# PERSPECTIVA CRIMINOLÓGICA DEL CRIMEN POR COMPUTADORA

**Catedrático Alonso Salazar***
Abogado costarricense

*El mito de la razón no dejará precisamente de ser mito, sólo en una ofuscación ilusoria podrá ser transformado en una parte del saber. La legitimidad del medio de la demostración no podrá ser probada antes de que se acepte la razón.*[A]

*Un problema puramente teórico –un problema de ciencia pura- siempre consiste en la tarea de encontrar una explicación, la explicación de un hecho o de un fenómeno o de una regularidad notable o bien de una notable excepción a una regla.*[B]

*El Estado debe asegurar que los individuos que son considerados «criminales» merecen la desaprobación que este término denota.*[C]

(Recibido 09/07/18 • Aceptado 21/11/18 )

* Profesor Catedrático de Derecho Penal. Universidad de Costa Rica. Costa Rica
Email: asalazar@salazarabogados.net
Tel: (506)2588-1200

A Kolakowski, Leszek, *La presencia del mito.* Ediciones Cátedra, Madrid, España, 1999, p.50.

B Popper, Karl, *Enbusca de un mundo mejor*, Ediciones PaidósIbérica, S.A., Barcelona, España, 1994, p. 106.

C Husak, Douglas, Sobre criminalización. *Los límites del derecho pena*l. Marcial Pons, Ediciones Juridicas y Sociales, Madrid, España, 2013, p.159.

**Resumen:** El presente artículo establece un análisis histórico del delito informático principalmente en la República Federal de Alemania. La perspectiva criminológica de la Estafa Informática o Computerbretrug, resulta fundamental para lograr una desmitificación del tipo penal y se considera fundamental para una adecuada comprensión del fenómeno delictual. El análisis propuesto fue ampliamente fundamentado en fuentes bibliográficas y datos estadísticos que sirven de apoyo a las conclusiones del autor, por lo que se expone una visión muy completa del delito y sus principales características.

**Palabras Clave:** Delito informático. Fraude electrónico. Delito por computadora. Estafa informática. Cifra negra. Delincuente. Víctima.

**Abstract:** This article presents a historical analysis of cybercrime, mainly in the Federal Republic of Germany. The criminology-based perspective of the Computer Fraud or Computerbretug is paramount to achieve a criminal type demystification. Also, this is considered highly important for an adequate understanding of the criminal phenomenon. The proposed analysis is well-grounded on bibliographical sources and statistical data, which support the author's conclusions; to ensure a thorough view of this crime and its main characteristics.

**Key Words:** : Cybercrime, Electronic fraud, Computer-related crime, Computer fraud, Unrecorded Crime Rate, Criminal Offenders, Victim

## Indice

## Tabla de Abreviaturas

| | |
|---|---|
| 2. WiKG | 2ª. Ley para el Combate de la Criminalidad Económica (2. Gesetz zur Bekämpfung der Wirtschaftskriminalität). |
| AT | Parte General (Allgemeiner Teil). |
| BB | El Asesor Comercial (citado por año y página) Der Betriebs-Berater (zitiert nach Jahr und Seite). |
| BGBl | Boletín Oficial del Gobierno Federal (Bundesgesetzblatt). |
| BT-Drucks | Impreso del Parlamento Federal (Drucksache des Bundestages). |
| CR | Computación y Derecho (revista) (Computer und Recht Zeitschrift). |
| Diss | Tesis doctoral |
| EDV | Procesamiento electrónico de datos (Elektronische Datenverarbeitung). |
| FAZ | Frankfurter Allgemeine Zeitung (Periódico Alemán). |
| FS | Libro homenaje (Festschrift). |
| Hrsg. | Editor. |
| Jura | Enseñanza jurídica -revista (Juristische Ausbildung). |
| LK | Comentario Leipziger (Leipziger Kommentar). |
| NJW | Nueva Revista Jurídica Semanal (Neue Juristische Wochenschrift). |
| Nr. | Número. |
| NStZ | Nueva revista de Derecho Penal (Neue Zeitschrift für Strafrecht). |
| S. | Oración o página. |
| SRI | Stanford Research Institute International. |
| StGB | Código Penal alemán. |
| wistra | Revista de Economía, Impuestos, Derecho Penal (Zeitschrift für Wirtschaft, Steuer, Strafrecht). |

## 1) Planteamiento del problema.

El delito informático ha tomado en Costa Rica nuevos bríos. Debemos tener presente que podemos referir que el delito informático existe en nuestro país desde hace ya más de tres décadas, sus orígenes se remontan a la reforma de la Ley de Aduanas en el año 1995, luego al Código de Normas y Procedimientos Tributarios del año 1999, la Ley de Derechos de Autor y Derechos Conexos del año 2000, la Ley de Administración Financiera de la República y Presupuestos Nacionales del año 2001, la reforma del Código Penal del año 2001 (Ley 8148 de 24 de octubre de 2001[1] ), más recientemente, la Ley sobre Delitos Informáticos del año 2012 (Ley 9048).

El problema que presenta el análisis y comprensión de esta forma de delincuencia, radica fundamentalmente en la ausencia de un verdadero tratamiento dogmático de la cuestión y considero particularmente necesario, un abordaje desde la perspectiva criminológica del delito, que amplíe el espectro de comprensión y quizás, permita desmitificar algunos de los prejuicios que aún hoy existen en torno a ella, es a esta tarea a la que me abocaré en este trabajo.

El presente estudio lo fundamentaré en la dogmática alemana, el estado de la situación en Alemania y las estadísticas actualizadas al año 2000. No obstante, en el tiempo transcurrido, lo cierto es que la realidad no ha cambiado en lo que al objeto de estudio se refiere (historia del delito), por lo que la validez de los análisis hechos se conserva. Debe tenerse presente que se trata de una investigación cualitativa e histórica y no cuantitativa, así que el empleo de datos estadísticos es más bien una herramienta de apoyo de esa perspectiva histórica.

## 2) Introducción y antecedentes históricos.

Desde hace ya 17 años regresé de la República Federal de Alemania, luego de hacer estudios de post grado en la Universidad de Friburgo de Brisgovia con el Profesor Klaus Tiedemann, en aquel entonces, una de las más destacadas autoridades académicas mundiales en el ámbito de la Criminalidad Económica y dentro de ésta, la criminalidad informática.

---

1 Cfr. Chinchilla Sandí, Carlos, *Delitos Informáticos, Elementos básicos para identificarlos y su aplicación*, San José, Costa Rica, Ediciones Farben, 2004, p. 24.

Precisamente mis estudios lo fueron en relación con la Estafa por Computadora (Computerbretrug gemäβ dem § 263a StGB), de acuerdo con el artículo 263 del Código Penal alemán. Ese tipo penal, prácticamente idéntico, fue el que se copió y se introdujo en Costa Rica en el artículo 217 bis del Código Penal mediante la Ley 8148 del 24 de octubre de 2001.

Ya para la fecha de la reforma costarricense, el texto del artículo 263a del Código Penal alemán, había sufrido algunas modificaciones, que fueron introducidas por la Sexta Ley de Reforma del Código Penal alemán[2] (Das sechste Strafrechtsreformagesetz[3]).

He de confesar, que mi intención inicial al regresar de Alemania, fue traducir mi tesis, y de esta manera acercar al costarricense que no tuviera conocimiento de la lengua alemana; con lo que consideraba era el texto más actual sobre dicho delito que se había escrito en ese momento en nuestro medio y que además, incorporaba prácticamente el análisis del tipo penal que contenía la Ley 8148 del 24 de octubre de 2001. Es más, reconozco que ello era una obligación moral que debí haber cumplido.

Para esa fecha y casi coincidiendo con mi regreso de Alemania, la Corte Suprema de Justicia a través de la Escuela Judicial, en esa época dirigida por el hoy decano de la Facultad de Derecho, el Prof. Dr. Eric Alfredo Chirino Sánchez, publicó una licitación para hacer una consultoría en delitos informáticos.

Cuando se publicó dicha licitación, para mí fue como un sueño hecho realidad, pues dentro de la propuesta se solicitaba la elaboración de un texto que sirviera de base para la capacitación de jueces, fiscales y defensores, así como operarios jurídicos, sobre lo que se denominaba

---

2 Ver *in toto*, Salazar Rodríguez, Alonso, La Sexta Ley de Reforma del Código Penal de la República Federal de Alemania, en Cuadernos de Doctrina y Jurisprudencia Penal, Argentina, Año V, Número 8 C, p. 1117-1132, y en RdPP (Revista de Derecho Penal y Procesal Penal), España, núm. 3, 2000 p. 233-236, en Revista de Ciencias Jurídicas, Universidad de Costa Rica - Colegio de Abogados de Costa Rica, Número 93, Setiembre - Diciembre 2000, p. 57 sgtes.

3 La Sexta Ley de Reforma del Código Penal Alemán, fue aprobada por el *Deutscher Bundestag* (Parlamento alemán) el 14.11.1997, se publicó en el BGBl (Diario oficial alemán) 1998/I 164 ss. el 26.1.1998, entró en vigencia el 1° de Abril de 1998. En adelante se cita por sus siglas en alemán como 6. StrGR.

como "una nueva forma de delincuencia casi desconocida en nuestro medio".

Confieso, que me emocioné en aquel momento y decidí participar en el proceso, sin embargo, no resulté ganador del concurso, sino que el mismo le fue adjudicado al Prof. Henry Issa el Khoury Jacob, quien no sólo había sido mi profesor de Derecho Penal general en la Facultad de Derecho, sino profesor de prácticamente todas las personas vinculadas con el Derecho Penal en aquel momento, y con quién tenía para ese entonces una relación muy cordial.

Al ver el resultado del concurso, sentí que yo era quien mejor capacitado estaba en aquel momento en el país para hablar del tema, al fin y al cabo, era en ese entonces probablemente el único experto en la materia, graduado en ese tema y venía con grandes deseos de transmitir el conocimiento adquirido durante mis estudios. Con resignación, acepté el resultado del concurso y simplemente esperé a que el Prof. Issa, realizara su obra y la presentara. Mi intención [muy al estilo alemán], era que una vez que viera la luz dicha obra, contrastarla con la mía y allí iniciar una discusión sobre el tema, según yo, para mediante esa vía hacer progresar la dogmática costarricense.

Poco tiempo después de que se dio la adjudicación del concurso, en la Facultad de Derecho fui abordado por el Prof. Issa quién me pidió que colaborara con su proyecto, pues según me decía, quería contar con mi apoyo en ello.

Recuerdo muy bien que le dije al Profesor Issa, que me parecía más adecuado, que él hiciera la investigación y que una vez que estuviera lista y publicada, yo con mucho gusto la estudiaría y le haría las observaciones que considerara pertinentes. Con gran asombro para mí, el Prof. Issa me dijo, que él tenía que empezar de cero, que era un tema nuevo para él y que consideraba que yo podía colaborar al respecto, le respondí, que si él consideraba que tenía ese tipo de problemas, que no contaba con la bibliografía y la pericia en el campo, que lo correcto y ético, era que renunciara al proyecto y me permitiera a mí hacer el trabajo. Ni el profesor Issa ni yo cedimos un ápice y a partir de ese momento nuestra relación se deterioró.

Sé muy bien, que ese acontecimiento marcó mucho mi destino y consecuentemente mi relación con el profesor Issa y de allí se derivaron

una serie de problemas con otros colegas en la misma Facultad de Derecho, de eso estoy muy consciente y no me arrepiento de lo que hice, incluso lo volvería a hacer si fuera necesario; es más, estoy seguro que esta introducción probablemente me traerá problemas en el futuro próximo, pero francamente; ya eso me tiene sin cuidado, he aprendido a vivir con ello.

Un tiempo después, tal vez uno o dos años luego de que se inició la ejecución del proyecto por parte de la Escuela Judicial, me buscó otro gran jurista a quien he considerado siempre un maestro y una persona de una entereza y calidad excepcional, el Prof. Dr. Daniel González Álvarez, con quien para ese entonces tenía una muy cercana relación académica y quien era Presidente de la Sala Tercera de la Corte Suprema de Justicia. Don Daniel, me pedía ayuda para sacar adelante el proyecto que la Escuela Judicial le había adjudicado al Profesor Issa, que según me indicaba, nunca vio la luz (las razones las desconozco, pero creo conocerlas y prefiero reservármelas).

Cuando Don Daniel me buscó, me reconoció el hecho de que el proyecto no avanzaba, que la Corte seguía teniendo la necesidad de que concluyera y pedía mi colaboración para realizarlo. Yo en ese momento me sentí profundamente orgulloso de ver que finalmente la misma Corte a través de tan insigne emisario, pretendía enmendar lo que siempre consideré un error y me dispuse de inmediato a colaborar en ello.

He de reconocer eso sí, que casi de inmediato mi ilusión y orgullo se transformaron en desilusión y enfado, cuando Don Daniel me dijo que mi colaboración debía ser ad honorem, ya que no se podía remunerar mi trabajo puesto que ésta era una idea más personal que institucional con el afán de lograr concluir el proyecto.

Yo conocía claramente lo que la Escuela Judicial tenía de presupuesto para el proyecto y lo que había sido adjudicado y desde luego a quién, razón por la cual le dije a Don Daniel que no estaba dispuesto a permitir que finalmente el proyecto fuera concluido con mi esfuerzo y conocimiento, cuando él bien sabía dónde habían ido a parar los fondos previstos para el mismo y que en tales condiciones y sin que existiera una enmienda de lo actuado no estaba dispuesto a colaborar. Don Daniel, que es un gran caballero, me pidió que reflexionara, que pensara, que le ayudara y yo, lo deseaba, pero mis principios morales no me permitían hacerlo en tales condiciones y no lo hice.

Producto de mi enfado, me juré, que nunca iba a volver a escribir sobre este tema, hasta que la obra de la Escuela Judicial viera la luz y así poder literalmente "confrontarla con la mía". En mi mal proceder pretendí evidenciar que era a mí a quien debió haber sido adjudicado ese proyecto [pura vanidad personal y orgullo, egoísmo si se quiere, queda al (la) lector (a) autorizado a calificarlo como mejor le parezca, al fin y al cabo lo merezco y pido perdón por ello, si es que cabe], es la razón por la cual, a pesar de tener mi tesis tanto en alemán como en español traducida desde hace unos 16 años, nunca he querido publicar nada de ella… sigo esperando la obra de la Escuela Judicial. El profesor Issa murió prematuramente, a la edad de 56 años, el 2 de junio del año 2003 (q.d.D.g) y nunca ha llegado a mis manos, texto suyo alguno sobre delitos informáticos…entonces al fin y al cabo qué más da!

El día 16 de noviembre de 2016, se le rindió un merecidísimo homenaje al Prof. Dr. Dr. Francisco Castillo González, por parte de la Asociación Costarricense de Ciencias Penales, en ese evento coincidí con el Dr. Daniel González Álvarez quién como siempre con su don de gentes, me hizo sentir como en los "viejos tiempos" y me dijo que al estar a cargo de la Revista de la Asociación de Ciencias Penales de Costa Rica con gusto recibiría cualquier artículo que tuviera a bien enviarle. Comprendiendo por medio de las palabras del Prof. Castillo al recibir el homenaje que se le hacía, que al final de cuentas lo que queda es lo escrito, he decidido cambiar de opinión y finalmente, comenzar a publicar algunas partes de mi tesis, que creo pueden aún ser de interés para el foro.

Así que: Don Daniel, creo que muy tarde, de muy mala manera y admitiendo mi gran error, espero que estas notas vean la luz en la Revista de la Asociación de Ciencias Penales de Costa Rica y que sirvan, al estar dedicadas a usted, como una disculpa por mi mal proceder. Indico que debido a que esta revista dejó de publicarse, mi artículo no fue publicado. Por este motivo, se incluye ahora, en la Revista de Ciencias Jurídicas .

## 3) Perspectiva criminológica del crimen por computadora.

A la perspectiva criminológica del crimen por computadora pertenecen entre otros las características del delito, del delincuente, de la víctima, así como las características de la acción punible (relación delincuencial). Las características que aquí se analizan, sólo son aquellas

que identifican en detalle el delito por computadora. Con respecto a los delincuentes y víctimas es necesaria una comprobación de su prototipo típico, que hasta el momento ha sido manejado por la dogmática penal, para poder entender el fenómeno de este "crimen por computadora" y su desarrollo.

### 4) Características del delito por computadora.

Los delitos por computadora, los cuales son llevados a cabo por medio de una computadora, tienen una especial característica con respecto al recurso utilizado, ya que hacen parecer a estos delitos como "sui generis". Con estas particularidades encontramos p.ej. el hecho, las posibilidades de descubrimiento y la fijación del daño por un lado (víctima) o del beneficio por el otro lado (delincuente), los cuales resultan de estos delitos.

El crimen por computadora se presenta como un fenómeno internacional que, con la acentuación diferenciada e independiente de toda formación de sistemas económicos, aparece como tendencia en todas partes donde se utilizan computadoras[4]. Como características válidas para casi todos los delitos por computadora, se pueden mencionar las siguientes: a) rapidez y acercamiento del hecho, con respecto al tiempo y lugar de comisión, b) posibilidades de encubrimiento, c) posibilidad de eliminación de rastros, d) efecto permanente o "permanencia del hecho", e) cifra negra y f) valor del daño.

### a) Rapidez y acercamiento del hecho (tiempo y lugar de comisión).

Los equipos de informática y sus programas hacen posible que hechos criminales, manipulaciones y otros hechos sean trasladados en tiempo, quiere decir, que el delincuente no tiene que estar presente cuando se lleva a cabo el "hecho" – acción que fue programada por el delincuente. El delincuente puede estar muy lejos del lugar del hecho o hasta en el extranjero. De manera muy distinta sucede con delitos normales, en los que existe por lo general una relación directa entre el delincuente y el hecho.

---

[4] Tiedemann, Klaus; Cosson, Jean, Straftaten und Strafrecht im deutschen und französischen Bank- und Kreditwesen, Köln/Berlin/Bonn/München, 1973, p. 25.

Gracias a las posibilidades de desplazamiento de tiempos, el delincuente puede llevar a cabo otras actividades, mientras el delito se está cometiendo. Estas características del delito por computadora dificultan, de cierto modo, el descubrimiento del hecho, la identificación del delincuente y sobre todo las medidas de control.

### b) Posibilidades de encubrimiento.

La característica mencionada anteriormente da a los delincuentes de delitos por computadora una gran variedad de posibilidades para camuflar su acción[5]. Existe la posibilidad, p.ej. de que el delincuente manipule un programa de cómputo para que el programa ejecute una tarea no autorizada o reprogramada. El delincuente o una persona escogida por éste, obtienen así un beneficio patrimonial ilícito y el programa reprogramado "automáticamente" elimina esta orden dejando el programa en el estado original, o sea, como se encontraba antes de la manipulación[6].

De esta forma no se podrá saber lo que sucedió realmente, ni cómo lo logró el delincuente, no se podrá hacer de forma visual, ni por análisis del programa, ni por la comprobación del proceso.

Históricamente muchos de los delitos que se llegaron a conocer fueron descubiertos por casualidad[7], por razones aleatorias como un error o una "traición" de una persona involucrada en el caso. Por ejemplo, otro delincuente, ayudantes o co-delincuentes, por distracción, cuando un colaborador deja de laborar y el programa ya no funciona en forma óptima, o por una revisión o control del programa por una falla técnica o daño[8].

Como muestran las estadísticas de la República Federal de Alemania, la tasa de reconocimiento del crimen por computadora desde la entrada

---

5 United Nations, op. cit.; Möhrenschlager, Manfred, Computerstraftaten und ihre Bekämpfung in der Bundesrepublik Deutschland, wistra 1991, p. 128.

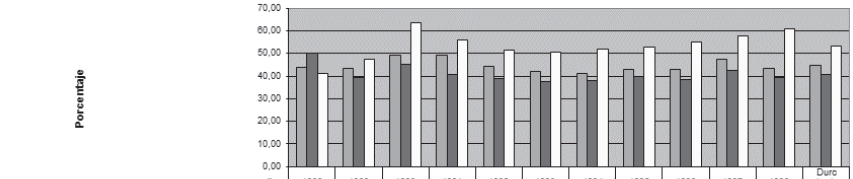
6 Devara Rodríguez, Miguel Ángel, *Manual de Derecho Informático*, Madrid, Editorial Aranzadi, 1997, p. 299 s.

7 Tiedemann, Klaus; Cosson, Jean, op. cit, p. 152; Parker, Donn B./Nacum,, Susan/Aura, S.Stephen, (Hrsg.), *Computer Abuse von Stanford research Institute*, 1973, p. 53.

8 AHL, D.H. *Employee Computer Crime on the Rise*, Creative Computing, Band 11, Juni, 1985, p. 80 s.; Sieber, Ulrich, *Computerkriminalität und Strafrecht, 2.*, um einen Nachtrag ergänzte Auflage, Köln, Berlin, Bonn, München, 1980, p. 174 s., con referencias bibliográficas adicionales.

en vigencia de la ley que introdujo en el Código Penal este tipo de delitos (1986) hasta el año 1998, era por debajo del 50%. Con respecto al crimen por computadora en general, se puede decir que la tasa de reconocimiento en un período de 11 años fue en promedio de 44,5%. Pero con respecto al fraude por computadora, aparece en la estadística una división entre el fraude por medio de tarjetas obtenidas ilegalmente para obtención de efectivo o uso en cajeros automáticos y las demás variantes según § 263a StGB. En el primer caso, el fraude por medio de una tarjeta obtenida de forma ilícita, se encuentra la tasa de reconocimiento por debajo del 40,89%. Con respecto a las demás variantes del fraude por computadora es la tasa de reconocimiento del delito es mucho más elevada, en promedio 53,41%.

**Tasa de reconocimiento de delitos por computadora**




| Año | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | 1994 | 1995 | 1996 | 1997 | 1998 | Durchschnitt |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Computerkriminalität | 43,70 | 43,50 | 49,20 | 49,30 | 44,30 | 42,10 | 41,20 | 42,90 | 43,00 | 47,50 | 43,40 | 44,55 |
| Betrug mittels rechtswidrig erlangter Karten für Geldausgabe bzw. Kassenautomaten | 50,30 | 39,40 | 45,20 | 40,60 | 39,00 | 37,40 | 37,90 | 39,70 | 38,50 | 42,40 | 39,40 | 40,89 |
| Andere Varianten des § 263a StGB | 41,10 | 47,20 | 63,70 | 56,80 | 51,40 | 50,50 | 51,80 | 52,60 | 55,20 | 57,50 | 60,70 | 53,41 |

- *Computerkriminalitat: criminalidad por computadora*
- *Betrug mittels rech tswidrig erlang Karten fur Geldausgabe bzw: Estafa por medio de tarjetas de pago y/o tarjetas de cajero automático obtenidas ilegalmente*
- *Andere Varianten des 263ª StGB: Otras variantes del artículo 263del StGB*

Fuente: Bundeskriminaltamt [Anm. 53]

## c) Posibilidad de eliminación de rastros/huellas.

La tercera característica del delito por computadora es la facilidad de eliminación de rastros, que es lo que realmente obstaculiza el descubrimiento del delito. Esta característica se desarrolla en muchos casos por la familiaridad del delincuente con el equipo de informática y la eliminación de rastros se hace posible por su carácter de profesional.

La eliminación de rastros depende de factores como, si el equipo de informática ofrecía medidas adecuadas de seguridad y control o, si por la flexibilidad o dinámica del proceso de información el descubrimiento de actividades ilegales es obstaculizado después de su descubrimiento. En otros casos es posible que el equipo de informática o el programa admitan

relativamente fácil – hasta para usuarios externos – la eliminación de datos, programas, procesos matemáticos, etc. Especialmente difícil es la prevención y persecución penal de Hackers profesionales, los cuales no dejan rastros en el sistema y en no poco casos, se terminan esclareciendo por las mismas declaraciones de los autores[9].

### d) Efecto permanente o "permanencia del hecho".

Una característica de las manipulaciones por computadora es el efecto permanente o "permanencia del hecho"[10], el cual se da a raíz de las múltiples posibilidades de repetición de la manipulación, un cierto automatismo del recorrido del hecho, así como por una imposibilidad práctica de control[11]. Si el hecho o acción da resultado con el primer intento, entonces se repetirá permanentemente – especialmente con respecto a la manipulación de programas y de los llamados datos básicos – hasta que por casualidad[12], o por controles muy dirigidos, son encontrados[13]. Esta característica también tiene relación con respecto a la desvinculación espacio- temporal de hechos y efectos.

Se han llegado a conocer casos[14], en los cuales p.ej. un solo delincuente realizó más de setenta retiros, para conseguir el monto deseado[15], o los delincuentes hicieron uso de las "tarjetas falsas" elaboradas por ellos, para cajeros automáticos, en un caso 3000 tarjetas[16].

---

9 Tiedemann, Klaus; Cosson, Jean, *op. cit.,* p. 1373 (1378).

10 Fischer, Thomas, *Computer-Kriminalität*, Gefahren und Abwehrmaßnahmen, Bern, 1979, p. 14.

11 Göppinger, Hans, *Kriminologie*, 5. Auflage, München, 1997, p. 546.

12 Fischer, Thomas, op. cit., p. 12.

13 Tiedemann, Klaus, *Computerkriminalität und deutsche Strafrechtsänderung von* 1986, Publications de la Section Hellenique de la Société Internationale de Défense Sociale, 1988, p. 29; Tiedemann, Klaus, *Wirtschaftstrafrecht und Wirtschaftskriminalität II*, Besonderer Teil, Hamburg, Rowohlt, 1976, p. 152; Mühlen, Rainer A.H. von zur, *Computer-Kriminalität*, Gefahren und Abwehr. Neuwied/ Berlin, 1973, p. 25.

14 Bandekow, Klaus, *Strafbarer Missbrauch des elektronischen Zablungsverkehrs.* Zur Strafbarkeit der missbräuchlichen Inanspruchnahme von Geldausgabeautomaten, Chip-Karten-Systemen und Bildschrirmtext-Leistungen unter Berücksichtigung von Kriminologie und Kriminalistik, Diss., Lübeck, 1988, p. 71, con referencias adicionales.

15 Cfr. LG Hannover, VM 1984, p. 804 s.

16 Sieber, Ulrich, op. cit., p. 10.

Con respecto a esta característica Sieber diferencia entre un inexacto Output impreso o datos de ingreso inexactos que conllevan a manipulaciones en programas de Inputs, Manipulaciones de consola y Manipulaciones en programas privados, todas las manipulaciones Output y manipulaciones de programas regulares, así como manipulaciones que conllevan a datos de ingreso inexactos. El delincuente se encuentra en posibilidad de hacer uso repetidamente de las manipulaciones mencionadas de primero, por haber encontrado en el desarrollo organizacional del centro de informática un error o posibilidad de manipulación, lo que llama Sieber una "frecuente posibilidad repetitiva de manipulación". Por otro lado se tiene el "automatismo del hecho". En este segundo grupo de manipulaciones se entiende bajo automatismo, la manipulación de la computadora que se lleva a cabo independientemente cada vez que se hace uso del programa manipulado o con cada levantamiento de datos básicos inexactos[17]. El efecto constante del delito por computadora también fue llamado el fundamento para la cifra negra del delito por computadora[18].

### e) Cifra negra.

Las cifras desconocidas del crimen por computadora deben ser muy altas[19], y una simple estimación de esta cifra sería prácticamente imposible[20]. Como cifra negra/desconocida o espacio oscuro se describe el área de hechos criminales que no aparecieron en las estadísticas[21] o

---

17 *Ibid*., p. 133 s., con referencias bibliográficas adicionales y ejemplos.

18 Kaiser, Günter, *Kriminologie*, 3. Aufl., Heidelberg, 1996, § 74, Rn. 60.

19 Tiedemann, Klaus; Cosson, Jean, op. cit., p. 1373; *Möhrenschlager, Manfred, Das neue Computerstrafrecht, wistra* 1986, también el mismo en *Möbrenschlager, Manfred, op. cit*., p. 321 (324); *Göppinger, Hans,* op. cit.; p. 542; Sieber, Ulrich, op. cit., p. 2/131; Council of Europe, Computer-related Crime, 1990, Recommendation No. R (89), Strasbourg, 1990, p. 17. Exorbitantemente alto según Hofmann, Rolf, *Unterschlagungsprophylaxe* und *Unterschlagungsprüfung*, Berlin, 1997, p. 84 y Kolz, Harald, Zur *Aktualität der Bekämpfung der Wirtschaftskriminalität für die Wirtschaft*, wistra 1982, p. 167 (170); Bandekow, Klaus, op. cit., p. 71 sgte.

20 *Tiedemann, Klaus*, op. cit., p. 27; la critica por Poerting, Peter/Pott, Ernst G, *Computerkriminalität, Bundeskriminalamt*, Wiesbaden, 1986, p. 39 s.

21 Meier, O, *Dunkelziffer oder Dunkelfeld,* Bonn, Diss., 1956, p. 4; Hentig, Hans von, *Zur Psychologie der Einzeldelikte*, Band 1: Diebstahl, Einbruch, Raub, Tübingen: Mohr, 1954, p. 18.

que no fueron dadas a conocer oficialmente, o sea, las que no fueron dadas a conocer en las entidades penales y por lo tanto no incluidas en las estadísticas criminales[22]; quiere decir, las violaciones legales que oficialmente no se conocieron ni se registraron[23]. Kaiser parte del punto, que los casos llegados a conocer del crimen por computadora, sólo representan la punta de un iceberg y que se debe partir de una cifra oscura muy alta[24]. Se dice, que para un caso descubierto se deben tomar un aproximado de 4 - 100 casos no descubiertos[25].

Esto también fue tratado en los Estados Unidos. Las cifras numéricas publicadas, las cuales partían de una alta cifra negra y de una tendencia creciente de criminalidad por computadora[26], sólo resultarían en toscas estimaciones. Jay Becker[27], Jefe del "National Center for Computer Crime Data" en base a fuentes del FBI, menciona que solo un 1% del crimen por computadora es descubierto, y que de este aproximadamente solo un 14% llega al conocimiento de las entidades investigadoras, y de estas a su vez, sólo un 3% de los casos son llevados a sentencia de pena privativa de libertad[28].

Dentro del crimen por computadora cabe la posibilidad de la existencia de un amplio espacio oscuro[29], sobre todo por las escasas

---

22 Sieber, Ulrich, op. cit., p. 173, con referencias bibliográficas adicionales.

23 Kaiser, Günter, op. cit., Rn. 80 s., con referencias bibliográficas adicionales. Göppinger, Hans, op. cit., p. 490.

24 Kaiser, Günter, op. cit., Rn. 58.

25 Steinke, Wolfgang, Die Kriminalität durch Beeinflussung von Rechnerabläufen, NJW 1975, p. 1867-1869, NStZ 1984, 295 (297) con referencias bibliográficas adicionales.

26 Los factores de este fenómeno fueron mencionados por Sieber, una repetición en este punto no es necesaria, además, el mismo autor no pudo comprobar si en la práctica los factores citados por Sieber todavía deben ser considerados. De todas formas se debe suponer, que la cifra negra (desconocida) del crimen por computadora debe ser muy alta. Cfr. Sieber, Ulrich, op. cit., p. 174 s.

27 Baker, Jay J., The Investigation of computer crime. An Operational Guide to White Collar Crime Enforcement, National Center for Computer Crime Data Head, Antitrust Section, Los Angeles Country District Attorney´s Office, California, sin fecha, p. 6, 43.

28 Cfr. Sieber, Ulrich, op. cit., 2/130.

29 Sieber, Informationstechnologie und Strafrechtsreform. Zur Reiche des künftigen Zweiten Gesetzes zur Bekämpfung der Wirtschafskriminalität, Köln, Berlin, Bonn, München, 1985, p. 33 s.

posibilidades de descubrimiento, los escasos estándares de seguridad, así como la creciente propagación de la informática. Precisamente la existencia de esta cifra negra no permite emitir conclusiones finales sobre el volumen total de delitos ni sobre la estructura del espacio oscuro de este tipo de criminalidad[30].

### f) Valor del daño.

El valor del daño de un delito por computadora se refleja en la estadística de los años setenta como una característica[31], esto es, que se consideraba un hecho distintivo del delito el que los daños causados con esta forma de delincuencia eran enormes. Las investigaciones realizadas se enfocaron principalmente en el abordaje de esta característica[32], adicionalmente fundamentaron el que los daños resultaran enormes o encontraron una justificación para ello en el hecho de que para ese momento existía una reducida regulación del crimen por computadora, a la que denominaban una "nueva forma de delitos"[33], que es exactamente lo se denominó "el valor del daño" ocasionado[34]. En varios de los casos

---

30 Poerting, Peter/Pott, Ernst G, *op. cit*., p. 45.

30 Poerting, Peter/Pott, Ernst G, op. cit., p. 45.

31 BT-Drucks. 10/318, p. 12; Sondermann, Markus, Computerkriminalität, Die neuen Tatbestände der Datenveränderung gem. § 303 a StGB und der Computersabotage gem. § 303 b. StGB, Diss., Münster, 1989. p. 3 s.; Fischer, Thomas, op. cit., p. 9 sgte; Möhrenschlager, Manfred, op. cit., p. 128 (131); Sieg, Rainer, Strafrechtlicher Schutz gegen Computerkriminalität, Jura 1986, p. 352 (353).

32 Bequai, A. Computer Crime, Lexington, 1978, p. 1 sgte.

33 Cfr. Sieber, Ulrich, op. cit., p. 34 s.; Soyka Joachim, *Tatwaffe Computer*, Datenmanipulation, Softwarediebstahl, EDV-Spionage, München, 1988, p. 253 s.; Norman, Adrian R.D., *Computer insecurity*, London/New York, 1983. Passim; Zimmerli, Erwin/Liebl, Karlhans, *Computermissbrauch*, *Computersicherheit*, Fälle-Abwehr-Aufdeckung, 1. Aufl., Ingelheim: Hohl, 1984, p. 17 s.; Dinardo, C.T., Computer crime, in: The Information Technology Series, Computers and Security, Volume III, New Jersey, 1978, Passim; Farr, Robert, The Electronic criminals, New York/St. Louis/San Francisco/Düsseldorf/London/Mexico/Sydney/Toronto, 1975, p. 33 s.; Wasik, Martin, *Crime and the Computer,* Oxford, 1991, p. 34 s., con referencias bibliográficas adicionales.

34 Schlüchter, Ellen, *Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität,* Kommentar mit einer kriminologischen Einführung, Heidelberg, 1987, p. 85 con referencias bibliográficas adicionales; cfr. Kolz, Harald, op. cit., p. 167 (170).

llegados a conocer, se demostró que los daños eran enormes, p.ej. "The Equity Funding case", en donde una empresa aseguradora perdió más de $ 30,1 millones a razón de 56.000 manipulaciones[35]. En la actualidad también existe la opinión, que el daño ocasionado por el crimen por computadora es muy alto[36].

El problema que persiste todavía es el de la definición del valor del daño con respecto al crimen por computadora, ya que los diferentes estudios empíricos parten de diferentes criterios y de diferentes definiciones del problema, sobre todo de métodos y fuentes que fueron utilizados o por lo menos que fueron citadas[37]. Por esta razón fueron muy criticados los trabajos de SRI (Stanford Research Institut)[38] en USA y en la República Federal de Alemania (von zur Mühlen)[39].

Taber[40] repara con referencia a esta crítica lo siguiente: a los estudios de SRI se les da más significado del que merecen; SRI causa confusión, ya que no sólo abarca hechos criminales, sino que los casos reconocidos muchas veces fueron descritos como violaciones por computadora, ya que SRI las toma como tales y no ve oportuno una discusión al respecto. Muchos casos, los cuales SRI toma de la prensa especializada, se remontan a noticieros no confirmados, los cuales la prensa especializada recibe a su vez del servicio de recorte de periódico. Los indicadores de verificación de SRI son engañosos y las estimaciones de daños de SRI son dudosas[41]. En la República Federal de Alemania también se criticaron las estimaciones de von zur Mühlen, ya que las fuentes utilizadas por él no eran claras. Pero por la actividad de von zur Mühlen, como asesor empresarial para asuntos de seguridad y revisión, se estima que él dispone de una buena fuente de conocimiento[42].

---

35 Cfr. Council of Europe, *op cit*.; de forma detallada por Sieber, Ulrich, *op. cit*., p. 141 s., con referencias bibliográficas adicionales.

36 *Tiedemann*, Kaiser-FS, 1373 (1373) con referencias bibliográficas adicionales; Kaiser, Günter, *op. cit.*, § 74, Rn. 59 s.

37 Cfr Wasik, Martin, op. cit.; Sieber, Ulrich, *op. cit.,* p. 29.

38 Parker, Donn B./Nacum,, Susan/Aura, S.Stephen, *op. cit.* , p. 53; Parker, Donn B., *Crime by Computer*, New York, 1. Aufl, 1976; Parker, Donn B., Fighting *Computer Crime*, New York, 1983.

39 Mühlen, Rainer A.H. von zur, op. cit., p. 17.

40 Taber, John K, *A Survey of Computer Crime Studies*, in: Computer/Law Journal, Vol. II, 1980, p. 288 s.

41 Cfr. Wasik, Martin, op. cit., p. 34 s.

42 Poerting, Peter/Pott, Ernst G, op. cit., p. 26.

Las estadísticas han demostrado[43], que los daños por los delitos por computadora son en promedio más altos que los de los delitos patrimoniales clásicos. El significado económico de la tecnología de información actualmente no se discute. En la República Federal de Alemania, p.ej. hacia finales de los años 90 había instalados equipos de cómputo por un valor de aproximadamente 50 mil millones de marcos, y el valor del software para las computadoras podría llegar al doble, la digitalización y la creación de la planificada red de fibra de vidrio estaba estimada en aproximadamente 300 mil millones de marcos. De acuerdo a una estimación de la Comisión Europea del año 1987 el procesamiento de información en su definición más amplia, representa dos tercios del producto interior bruto en Europa[44].

## 5) El delincuente, la víctima y la acción punible.

Como en casi todos los delitos, el delito por computadora tiene su especialidad, la cual, está relacionada con las personas involucradas en el hecho. Por un lado se debe observar el delincuente con más cuidado, ya que éste juega el papel más importante dentro de la observación criminológica, hay que recordar que es el delincuente el que provoca el delito, y no otra persona. Por otro lado y aunque se trate de un crimen por computadora, hay una víctima. Con referencia en hechos perpetrados de casos llegados a conocer del crimen por computadora, se diferencian cuatro grupos de acciones criminales que son la manipulación, el espionaje, el sabotaje y el hurto de tiempo[45].

### a) El delincuente.

La descripción de un delincuente "típico" del delito por computadora con base a los casos llegados a conocer[46] corresponde al de una persona extraordinariamente inteligente y con un "exclusivo conocimiento especializado" en el campo de la informática[47].

---

43 Cfr. Kaiser, Günter, *op. cit.*, § 74, Rn. 59, con referencias bibliográficas adicionales

44 Sieber, Ulrich, Informationsrecht und Recht der Informationstechnik, NJW 1989, 2569 (2569).

45 Cfr.Tiedemann, Klaus, *op. cit*., p. 150 s.; Poerting, Peter/Pott, Ernst G, *op. cit*., p. 27; Fischer, Thomas, *op. cit*., p. 19 s.; Sieber, Ulrich, op. cit., p. 39 s, todos con referencias bibliográficas adicionales.

46 Cfr. Gutiérrez Francés, *María Luz, Fraude Informático y Estafa,* Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones, Madrid, 1991, 74 sgte.

47 Así Sieber, Ulrich, *op. cit*., p. 127 sgte.

El modelo del delincuente de delitos por computadora fue un inofensivo joven americano proveniente de una familia de nivel medio, el cual no tenía conocimiento alguno de que su acto fuera ilegal y frecuentemente[48] se hace mención al síndrome de "Robin Hood"[49]. El delincuente se describió como un hombre joven de 20 a 30 años de edad[50], aficionado[51], inteligente[52], educado[53], terrorista o miembro de una banda[54], muy activo, avispado, con aspiraciones a distinciones y sin ser un delincuente primerizo[55], sin antecedentes penales[56]. La característica de no tener antecedentes penales corresponde sobre todo con la característica de la edad del delincuente[57].

De acuerdo al siguiente cuadro se puede determinar fácilmente que el delito por computadora no puede ser realizado por niños, o sea, delincuentes menores de 14 años. La relación a jóvenes y adolescentes fue en los últimos once años antes de finales de siglo relativamente estable. Desde 1988 la tasa de delincuentes jóvenes fue siempre menor que la de adolescentes, ambas tasas se mantuvieron por debajo del 20%. En el año 1991 se dio el porcentaje más alto de ¨18,3%¨ de delincuentes jóvenes, ya que generalmente este porcentaje se encontraba por debajo del 14% y hasta por debajo del 10% - esto entre 1988 hasta 1990. Niños y jóvenes tienen relativamente menos oportunidad de realizar un abuso[58]. El porcentaje de adolescentes en esta clase de crimen ascendía a 19,4%

---

48 González Rus, J.J., *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, N° 12, Monográfico sobre Informática y Derecho, 1986, p. 111.

49 United Nations, *op. cit.*, p. 8.

50 *Sieber* cita, que este rango tiene entre 23 y 36 años, cfr. Sieber, Ulrich, op. cit., p. 130, con referencias bibliofráficas adicionales, cfr. Bandekow, Klaus, op. cit., p. 58, con referencias bibliográficas adicionales también.

51 Baker, Jay J., op. cit., p. 42.

52 *Tiedemann*, Kaiser-FS, 1373 (1373).

53 Cr. Fischer, Thomas, *op. cit*., p. 14.

54 United Nations, op, cit., p. 5.

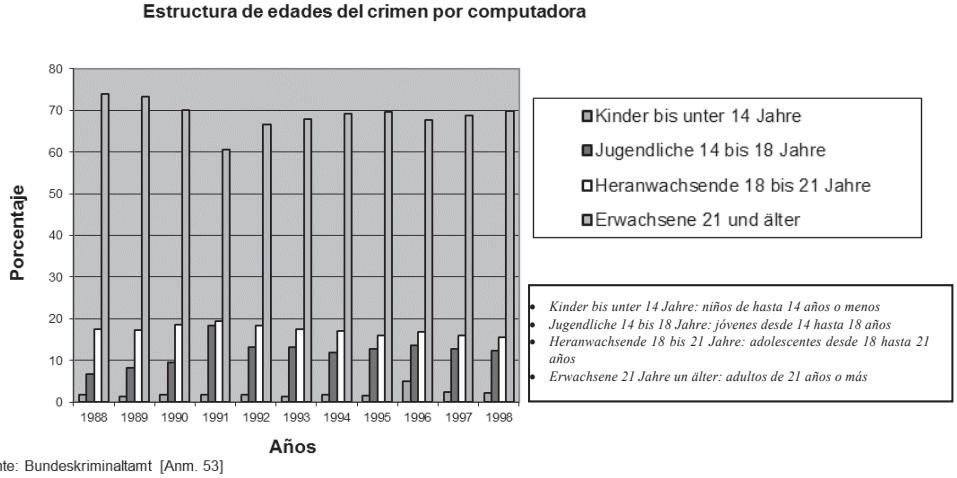
55 Cfr. Parker, Donn B., *op. cit.*, p. 44; Mühlen, Rainer A.H. von zur, *op. cit*., p. 27; Sieber, Ulrich, op. cit., p. 131.

56 Cfr. Bequai, A, *op. cit*., p. 4; González Rus, J.J., op. cit., p. 111; Gutiérrez Francés, María Luz, *op. cit*., p. 75, con referencias bibliográficas adicionales.

57 Cfr. Bandekow, Klaus, op. cit., p. 61.

58 Bandekow, Klaus, *op. cit*., p. 59.

en el año 1991, y a 15,5% en el año 1998. La mayoría de los casos llegados a conocer, o sea, más del 60%, son llevados a cabo por adultos; p.ej. 60,5% en el año 1991 (el menor porcentaje) y 74% en el año 1988[59]. Se estima que personas mayores a los 50 años estarían poco involucradas, especialmente a raíz de esta nueva técnica que para ellos es tan ajena, que prefieren no hacer uso de estos equipos[60].




Fuente: Bundeskriminaltamt [Anm. 53]

Con respecto a la amplia publicidad del "Hacking" en la prensa, se debe indicar que los delitos más sobresalientes para los sistemas de procesamiento de datos de los países industrializados no son realizados por adolescentes, que se limitan simplemente a ingresar a sistemas de cómputo ajenos y a divulgar sus puntos débiles por medio de circulares, sino por delincuentes profesionales, motivados ideológicamente o que operan desde el extranjero. Estos delitos los llevan a cabo por medio del procesamiento de datos, manipulaciones, trastornos empresariales y actos de espionaje[61].

---

59 Bundeskriminalamt (Hg), Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, Bundeskriminalamt Wiesbaden, Berichtsjahr 1987-1998, resumen hecho por el autor.

60 *Ibid*., p 59, con referencias bibliográficas adicionales.

61 Sieber, *op. cit*., p. 19.

Anteriormente los delincuentes, de los casos que se llegaron a conocer[62], eran delincuentes internos, personal de la misma empresa en donde sucedían los hechos[63]. Se pudo determinar, que la participación de las mujeres en abusos en las operaciones de pago, sólo se encontraba en un 11%[64]. Se estima (en manipulaciones), que en casi el 90% de los casos se llevó a cabo el hecho por colaboradores de la víctima[65]; otros estudios en U.S.A. y en Europa muestran, que el porcentaje de "internos" está por debajo del 73%[66]. Únicamente profesionales especializados o personas de especial responsabilidad, que manipulan el Input, el programa o el hardware, y un hacker especializado como externos, fueron tomados anteriormente en consideración, pero actualmente los delincuentes, especialmente en ´Homebanking´ y ´Teleshopping´, son los propios usuarios . En el marco del constante desarrollo tecnológico aparecerá un creciente círculo de delincuentes externos[68], con la divulgación de ´Telebanking´, ´Teleshopping´ etc. así como por el uso de redes globales (Internet) y hoy la expansión en el uso de las redes sociales.

Con respecto a la estructura de género del crimen por computadora en la República Federal de Alemania (antes del año 2000) se deben mencionar ciertas características. Por un lado muestran las estadísticas, que en la mayoría de los casos los ejecutores eran hombres, en promedio un 80% de los casos llegados a conocer en los últimos once años. El porcentaje de mujeres se encontraba por lo tanto por debajo del 20%. Si se ilustra por medio de un gráfico, se daría el siguiente cuadro:

---

62 Cfr. Tiedemann, Klaus, op. cit., p 150 s.; el mismo JZ 1986, 865 (869); Sieber, Ulrich, op. cit., p. 46 s.

63 Cfr. Council of Europe, op cit., p. 19, 37; cfr. Hofmann, Rolf, op. cit., p. 84; Möhrenschlager, Manfred, *Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität* (2. WiKG), wistra 1986, p. 128 (131).

64 Bandekow, Klaus, op. cit., p. 57, con referencias bibliográficas adicionales.

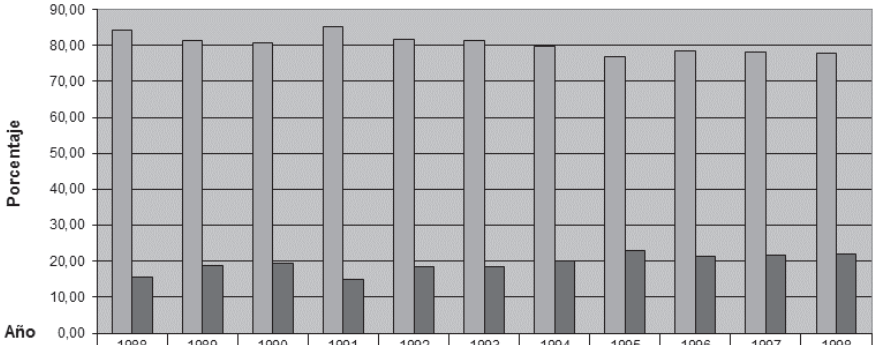
65 Sieber, Ulrich, op. cit., p. 11.

66 United Nations, op. cit. § 35, con referencias bibliográficas adicionales.

67 Tiedemann, Kaiser-FS, 1373 (1376).

68 Tiedemann, LK § 263a, Rn.2.

**Estructura de génro del crimen por computadora**

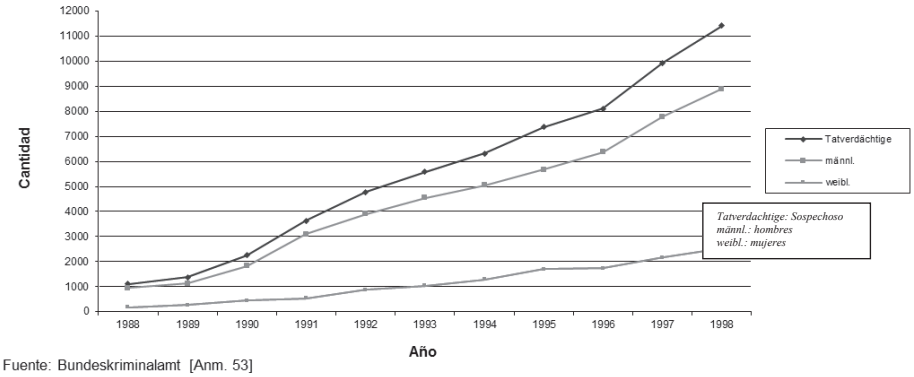



Fuente: Bundeskriminalamt [Anm.

Las estadísticas muestran por otro lado una tendencia, llamada dirección hacia el "crimen femenino por computadora". Está bien claro, que desde la entrada en vigencia del § 263a StGB las mujeres no sólo siempre han participado en el crimen por computadora (como sospechosas - Tatverdächtige), sino que también la tasa porcentual de mujeres involucradas en delitos tiende a aumentar. Con base en el constante crecimiento de mujeres profesionales, no se puede esperar un cambio de esta tendencia[69]. Con referencia a la participación de los hombres se pude decir que el crecimiento de casos en los que están involucrados es menor que comparado con las mujeres.

[69] Bandekow, Klaus, *op. cit.*, p. 58.

**Estructura de género en el crimen por computadora**




Fuente: Bundeskriminalamt [Anm. 53]

Con respecto a este tema lamentablemente no existen estudios, pero teóricamente se puede especular. Una primera hipótesis sería que el aumento de incidencia en este crimen en mujeres, se debe a la gran participación de mujeres en el trabajo con equipos de informática. Sin embargo, es notorio, que en la mayoría de los casos llegados a conocer en el crimen por computadora, se trata de fraudes por medio de tarjetas obtenidas ilegalmente para uso en cajeros automáticos, por lo tanto la hipótesis es errónea.

Una segunda hipótesis sería que el aumento de los crímenes realizados por mujeres es un resultado del aumento del crimen por computadora en general. Por lo tanto se debe hacer el cuestionamiento, de ¿por qué la incidencia en este ámbito criminal es mayor en las mujeres que en los hombres?

Una tercera hipótesis sería, que el fraude por medio de tarjetas obtenidas ilícitamente para el uso en cajeros automáticos es un delito que se mueve mejor en el nuevo desarrollo económico que en el crimen, o sea, que la actual "sociedad sin efectivo" ofrece nuevas posibilidades y estas posibilidades se tienen a la mano. Se puede pensar por lo tanto, que para las mujeres todavía hay posibilidades de cometer este delito, ya que su participación en la "sociedad consumista" es mayor que antes. Como fue mencionado anteriormente, aquí no se pretende aclarar razones. Pero sería interesante, aunque no existan estadísticas al respecto, poder realizar por lo menos un estudio comparativo sobre el tema.

Por regla, un comportamiento humano no es definido sólo por un motivo, sino por un manojo de motivos[70]. El motivo del hecho, es frecuentemente el instinto al juego del delincuente, el cual (por el momento) sólo quiere probar si es más astuto y puede engañar las medidas de seguridad presentadas por la respectiva empresa (el llamado motivo-challenge)[71], aunque cuantitativamente dominan los delitos económicos[72].

Otros motivos son la venganza, el enriquecimiento o simplemente la respuesta del delincuente a la "inteligencia de la computadora", o sea, el desafío[73]. Con respecto a los llamados "Hacker" p.ej. se definió el motivo del hecho[74] como una simple distracción inteligente de los entusiastas electrónicos, los cuales intentan ingresar sin autorización a computadoras como un deporte relajante, para "ver lo que hay".

Con respecto al sabotaje por computadora se tienen otros motivos, p.ej. políticos, éticos o racistas[75]. Bandekow habla de: a) motivos económicos, p.ej. afán de lucro o necesidad económica real; b) motivos egocentristas, p.ej. ansia de notoriedad, vanidad, orgullo o ambición; c) motivos ajenos, p.ej. condicionante filantrópico, naturaleza servicial, lástima, motivos misantrópicos como p.ej. envidia, odio, venganza; y d) imprudencia y negligencia[76].

Estas características avaladas también por investigaciones americanas del "Stanford Research Institutes" no son casualidad, sino – por lo menos para finales de los años sesenta y principios de los setenta - que se encuentran en una gran cantidad de personas relacionadas con el campo de la informática. El origen para ello lo encontramos en el gran auge y propagación de la informática que apenas inició en los años sesenta. Las profesiones informáticas son por lo tanto profesiones relativamente

---

70 Bandekow, Klaus, *op. cit.,* p. 62, con referencias bibliográficas adicionales.

71 Cfr. Parker, Donn B., *op. cit*., p. 46 s.; Sieber, Ulrich, *op. cit*., p. 132, con referencias bibliográficas adicionales.

72 Göppinger, Hans, *op. cit*., p. 547; Möhrenschlager, Manfred, *op. cit*., p. 321 (322); cfr. Sieber, Ulrich, *op. cit*., p. 6.

73 Cfr. Bandekow, Klaus, *op. cit*., p. 62; Gutiérrez Francés, María Luz, op. cit., p. 76; González Rus, J.J., *op. cit*., p. 111.

74 Cfr. Kaiser, Günter, *op. cit*., § 74, Rn. 51.

75 Cfr. Council of Europe, op. cit. p. 43; Sieber, Ulrich, op. cit., p. 15 s; Wasik, Martin, *op. cit*., p. 6 s.

76 Bandekow, Klaus, *op. cit*., p. 64 s.

nuevas, las cuales son tomadas por personas jóvenes o personas flexibles y con poco arraigo con sus viejas profesiones[77].

Actualmente está claro, que los casos más peligrosos y más importantes que se llegaron a conocer, fueron realizados por delincuentes que trabajaban con programas de cómputo o con equipos de informática. Una gran cantidad de casos fueron originados por empleados de la empresa víctima[78], eran evidentemente mayores que un delincuente joven y con la mitad de su inteligencia[79]. En muchos casos no era realmente necesario el conocimiento informático para la realización del hecho[80]. Como delincuente del sabotaje por computadora se tenían p.ej. internos de la empresa, familiares de empresas competidoras y – sobre todo en el extranjero – personas motivadas políticamente[81].

Es importante mencionar, que los buenos conocimientos de la organización y de las medidas de seguridad internas de la empresa víctima son frecuentemente más importantes que los conocimientos informáticos para la realización de un delito por computadora[82]. Por el crecimiento en el uso de computadoras en casi todas las áreas de la vida de la sociedad actual, ha llegado el delincuente profesional del crimen por computadora a jugar un rol importante; la computadora ha sido utilizada también como una herramienta para el crimen organizado[83], y por lo tanto se debe tomar el crimen por computadora como un negocio real y no como un típico caso aislado[84].

### b) La víctima.

Hasta el año 1978 fueron las víctimas del crimen por computadora los bancos, las empresas aseguradoras, entidades públicas, la industria e

---

77 Así Sieber, Ulrich, *op. cit*., p. 131.

78 Cfr. Kaiser, Günter, *op. cit*., § 74, Rn. 48, 52; Romeo Casabona, Carlos María, Poder informático y seguridad jurídica, Madrid, 1988, p. 36 con referencias bibliográficas adicionales.

79 Cfr. Gutiérrez Francés, María Luz, *op. cit*., p. 74.

80 Cfr. Sieber, Ulrich, *op. cit*., p. 129 s.; Bandekow, Klaus, *op. cit*., p. 59.

81 Cfr. Kaiser, Günter, *op. cit*., § 74, Rn. 55.

82 Sieber, Ulrich, *op. cit.*, p. 130.

83 Cfr. Bequai, A., *Technocrimes. (The Computerization of Crime and Terrorism)*, Heath Lexington Books, Lexington, 1987, p. 61 s.

84 Sieber, Ulrich, *op. cit.*, p. 133.

instituciones educativas[85]. No sorprende que el primer caso de crimen por computadora que se descubrió en los U.S.A. se conociera con el título "Computer Expert Acussed of Fixing His Bank Balance"[86].

Los bancos en el extranjero han sido las mayores víctimas, especialmente cuando se refiere a la manipulación por computadora[87]; algunos afectados p.ej. también han sido computadoras médicas en Inglaterra o enajenación de información a los servicios secretos soviéticos de entonces[88], o entidades de telefonía[89].

Una característica es, que las víctimas del crimen por computadora, especialmente los bancos, temen consecuencias negativas en su reputación por la emergente publicidad[90].

Si se parte del punto que en casi todas las áreas mencionadas sólo se encuentran empresas, o sea firmas, entonces se debería de determinar fácilmente, que la víctima de un delito por computadora simplemente es una persona jurídica[91].

Normalmente no se trata de cualquier persona jurídica, sino de personas jurídicas que son reconocidas públicamente como lo son las grandes empresas, el delincuente – el delincuente no profesional –realiza el delito contra esta "gran y rica víctima" de forma fácil, o sea, que estos delincuentes no encuentran obstáculo moral alguno al realizar un delito en contra de esta empresa[92].

Frecuentemente se describe a la víctima de un delito por computadora como un "verdadero y más importante auxiliar del delincuente". La base

---

85 Cfr. Wasik, Martin, *op. cit.*, p. 65; González Rus, J.J., *op. cit.*, p. 109; Gutiérrez Francés, María Luz, *op. cit.*, p. 76.

86 Minneapolis Tribune for Tuesday, October 18, 1966, citado por Parker, Donn B., op. cit.; Parker, Donn B., op. cit., S. X Introduction.

87 Cfr. Sieber, Ulrich, *op. cit.*, p. 2/132, con referencias bibliográficas adicionales.

88 FAZ v. 14 y 16.2.1990; FAZ Nr. 66 v. 19.3.94

89 Cfr. Kaiser, Günter, *op. cit.*, § 74, Rn. 51.

90 Cfr. Tiedemann, Klaus, *op. cit.*, p. 27; también en: Tiedemann, Klaus/Cosson, Jean, *op. cit.*, p. 5; Sieber, Ulrich, *op. cit.*, p. 175 con referencias bibliográficas adicionales; comparando la situación en los U.S.A. por Wasik, Martin, op. cit., p. 65 s.; Fischer, Thomas, *op. cit.*, p. 12.

91 Sieber, Ulrich, *op. cit.*, p. 36 s.; Wasik, Martin, *op. cit.*, p. 6 s.

92 En sentido similar a Gutiérrez Francés, María Luz, *op. cit.*, p. 76.

para la realización de un delito por computadora es, en muchos casos, la falta de medidas de control y obstaculización, las cuales incrementan el costo, ya que la causa existencial de un centro de cómputo o de la automatización de trabajo es la posible reducción de costos.

Por otro lado existen frecuentemente en la historia del crimen por computadora, delitos que fueron posibilitados por la alta negligencia por parte de la víctima; en muchos casos por un error de un colaborador, de los programadores o por alguna persona del personal relacionada con el manejo del centro de informática, como lo es el personal de seguridad o de mantenimiento[93].

El que la víctima no denuncie un delito por computadora es, por lo tanto, una forma de colaboración con el delincuente, ya que ni la policía, ni la justicia tienen posibilidad de reducir la frecuencia de estos delitos debido a que las víctimas dejan el delito en la sombra –es decir, prefieren no denunciarlo. Aunque la víctima puede tener sus razones muy fundadas para no poner la denuncia, es obvio, que sólo por medio del reconocimiento y el estudio del crimen por computadora, sus apariciones y modus operandi se puedan desarrollar medidas adecuadas y sistemas para combatirlas.

### c) Los hechos.

Con respecto a los hechos, se han llegado a dividir los casos conocidos en cuatro grupos, a saber, las manipulaciones, el espionaje, el sabotaje y el hurto de tiempo[94]. La manipulación por computadora es la forma más frecuente del crimen por computadora[95]; es el área prioritaria del crimen por computadora[96].

---

93 Cfr. Sieber, Ulrich, *op. cit.*, p. 36 s.; Wasik, Martin, *op. cit*., p. 65 s. con referencias bibliográficas adicionales; Gutiérrez Francés, María Luz, *op. cit*., p. 76

94 Cfr. Tiedemann, Klaus, *op. cit.*, p. 150 s.; Poerting, Peter/Pott, Ernst G, op. cit., p. 27; Fischer, Thomas, *op. cit.*, p. 19 s., Sieber, Ulrich, *op. cit.*, p. 39 s.; todos con referencias bibliográficas adicionales.

95 Tiedemann, WM 1983, 1326 (1327); Sieber, BB 1982, 1433 (1433); Schmitz, Herbert/Schmitz, Detlef, *Computerkriminalität*, Wiesbaden, 1990, p. 25.

96 Tiedemann, Kaiser-FS, 1373 (1373) con referencias bibliográficas adicionales; Lampe, GA 1975, 1 (2); Kaiser, Günter, *op. cit*., § 74, Rn. 48 con referencias bibliográficas adicionales; United Nations, op. cit. § 63, p. 8.; Sieber, CR 2/1995, 100 (101).

Al mencionar el fraude por computadora se está haciendo referencia a una manipulación por computadora. Von zur Mühlen[97] diferencia las siguientes formas de manipulación por computadora: manipulación de programas, manipulación de ingresos, manipulación por acceso a la consola y manipulación del hardware.

Las manipulaciones se pueden referir tanto a la fase de ingreso de datos, de procesamiento de datos o de salida de datos informáticos[98]. La manipulación de inputs se refiere al ingreso de datos en la computadora. La manipulación de outputs corresponde a la salida de datos en la informática. Las alteraciones en la fase de procesamiento pueden describirse como manipulaciones del programa[99].

En la técnica de la informática se diferencia entre los dos componentes, el hardware y el software. Bajo hardware se entiende el equipamiento técnico para el procesamiento de datos, o sea, su unidad central con procesador, su unidad de control, su memoria principal, así como los aparatos periféricos para el ingreso, salida, memorización y diálogo. Bajo software se entiende la parte ideológica o intelectual de la computadora; pero aquí se debe hacer una diferenciación entre el software básico operativo de la computadora, en especial el software requerido para el funcionamiento de la unidad central, y el software de programación y utilización más problemático, que consiste de los llamados programas de cómputo . Las manipulaciones en el hardware, a las que pertenecen las partes técnicas de los equipos informáticos, casi no tienen significado, desde el punto de vista de la comisión del hecho punible[101].

Las intervenciones en la consola son los resultados de manejos ilícitos sobre el equipo de informática, o sea, que se encuentran en el mal manejo de la mecánica del equipo, y estas pueden ser de muy distintas maneras[102]. La característica de esta forma de manipulación por computadora se encuentra en la intervención mecánica sobre el hardware de la computadora posibilitando así la manipulación de datos[103].

---

97 Mühlen, Rainer A.H. *von zur,* op. cit., p. 18 s. y 45-107.
98 Tiedemann, Klaus, *op. cit*., p. 25.
99 Ibid., p. 148.
100 Sieber, Ulrich, *op. cit*., p. 11.
101 Ver Tiedemann, *op. cit*., 1326 (1327).
102 Cfr. Sieber, Ulrich, op. cit., p. 60 s. con referencias bibliográficas adicionales y ejemplos.
103 Schmitz, Herbert/Schmitz, Detlef, op. cit., p. 27

La peligrosidad de estas manipulaciones por computadora está en la complejidad técnica de estos equipos de informática; la manipulación de los datos difícilmente se logra aclarar y después de que se han determinado casi no se pueden comprobar[104].

Un tema importante relacionado con el crimen por computadora es el tema del lugar de los hechos. Se debería de pensar que en la mayoría de los casos de crimen por computadora que se llegaron a conocer, el lugar de los hechos era en la misma ubicación del equipo de cómputo. Pero hay que considerar la posibilidad de hacer una corrección en las estadísticas con respecto a una afirmación como esta, ya que los hechos y efectos de los delitos por computadora – muy diferente a los delitos clásicos patrimoniales – se desintegran regularmente, lo que juega un papel importante en el esclarecimiento del hecho[105].

También se puede pensar que una gran cantidad de delitos por computador son llevados a cabo en grandes ciudades, donde se encuentran ubicados la mayor parte de equipos de cómputo. Ambas afirmaciones son ciertas; pero sorprende que las estadísticas de los últimos años del siglo pasado en la República Federal de Alemania muestren claramente, que la repartición de los delitos por computadora es muy diferenciada e irregular entre las grandes y pequeñas ciudades y que las ubicaciones de los grandes equipos de cómputo (en grandes ciudades) no son un punto relevante.

Aunque la mayor cantidad de delitos descubiertos se ubicaban más en las grandes ciudades que en las pequeñas, esto con toda seguridad se relaciona más con la cantidad de habitantes – o sea, posibles delincuentes – que por la ubicación en sí. Además, la frecuencia absoluta es mayor en las ciudades pequeñas que en las grandes. El fenómeno[106] se describe de la siguiente forma:

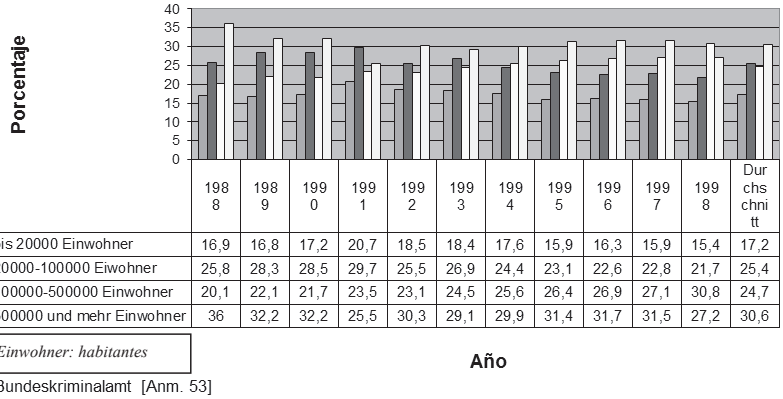
---

104 Ibid., p. 25.

105 Tiedemann, *op. cit*., 1326 (1327).

106 Bundeskriminalamt (Hg), Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, Bundeskriminalamt Wiesbaden, Berichtsjahr 1987-1998, resumen hecho por el autor.

**Repartición del lugar de los hechos en delitos por computadora**




| | 1988 | 1989 | 1990 | 1991 | 1992 | 1993 | 1994 | 1995 | 1996 | 1997 | 1998 | Durchschnitt |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| bis 20000 Einwohner | 16,9 | 16,8 | 17,2 | 20,7 | 18,5 | 18,4 | 17,6 | 15,9 | 16,3 | 15,9 | 15,4 | 17,2 |
| 20000-100000 Eiwohner | 25,8 | 28,3 | 28,5 | 29,7 | 25,5 | 26,9 | 24,4 | 23,1 | 22,6 | 22,8 | 21,7 | 25,4 |
| 100000-500000 Einwohner | 20,1 | 22,1 | 21,7 | 23,5 | 23,1 | 24,5 | 25,6 | 26,4 | 26,9 | 27,1 | 30,8 | 24,7 |
| 500000 und mehr Einwohner | 36 | 32,2 | 32,2 | 25,5 | 30,3 | 29,1 | 29,9 | 31,4 | 31,7 | 31,5 | 27,2 | 30,6 |

Fuente: Bundeskriminalamt [Anm. 53]

Ya que en la mayoría de los casos de crimen por computadora esclarecidos se trataba de fraude por medio de tarjetas obtenidas ilegalmente para cajeros automáticos, se sobreentiende, que la repartición del crimen por computadora se da por frecuencia de los cajeros automáticos, que conlleva a más posibilidades para un delito. La razón por la cual se obtiene una frecuencia absoluta en las pequeñas ciudades sigue sin aclararse.

## Conclusión.

Al llegar a este punto se plantea la interrogante de si se pueden emitir o no conclusiones definitivas. Es claro, que habrá comprendido el lector, que el presente es un aporte parcial de un análisis mucho más grande y elaborado. No obstante, tal y como adelanté en la introducción, las bases científicas de los distintos puntos tratados y abordados, permiten sacar conclusiones al lector (a) sobre aspectos considerados tabúes sobre la delincuencia informática. Incluso en la actualidad, en donde la proliferación de aparatos electrónicos como computadoras, tablets, teléfonos inteligentes, reproductores de música con acceso a internet, videoconsolas con acceso a internet, incluso televisores con acceso a internet, por citar algunos ejemplos; así como proliferación de distintas plataformas de comunicación como servicios de mensajería, redes sociales y un larguísimo etcétera; hace que el tema del delito por computadora vuelva a estar sobre el tapete, ya no solo como una forma delictiva especial, sino y aquí un adelanto, como una forma delictiva convencional, que requiere para un adecuado tratamiento,

de un abordaje muy distinto al que hasta ahora se le ha dado. Espero poder publicar otras partes de mi estudio, que permitan desarrollar una teoría acerca de un posible tratamiento de esta forma de delito, todavía hoy no comprendida de una manera satisfactoria según mi leal saber y entender.

## Bibliografía.

### Lehrbücher[107]

Göppinger, Hans, Kriminologie, 5. Auflage, München, 1997.

Kaiser, Günther, Kriminologie, 3. Aufl., Heidelberg, 1996.

### Monographien[108]

AHL, D.H. „Employee Computer Crime on the Rise“, Creative Computing, Band 11, Juni, 1985.

Baker, Jay J., The Investigation of computer crime. An Operational Guide to White Collar Crime Enforcement, National Center for Computer Crime Data Head, Antitrust Section, Los Angeles Country District Attorney´s Office, California, ohne Datum.

Bandekow, Klaus, Strafbarer Missbrauch des elektronischen Zahlungsverkehrs. Zur Strafbarkeit der missbräuchlichen Inanspruchnahme von Geldausgabeautomaten, Chip-Karten-Systemen und Bildschrirmtext-Leistungen unter Berücksichtigung von Kriminologie und Kriminalistik, Diss., Lübeck, 1988.

Bequai, A. Computer Crime, Lexington, 1978.

Chinchilla Sandí, Carlos, Delitos Informáticos, Elementos básicos para identificarlos y su aplicación, San José, Costa Rica, Ediciones Farben, 2004.

Davara Rodríguez, M.A., Manual de Derecho Informático, Editorial Aranzadi, Madrid, 1997.

Dinardo, C.T., Computer crime, in: The Information Technology Series, Computes and Security, Volume III, New Jersey, 1978.

---

107 Tratados.

108 Monografías o libros de texto.

Fischer, Thomas, Computer-Kriminalität, Gefahren und Abwehrmaßnahmen, Bern, 1979.

Gutiérrez Francés, María Luz, Fraude Informático y Estafa, Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones, Madrid, 1991.

Hentig, Hans von, Zur Psychologie der Einzeldelikte, Band 1: Diebstahl, Einbruch, Raub, Tübingen, Mohr, 1954.

Hofmann, Rolf, Unterschlagungsprophylaxe und Unterschlagungsprüfung, Berlin, 1997.

Meier, O, Dunkelziffer oder Dunkelfeld, Bonn, Diss., 1956.

Mühlen, Rainer A.H. von zur, Computer-Kriminalität. Gefahren und Abwehr. Neuwied/ Berlin, 1973.

Norman, Adrian R.D., Computer insecurity, London/New York, 1983.

Parker, Donn B./Nacum, Susan/Aura, S. Stephen, (Hrsg.), Computer Abuse vom Stanford Research Institute, 1973.

Parker, Donn B., Crime by Computer, New York, 1. Aufl, 1976.

Poerting, Peter/Pott, Ernst G, Computerkriminalität, Bundeskriminalamt, Wiesbaden, 1986.

Romeo Casabona, Carlos María, Poder informático y seguridad jurídica, Madrid, 1988.

Schlüchter, Ellen, Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, Kommentar mit einer kriminologischen Einführung, Heidelberg, 1987.

Sieber, Ulrich, Computerkriminalität und Strafrecht, 2., um einen Nachtrag ergänzte Auflage, Köln, Berlin, Bonn, München, 1980.

Sieber, Ulrich, Informationstechnologie und Strafrechtsreform. Zur Reiche des künftigen Zweiten Gesetzes zur Bekämpfung der Wirtschafskriminalität, Köln, Berlin, Bonn, München, 1985.

Schmitz, Herbert/Schmitz, Detlef, Computerkriminalität, Wiesbaden, 1990.

Sondermann, Markus, Computerkriminalität, Die neuen Tatbestände der Datenveränderung gem. § 303 a StGB und der Computersabotage gem. § 303 b. StGB, Diss., Münster, 1989.

Soyka Joachim, Tatwaffe Computer, Datenmanipulation, Softwarediebstahl, EDV-Spionage, München, 1988.

Tiedemann, Klaus/Cosson, Jean, Straftaten und Strafrecht im deutschen und französischen Bank- und Kreditwesen, Köln/Berlin/Bonn/München, 1973.

Tiedemann, Klaus, Wirtschaftstrafrecht und Wirtschaftskriminalität II, Besonderer Teil, Hamburg, Rowohlt, 1976.

Wasik, Martin, Crime and the Computer, Oxford, 1991.

Zimmerli, Erwin/Liebl, Karlhans, Computermissbrauch, Computersicherheit, Fälle-Abwehr-Aufdeckung, 1. Aufl., Ingelheim: Hohl, 1984.

**Aufsätze**[109]

González Rus, J.J., Aproximación al tratamiento penal de los ilícitos patrimoniales realcionados con medios o procedimientos informáticos, Revista de la Facultad de Derecho de la Universidad Complutense de Madrid, N° 12, Monográfico sobre Informática y Derecho, 1986.

Kolz, Harald, Zur Aktualität der Bekämpfung der Wirtschaftskriminalität für die Wirtschaft, wistra 1982, p. 167-172.

Möhrenschlager, Manfred, Computerstraftaten und ihre Bekämpfung in der Bundesrepublik Deutschland, wistra 1991, p. 321-331.

Möhrenschlager, Manfred, Das neue Computerstrafrecht, wistra 1986, p. 128-142.

Möhrenschlager, Manfred, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), wistra 1986, p. 123-127.

Salazar Rodríguez, Alonso, La Sexta Ley de Reforma del Código Penal de la República Federal de Alemania, en Cuadernos de Doctrina y Jurisprudencia

109 Artículos de revista y/o académicos.

Penal, Argentina, Año V, Número 8 C, p. 1117-1132, y en RdPP (Revista de Derecho Penal y Procesal Penal), España, núm. 3, 2000 p. 233-236, en Revista de Ciencias Jurídicas, Universidad de Costa Rica - Colegio de Abogados de Costa Rica, Número 93, Setiembre - Diciembre 2000, p. 57 sgtes.

Sieber, Ulrich, Informationsrecht und Recht der Informationstechnik, NJW 1989, p. 2569-2580.

Sieg, Rainer, Strafrechtlicher Schutz gegen Computerkriminalität, Jura 1986, p. 352-363.

Steinke, Wolfgang, Die Kriminalität durch Beeinflussung von Rechnerabläufen, NJW 1975, p. 1867-1869, NStZ 1984, p. 295-297.

Taber, John K, A Survey of Computer Crime Studies, in: Computer/Law Journal, Vol. II, 1980, p. 275-327.

Tiedemann, Klaus, Computerkriminalität und deutsche Strafrechtsänderung von 1986, Publications de la Section Hellenique de la Société Internationale de Défense Sociale, 1988.

### Sonstiges Material[110]

Council of Europe, Computer-related Crime, 1990, Recommendation No. R (89), Strasbourg, 1990.

United Nations Manual on the prevention and control of computer-related crime, United Nations, New York, 1994, in: International Review of Criminal Policy, Nos. 43 and 44, 1994.

110 Otro material utilizado.