferencias, así como las cuestiones dudosas sobre su tratamiento penal, demuestran nuevamente que la adaptación del Derecho al progreso constituye una tarea permanente de la ciencia jurídica y de la legislación. El medio de la computadora para la comisión de un delito por cierto no cambia la naturaleza jurídica del tipo penal (hurto, estafa, etc.). Pero el uso de este medio moderno puede hacer surgir nuevos conflictos de intereses y, de esta manera, necesitar una protección de nuevos bienes jurídicos por vía de la reforma penal. El uso de balances falsos como medio para cometer estafas y la posterior introducción de tipos particulares de balance falso (como protección de derechos e intereses de información) constituye un ejemplo clásico de este desarrollo de la dogmática penal en su estrecha vinculación con la política criminal y la criminología.