Revista Digital de Ciencias Penales de Costa Rica, número 1 (32) (13). Homenaje al Prof. Dr. Daniel González Álvarez. Año 1. ISSN **pendiente**. RDCP-UCR. 2021.
https://revistas.ucr.ac.cr/index.php/RDMCP

SOBRE LA "POLUCIÓN" DEL DELITO INFORMÁTICO

ON THE "POLLUTION" OF THE INFORMATION TECHNOLOGY CRIME

Luis Alonso Salazar Rodríguez[1]

Amicus optima vitae possessio.

Los dioses no nos revelaron, desde el principio todas las cosas a los humanos; pero en el curso del tiempo, podemos aprender indagando, y conocer mejor las cosas. Por lo que respecta a la verdad certera, nadie la conoce, ni la conocerá; ni acerca de los dioses, ni tampoco de todas las cosas de las que hablo. E incluso si por azar alguien llegase a expresar la verdad perfecta, lo desconocería: pues todo no es más que una tela tejida de conjeturas[2].

Aún contando con el casi inevitable riesgo del personalismo, presentamos este texto a otros autores para que ellos lo despersonalicen y obtengan así teorías objetivas a partir de nuestras experiencias subjetivas[3].

Sumario.

1) Excurso: de Daniel González Álvarez.

[1] Prof. Catedrático de Derecho Penal y Procesal Penal. Universidad de Costa Rica.
[2] JENÓFANES (hacia el año 500 A.C.) citado por POPPER, K. En busca de un mundo mejor. Ediciones Paidós Iberoamérica. Barcelona. Buenos Aires. México, 1994, p. 17 quien señala que lo que denominamos conocimiento no es más que conjetura y opinión -doxa en vez de epistme.
[3] FRANKL, V. El hombre en busca de sentido. Editorial Herder. Barcelona. 1979. p. 33.

2) Planteamiento del problema.

3) Delito informático y autoría mediata.

   a) Delito informático.

   b) Autoría mediata.

4) La "*polución"* del delito informático.

5) Conclusión.

6) Comentario final.

7) Bibliografía.

1) Excurso: De Daniel González Álvarez.

Al Prof. Dr. Daniel González Álvarez, don Daniel, como le llamamos todos aquellos quienes le respetemos y reconocemos sus excelentes calidades humanas y profesionales, le conocimos en el año 1994. Fue nuestro profesor en el curso denominado "El recurso de casación" del programa del Post grado en Derecho Penal de la Universidad de Costa Rica, que en aquel entonces era una Especialidad Académica, base de lo que es hoy la Maestría en Ciencias Penales de esa casa de estudios superiores.

A lo largo de ese año académico (1994), don Daniel cultivó con nosotros una linda relación profesor-alumno, pues en nuestro caso particular investigaba la jurisprudencia de la Sala que él presidía y a menudo apostillábamos detalles de lo resuelto por la Sala de Casación durante las clases.

Justamente, casi al finalizar el curso lectivo, don Daniel fue primero lector y luego miembro del Tribunal examinador de nuestra tesis de licenciatura en derecho penal que fue precisamente un análisis jurisprudencial sobre recurso de casación por el fondo. El tema nos vinculó intelectualmente, porque en esa época don Daniel, no solo era el Presidente de la Sala Tercera de la Corte Suprema de Justicia como ya lo dijimos, sino que se puede decir sin reserva, él era Buque Insignia de la revolucionaria jurisprudencia que desarrollaba la Sala en torno al tema de la casación, principalmente dando contenido

a dos estandartes que en la época permearon las reglas de la materia impugnaticia en ese alto Tribunal: la justicia en el caso concreto y el principio de tutela judicial efectiva.

De los dos principios antes indicados, se derivaron una serie de reglas que le dieron al recurso de casación una nueva visión como lo fueron la des formalización del recurso, la admisibilidad de prueba en casación, el conocimiento de la violación de las reglas de la sana crítica racional como parte del recurso de casación por la forma, -cosa en la que nunca estuvimos de acuerdo porque siempre consideramos que eso es más un vicio de fondo que de forma-; y privilegiar el conocimiento y resolución del caso antes que el juicio de reenvío (darle a la casación efectos renovadores antes que contralores)[4].

Lo expuesto ut supra, se escribe rápido, en un solo párrafo, incluso, para un lector no avezado en el tema podría pasar hasta inadvertido, pero llegar a esa evolución costó aproximadamente 17 años de vigencia del Código de Procedimientos Penales, cientos de sentencias y otro tanto de personas juzgadas en nuestro país, grandísimas injusticias cometidas, yerros judiciales y por supuesto, una generación de magistrados y una magistrada (Dora Guzmán Zanetti quien en 1984 sustituyó a Don Ulises Valverde Solano y se integró a la Sala Tercera y fue la primera mujer miembro de la Corte Suprema de Justicia), que quisieron tomar el "toro por los cuernos" y cambiar poco a poco del rigor de la admisibilidad y el formalismo reinante a una visión más humana de la justicia penal.

Don Daniel se retiró como Presidente de la Sala el 1 de enero del año 2005, fue sustituido por Magda Lorena Pereira Villalobos, y para quienes nos hemos dedicado por años a la justicia penal, seguimos echando de menos a Don Daniel, en nuestra opinión se fue muy pronto, tenía mucho que dar aún, sin embargo; hay que reconocer que cada quien tiene derecho a decidir sobre su vida personal y profesional, y en nuestro caso, lo que queda es agradecer sus enseñanzas y tratar de seguir sus pasos.

[4] Para ampliar sobre el tema puede verse SALAZAR. A. Una nueva visión del Recurso de Casación penal por el fondo en Ciencias Penales. Revista de la Asociación de Ciencias Penales de Costa Rica, Año 12, N° 17, Marzo 2000, p. 55-82. reproducido con ampliaciones y bajo el título Una nueva visión del recurso de casación por el fondo en el derecho procesal penal costarricense, en CDJP (Casación), Nº 1 (2001).

Este homenaje llega a Don Daniel nos parece que un poco tarde, pero es más que merecido, nosotros en lo personal ya le habíamos hecho un guiño por allí[5], pero no es lo mismo que un reconocimiento individual que uno colectivo.

Don Daniel, esperamos que estas breves notas sean de su agrado, hemos seleccionado el tema por diversos motivos, pero el principal, porque como uno de sus exalumnos, quisiéramos en este libro homenaje, dejar plasmada una pequeña tesis, que esperamos sea tomada como el mejor tributo que un alumno puede hacer a uno de sus maestros.

Siempre guardamos en la memoria, los hermosos días que compartimos y disfrutamos del placer de ser su "lazarillo" en Friburgo de Brisgovia, en la República Federal de Alemania, cuando Costa Rica tuvo el honor de ser representado por usted, en la conferencia internacional organizada por el Max-Planck Institut für Auländisches und Interantionales Strafrechts, en el año 1998 con ocasión de la suscripción del Estatuto de Roma, que estableció la Corte Penal Internacional, allí tuvimos oportunidad de conocer a la persona de don Daniel González Álvarez más de cerca y saber la calidad humana de quien para nuestro gusto ha sido una de las cabezas más brillantes que ha pasado por la Corte Suprema de Justicia de Costa Rica en toda su historia.

2) Planteamiento del problema.

Uno de los grandes desafíos del derecho penal, es brindar soluciones adecuadas en tiempo y espacio, a los problemas que enfrenta determinada sociedad, con relación a la reacción del Estado frente a lo que se ha llegado a denominar como conductas desviadas [lo anterior, dicho en un lenguaje sencillo y llano pues por razones de espacio resulta imposible extenderse en grandes constructos teoréticos al respecto]; tarea no siempre fácil y que se ve afectada por una serie de factores en su mayoría externos, que desde luego, influyen la manera en como se percibe el sistema penal.

[5] Ver SALAZAR, A. Pespectiva criminológica del crimen por computadora en Revista de Ciencias Jurídicas, Universidad de Costa Rica - Colegio de Abogados de Costa Rica, Número 149, Mayo- Agosto, 2019, p. 133-166.

En su cuarta acepción, el diccionario de la Real Academia de la Lengua Española define "polución" en sentido moral, como "corrupción, profanación" y es en ese sentido en que lo emplearemos en este texto. Se trata entonces de entender, que en ocasiones el derecho penal es corrompido [entendido como un vicio o abuso de las cosas no materiales] o profanado [entendido como deslucir, desdorar, deshonrar, prostituir, hacer uso indigno de cosas respetables].

Así las cosas, entendemos aquí, que con respecto al denominado "delito informático", existe en nuestro derecho una "polución" que indefectiblemente nos lleva por el camino equivocado y que debemos rectificar cuanto antes.

3) Delito informático[6] y autoría mediata.

a) Delito informático.

Como ya se ha indicado ut supra, por limitaciones de espacio, no resulta posible extenderse en demasía en el desarrollo doctrinario en torno a estos dos supuestos teóricos, que encuentran en la literatura especializa un sinfín de textos que pueden servir de orientación al lector, no obstante; a manera de definición de tipo estipulativa, y con el propósito de que sirvan de base para un entendimiento de la tesis planteada, trataremos de hacer una brevísima presentación al respecto.

Desde hace muchos años[7], se habla de la necesidad de regular algunas conductas que hasta el momento permanecen impunes, conductas que se vinculan de una u otra forma con el abuso, la destrucción, variación, modificación o utilización fraudulenta de

[6] Para ampliar sobre le tema ver SALAZAR, A. Delito Informático (Análisis comparativo con el delito de daños y otros tipos del Código Penal costarricense), en Revista de Ciencias Jurídicas, Universidad de Costa Rica - Colegio de Abogados de Costa Rica, Número 88, Setiembre - Diciembre 1998, p. 63 sgtes, y Cuadernos de Doctrina y Jurisprudencia Penal, Argentina, Año V, Número 9 A, p. 709-727. En el sistema jurídico costarricense, no se puede hablar del delito informático **en sentido estricto**, pues la legislación penal costarricense adolece de normativa en este campo. Igual situación se presenta en otros sistemas jurídicos, como por ejemplo el español. No obstante, se utiliza la terminología „delito informático" simplemente por conveniencia, pues casualmente uno de los objetivos del presente artículo es precisamente hacer conciencia de la necesidad de regularlo. Al respecto y en relación con el estado de la situación en España, se recomienda la lectura de la obra de Miguel Angel Davara Rodríguez, Manual de Derecho Informático, Aranzandi Editorial, 1997.

[7] Cfr. SALAZAR, A./GUERRERO, E. Comentario críticos a a la reforma del Código Penal que introduce la ley 9048 (Sobre los delitos informáticos en el derecho penal costarricense) localizable en: https://escuelajudicialpj.poder-judicial.go.cr/images/DocsRevista/revistajudicial112.pdf

programas o paquetes de cómputo (Software) o bien bases de datos, cuya información se encuentra protegida por leyes especiales o simplemente su acceso es restringido, sea por razones de privacidad, protección de los derechos individuales (habeas data), o que por cualquier otro motivo, como por ejemplo, fines comerciales, se desea proteger[8]. Los tipos penales tradicionales resultan inadecuados para encuadrar las nuevas formas delictivas[9], la tecnología avanza a pasos agigantados, mientras las leyes penales se estancan y no dan respuesta a las nuevas formas de criminalidad que con ocasión de la utilización de los avances tecnológicos del mundo moderno, se encuentran a disposición de criminales que se sirven de ellas. Estas formas de criminalidad por lo general tienen un carácter transfronterizo, por lo que el Comité de Ministros del Consejo de Europa, ha recomendado la armonización de manera intensa, tanto de la legislación como de la práctica en todos los países miembros, con el propósito de poder dar una respuesta adecuada al problema[10].

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

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

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

Como ya lo hemos expuesto en otro lugar[11], la pregunta que surge en este momento es: ¿ha sido el problema correctamente entendido?

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

El 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[12]), más recientemente, la Ley sobre Delitos Informáticos del año 2012 (Ley 9048).

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[13].

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[14]. 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

[11] SALAZAR, A. El delito informático (Análisis comparativo con el delito de daños y otros tipos del código penal costarricense) en Revista de Ciencias Jurídicas, Universidad de Costa Rica - Colegio de Abogados de Costa Rica, Número 88, Setiembre - Diciembre 1998, p. 63 sgtes

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

[13] Para ampliar al respecto ver SALAZAR, A. Op. Cit., Perspectiva...

[14] TIEDEMAN, K.; COSSON, J., Straftaten und Strafrecht im deutschen und französischen Bank- und Kreditwesen, Köln/Berlin/Bonn/München, 1973, p. 25.

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[15].

b) Autoría mediata.

El derecho penal costarricense, conoce del instituto de la autoría mediata desde la promulgación del código penal de 1970, en ese sentido, el artículo 45 del Código Penal señala:

> *Artículo 45.- Es autor del hecho punible tipificado como tal, quien lo realizare por sí o sirviéndose de otro u otros, y coautores los que lo realizaren conjuntamente con el autor.*

Curiosamente, según lo relata el Prof. Dr. Dr. Francisco Castillo González, llama la atención que la norma encuentra su antecedente en el Código Penal alemán, en su artículo 25, que señala:

Versión en alemán:

> *§ 25 Täterschaft (1) Als Täter wird bestraft, wer die Straftat selbst oder durch einen anderen begeht.*

Versión en español:

> *§ 25. Autoría (1) Se castiga como autor a quien cometa el hecho punible por si mismo o a través de otro.*

El tema aquí, es que el Código Penal alemán, conoció de la versión de la norma transcrita, hasta la reforma de la parte general del código, que entró en vigor en el año 1975, que es la Primera Ley de reforma del Código Penal alemán:

> *"La reforma del Código Penal alemán representa, según ha manifestado el ministro federal de justicia, profesor Horst Ehlnke, en una conferencia de prensa celebrada en Bonn el 18 de agosto de 1969 (1), un replantarniento científico del Derecho punitivo con una orientación*

[15] Para ampliar sobre estos conceptos ver SALAZAR, A. Op. Cit. Perspectiva…

político-criminal humanitaria y resocializadora, que deja en segundo plano la tradicional misión retributiva"[16].

Como ya lo hemos expuesto, resulta imposible en pocas líneas hacer un análisis y/o estudio sobre la autoría mediata como instituto jurídico del derecho penal, a manera de síntesis podemos afirmar, que se echa mano de ella para sancionar la comisión de conductas punibles cuanto quien tiene el dominio funcional del hecho es una persona que no entra en contacto directo con la cadena causal, por decirlo de una forma simple[17].

Cuando hablamos entonces de autoría mediata, hacemos referencia a aquellas hipótesis delictivas en las que el autor del hecho punible no es quien [en apariencia] se vislumbra como tal, sino que se habla de la existencia de un autor que figura "detrás del autor", quien se vale de aquel y lo utiliza como "instrumento" para comisión del delito [se habla de instrumentos que actúan conforme a derecho, de instrumentos que actúan en forma culposa, de instrumentos que actúan sometidos a error e incluso, una tesis minoritaria y bastante discutida admite la posibilidad de un instrumento que actúa en forma dolosa][18].

De lo expuesto, lo que resulta destacable para efectos de esta exposición, es el hecho de que por una razón bastante ilógica [según nuestro leal saber y entender], en los casos en los que los tipos penales existentes no alcanzan a sancionar conductas punibles o supuestos denominados "novedosos" como es el caso de los así entendidos, "delitos informáticos", el constructo teórico recurre a la creación de "nuevos y en muchos casos, alambicados, tipos penales" para poder alcanzar esos supuestos con el brazo punitivo de la ley, mientras que en los supuestos en los que "intervienen sujetos como partícipes de la comisión de un hecho punible, pero su intervención no se aprecia con un dominio

[16] Citado por BERISTAIN, A. La reforma del código penal alemán en Anuario de Derecho penal y Ciencias penales, 1969, p. 371, tonado de: Dialnet-LaReformaDelCodigoPenalAleman-2784688.pdf

[17] Entre tantas obras escritas al respecto, sobresale sin duda el trabajo de ROXIN, C. denominado en alemán Täterschaft und Tatherrschaft (Autoría y dominio del hecho en español) en caulesquiera de sus múltiples ediciones.

[18] Para ampliar sobre el tema y con amplias referencias bibliográficas ver CASTILLO, F. Autoría Mediata; Autoría y Participación; y en su tratado de derecho penal, pues en todas estas obras aborda el tema de una manera adecuada, profunda y con referencias bibliográficas adiconales tanto en español como en alemán.

funcional del hecho, la teoría recurre a la instrumentalización -por llamarlo de alguna manera-; del sujeto, equiparándolo a un objeto, o sea, a la teoría de la autoría mediata.

Dicho de una forma más llana: la teoría recurre a nuevos tipos penales cuando hay un objeto de por medio que sirve como instrumento de comisión [la computadora] de un hecho típico y recurre a una ficción legal [autoría mediata] cuando existe un sujeto [al cual considera instrumento] de por medio, pero lo equipara al sujeto con un instrumento [por no tener dominio funcional del hecho]. Esto es algo así como al decir de nuestros abuelos y el saber popular: "colocar la carreta delante de los caballos".

4) La *"polución"* del delito informático.

En fechas recientes, hemos visto como pululan las noticias sobre fraudes informáticos y sobre nuevas modalidades de estafa por medios telemáticos y electrónicos. Se ha discutido una vez y otra también, sobre la necesidad de hacer algo al respecto, sobre el bloqueo de señal de telefonía celular desde los centros penitenciarios, sobre la necesidad de que la población extreme medidas para no ser víctima de grupos organizados que se dedican a estas modalidades delictivas, y un largo etcétera.

No hace mucho en tiempo se introdujo una reforma del Código Penal que fue la Ley 9048, del 10 de julio del año 2012 (Sobre Delitos Informáticos), que pretendió ser la panacea a los múltiples problemas que en torno a la Ciberdelincuencia se presentan en nuestra realidad forense, pero como ya se había anticipado[19], se quedó muy lejos de alcanzar sus objetivos manifiestos y fueron más los problemas que creó desde el punto de vista dogmático, que los que solucionó. Se dijo en su oportunidad:

> *"Ya se perciben una serie de concepciones erróneas en cuanto a la determinación de las acciones que configuran un "delito informático", favoreciéndose con ello el aumento en la creación de tipos penales innecesarios, así como la aparición de problemas de orden técnico-jurídico que merece la pena destacar".*

[19] Ver SALAZAR, A/GUERRERO, E. Op. Cit., Comentarios críticos…

En la doctrina –básicamente internacional, aún y cuando hay algunos trabajos de orden costarricense al respecto-, no existe un acuerdo en cuanto al concepto de delito informático[20]. Es con base en lo anterior, que precisar una definición absoluta sobre el delito informático[21] resulta ser una tarea pretensiosa y se escapa de nuestro objeto, preferimos citar algunas que simplemente faciliten al lector la comprensión del tema central de este escrito.

> *"podemos definir el delito informático como: acción delictiva que realiza una persona, con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de máquinas- hardware- o de los programas- software" (Davara Rodríguez, 1993, citado en CHINCHILLA. C.*

[20] Téngase en consideración que en la dogmática se tomó primero el concepto „crimen por computadora "como tal hecho delictivo en el cual el instrumento u objetivo del hecho es la computadora. SIEBER completó este concepto en forma importante con el concepto de „lesión patrimonial dolosa en el ámbito de la informática". De acuerdo con este concepto, el crimen por computadora contempla todas las lesiones patrimoniales dolosas que estén vinculadas de alguna forma con los datos almacenados en equipos de procesamiento de datos; y como modalidades delictivas se toman en consideración la manipulación de datos (ingreso de datos erróneos, cambio en los datos), el uso ilícito de equipos procesadores de datos (hurto de tiempo o de uso), así como la destrucción de datos (sabotaje de computadora). Esta limitación del crimen por computadora a la violación patrimonial fue criticada por LAMPE, ya que diferentes casos conocidos no tuvieron relación alguna con intereses patrimoniales, sino que la violación se dio en relación con otros bienes jurídicos. Desde 1974 se habla de tener que cambiar el concepto „crimen por computadora "a „abuso por computadora", ya que el concepto es lingüísticamente incorrecto, discrimina el procesamiento de datos y solo sirve para efectos clasificatorios y de recopilación de casos. La computadora por si sola no puede ser criminal. Este concepto fue aceptado por SIEBER y por los nuevos desarrollos en el ámbito de este tipo de criminalidad. Así, SALAZAR, A. (Salazar Rodríguez, Delito informático…) citando a Bundesministerium der Justiz, LAMPE, SIEBER, LINDEMANN citado por SIEBER y FISCHER. Para nuestros efectos, pese a las consideraciones supra indicadas, nos referiremos al término de delito informático pues ha de parecernos, en su consideración semántica, el que puede abarcar en mayor parte la cantidad de acciones delictivas que se pretenden penalizar mediante el tipo penal.

[21] A modo de aporte al estudio, cabe destacar que antes de 1960 el concepto de „crimen por computadora "(luego delito informático) casi no se trataba en la dogmática del derecho penal. Al inicio de las discusiones sobre el problema del crimen por computadora por ejemplo en Alemania se cuestionaba, si realmente un crimen como éste existía. Las discusiones sobre el abuso de las computadoras inician en la mayoría de los países en los años 60 con referencia al peligro de los derechos de la personalidad, el cual se define inicialmente en el rubro de la protección de datos, y no bajo el rubro de „crimen por computadora ". En los años 70 el interés aumentó y el crimen por computadora se definió como una nueva forma de criminalidad; en ese entonces se concentraba la ciencia jurídica dentro de los delitos económicos específicos de computadora, p.ej. manipulación por computadora, sabotaje por computadora, hacking por computadora, espionaje por computadora y robo de software. Actualmente el estado de la situación es totalmente diferente. Análisis empíricos no sólo en la República Federal de Alemania, sino también de Australia, Gran Bretaña, Japón, los Países Bajos, Austria, Suiza, Suecia, los Estados Unidos y una investigación de la Comunidad Europea, han ido demostrando la realidad de esta nueva forma de delito. El crimen por computadora aparece como un crimen que requiere de un tratamiento específico. Así SALAZAR, A., Ob. Cit., El delito informático… En las líneas mencionadas se citan autores como TIEDEMANN, SIEBER, MÖHRENSCHAGER, Council of Europe y Passim.

Delitos Informáticos. Elementos básicos para identificarlos y su aplicación, 2004 (Chinchilla Sandí, Delitos Informáticos. Elementos básicos para identificarlos y su aplicación, 2004). "[delito informático es] la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software" DAVARA RODRIGUEZ, 1997. (Davara Rodríguez, 1997)

"cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos" (Organización de para la Cooperación Económica y el Desarrollo citada en" DAVARA RODRIGUEZ, 1997. (Davara Rodríguez, 1997)

"El concepto de abuso por computadora abarca comportamientos ilícitos, éticamente reprochables o prohibidos, en los cuales los datos informáticos son alterados dolosamente, tanto en el procesamiento como en la transmisión de datos. Bajo alteración de datos se entiende el cambio doloso de los mismos (manipulación por computadora), destrucción (sabotaje por computadora), su obtención y uso no autorizados (espionaje por computadora) y conjuntamente el uso no autorizado de equipos de cómputo (hurto de tiempo)" SALAZAR, A, Op. Cit. Delito informático…

De esta manera en un conjugado de todas estas definiciones se tiene que, el delito informático necesariamente se constituye por una acción que es ilícita, delictiva, no autorizada, ni ética cuya comisión recae en dos posibilidades:

(1) La primera, en la comisión de la acción ilícita se utiliza un medio informático, y

(2) La segunda, producto de la comisión de la acción ilícita se afecta o produce un daño sobre dicho medio informático.[22]

[22]CHINCHILLA, C., Op. Cit. Delitos informáticos… , citando a Alfredo Sneyers (1990) expone que se incluye dentro de la consideración de medio informático, los ordenadores (computadoras), miniordenadores, microrordenadores, equipos de tratamiento de textos, redes de telecomunicaciones y otros equipos informáticos, software, ficheros de datos y bases de datos.

Ahora bien, también están quienes consideran la configuración del delito informático desde (1) la perspectiva de la *computadora como objeto del hecho* y (2) la *computadora como recurso para el hecho*. Por un lado, se menciona la computadora como objeto del hecho, cuando el delincuente tiene como meta del delito a la computadora, o sea, la intervención del delincuente es específicamente contra la computadora (p.ej. espionaje, sabotaje, daño de bienes, daño de datos). Por otro lado, se menciona la computadora como recurso para un hecho, cuando el delincuente utiliza la computadora como recurso de intervención contra un bien jurídico protegido (p.ej. fraude por computadora)[23]. Pero es imperativo aclarar esta diferencia, ya que no todos los hechos en los cuales se utiliza una computadora, deben tomarse como crimen por computadora.

De esta forma, la identificación de ambas posibilidades nos conecta simultáneamente con la perspectiva del *delito informático como medio y como fin*. Esta es precisamente la clasificación de los delitos informáticos que propone Téllez Valdés, misma que es expuesta por CHINCHILLA SANDÍ (Chinchilla Sandí, Op. Cit. Delito informático…) así:

- *Delitos informáticos como instrumento o medio*: los cuales se refieren a aquellas conductas criminales que se valen de las computadoras como método, medio o símbolo en la realización del ilícito.
    - En nuestra consideración esto se referiría a la comisión de la acción delictiva por medio del simple "USO DEL ORDENADOR".
- *Delitos informáticos como fin u objetivo*: los cuales se refieren a las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física, o bien el sujeto o autor del ilícito obtienen un beneficio perjudicando a un tercero[24].

[23]SALAZAR. A. Op. Cit. El delito informático … citando a KAISER.
[24]El subrayado y la cursiva son suplidos

- En nuestra consideración esto se referiría a la comisión de una acción delictiva que produce una "LESIÓN EN EL ORDENADOR"

En relación, agrega DAVARA RODRÍGUEZ, Op. Cit.:

"[p]ara poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática, y el fin que se persiga deber ser la producción de un beneficio al sujeto o autor del ilícito: una finalidad deseada que causa un perjuicio a otro, a un tercero"

Respecto a dicha clasificación hemos de plasmar nuestra posición. Somos partidarios de la configuración de un delito informático únicamente en cuanto al fin, pues es nuestro considerar que el elemento o medio informático utilizado no debe ser el factor determinante para que una conducta ilícita se configure como un delito informático [a esto es a lo que llamamos aquí polución del delito informático]. Esto no quiere decir que no se puedan configurar otras figuras delictivas, empero no susceptibles de ser consideradas "delitos informáticos".

Nos explicamos con un ejemplo sencillo:

Ejemplo. Para la tutela del bien jurídico vida, a la luz de la normativa penal costarricense, nuestro legislador toma en consideración la lesión a dicho bien y la condición de quien realiza la acción, de ahí que la tipifica en homicidio simple[25] o calificado[26], partiendo de la misma acción penal "quien haya dado muerte a una persona";

[25] **Código Penal de Costa Rica.** Homicidio simple. ARTÍCULO 111.- Quien haya dado muerte a una persona, será penado con prisión de doce a dieciocho años. (Así reformado por el artículo 1 de la ley Nº 7398 de 3 de mayo de 1994)

[26] **Código Penal de Costa Rica.** Homicidio calificado. ARTÍCULO 112.- Se impondrá prisión de veinte a treinta y cinco años, a quien mate: 1) A su ascendiente, descendiente o cónyuge, hermanos consanguíneos, a su manceba o concubinario, si han procreado uno o más hijos en común y han llevado vida marital, por lo menos durante los dos años anteriores a la perpetración del hecho. 2) A uno de los miembros de los Supremos Poderes y con motivo de sus funciones. 3) A una persona menor de doce años de edad. 4) A una persona internacionalmente protegida, de conformidad con la definición establecida en la Ley N.º 6077, Convención sobre la prevención y el castigo de delitos contra las personas internacionalmente protegidas, inclusive agentes diplomáticos, de 11 de agosto de 1977, y otras disposiciones del Derecho internacional. 5) Con alevosía o ensañamiento. 6) Por medio de veneno

sin dar mayor importancia al medio utilizado[27]. Poco relevante resulta entonces que se realice con un martillo, una roca, un cuchillo o un ordenador. Esto quiere decir que siempre lo que se configurará es un homicidio, así es, pues sería irrazonable pensar en un cuerpo legal que determine tipos penales específicos según el medio que se utilice para realizar la conducta ilícita: "homicidio simple o calificado con martillo, homicidio simple o calificado con roca,…Si un sujeto utiliza su ordenador para alterar otro ordenador que alimenta un respirador de un sujeto hospitalizado, ¿existe una sanción superior a la acción de homicidio, por haber sido cometido a través de un medio informático? Simplemente la acción es homicidio por provocar una lesión contra el bien jurídico vida.

Este cuestionamiento, es uno en un millón, basta con analizar cada tipo penal introduciendo la utilización de un medio informático para su comisión y plantearse la misma pregunta, para así arribar al mismo problema: "la acción penal no se define por el medio utilizado sino por el fin perseguido y la lesión causada". Existen tipos penales que no por el hecho de ser cometidos con la intervención de un elemento informático deben tipificarse como un delito informático.

Como primera precisión entonces tenemos que constituyen sólo delitos informáticos aquellas acciones que se dirijan (su fin sea) a causar una lesión o perturbación en la operación del ordenador, y como segunda precisión introducimos que esta afectación debe recaer específicamente sobre el software del ordenador, no así sobre el hardware.

Por lo tanto, se constituirían en acciones que abarca el delito informático:

---

suministrado insidiosamente. 7) Por un medio idóneo para crear un peligro común. 8) Para preparar, facilitar, consumar u ocultar otro delito o para asegurar sus resultados o procurar, para sí o para otro, la impunidad o por no haber logrado el fin propuesto al intentar otro delito. 9) Por precio o promesa remuneratoria. 10) A un miembro de los cuerpos policiales del Estado, municipal y de las demás fuerzas de policía públicas, cuya competencia esté prevista por ley, siempre que sea en ejercicio, por causa o en razón de sus funciones. (Así adicionado el inciso anterior por el artículo 1° de la ley N° 8977 del 3 de agosto del 2011, "Calificación de los delitos cometidos contra la integridad y vida de los policías en el ejercicio de sus funciones" (Así reformado por el artículo 1°, punto 1., aparte a) de la Ley de Fortalecimiento de la Legislación contra el Terrorismo, N° 8719 de 4 de marzo de 2009).

[27] Salvo ciertas excepciones como el uso de veneno o de medio idóneo para crear un peligro, situaciones que en todo caso se clasifican como calificantes del mismo tipo penal, sin necesidad de la creación de un tipo penal en específico como sería "homicidio con veneno". Ver artículos 111 y 112 del Código Penal costarricense.

1) La manipulación en los datos e informaciones contenidas en los archivos y soportes físicos informáticos ajenos[28], incluyendo sus cuatro fases:

   a) Almacenamiento de los datos.

   b) Procesamiento de los datos.

   c) Retroalimentación (feedback) con resultados intermedios de los datos, y;

   d) Transmisión de los resultados del proceso, ya sea en el mismo ordenador a ficheros de destino, ya sea por medio de comunicaciones o acceso a periféricos en los que se depositan.

2) El acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello.

3) La introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas, así como también el sabotaje de computadoras mediante "Bombas lógicas"[29].

[28] A saber: (1) Manipulación en el ingreso de los datos a la computadora, (2) Manipulación de datos ingresados a la computadora, (3) Manipulación de Programas, conocida como la famosa "técnica salami", en la que el autor no manipula ni altera los datos de la computadora, sino que por el contrario, la manipulación y/o alteración se genera en el programa. Un ejemplo de este caso, relativamente sencillo es el del empleado bancario, que altera el programa de cálculo de intereses de las cuentas de ahorro, de manera tal que solo los dos primeros dígitos de los decimales, se tomen como intereses y los restantes dígitos se transfieran a una cuenta, por él controlada. De esta manera tan simple, es posible obtener grandes sumas de dinero, pues los cuentahabientes no lo pueden detectar, y (4) Manipulación en los datos que salen de la Computadora o el "Caballo de Troya" que ocurre cuando los datos se transfieren a otra computadora, en los programas de impresión (output), o en programas de actualización, es decir, una vez que los datos son ingresados, ordenados y los procesos de cálculo elaborados, la información final, por lo general se imprime y almacena. Es posible así manipular la información que se imprime y almacena, de manera tal que la alteración no pueda detectarse, durante el procesamiento de datos.

[29] Esta forma de criminalidad tiene por objeto la afectación o destrucción tanto del programa, como de los datos almacenados en la computadora, bien puede provocarse un daño al hardware o disco duro, pero la forma más común de comisión es a través del deterioro de los datos almacenados y los programas. Un ejemplo clásico es la intromisión de los denominados virus, que son programas que se almacenan o instalan en determinados sectores del hardware y/o programas de la computadora y que se encargan de destruir la información, inutilizarla o bien producir daños al mismo disco duro, que lo hacen inaccesible y/o inservible.

4) La agresión a la privacidad mediante el procesamiento de datos personales con fin distinto al autorizado, lo que podríamos denominar "espionaje por computadoras"

5) Estafa Electrónica[30], el sabotaje informático, la interceptación de comunicaciones electrónicas y los demás tipos penales introducidos por la ley.

Bien, sin necesidad de ahondar en estos ejemplos y reafirmando nuestra posición respecto a que, delitos informáticos sólo deben configurarlos aquellas acciones que por su fin se dirijan a la lesión del software del ordenador.

Una vez realizadas las precisiones conceptuales precedentes, se impone en consecuencia esgrimir las bases teoréticas de nuestro planteamiento. Como ya se dijo, desde el punto de vista teórico, existe la posibilidad de pensar que en un futuro y con base en nuevos desarrollos tecnológicos, se vayan creando nuevas modalidades delictivas, nuevas formas de criminalidad asociadas con el uso de la tecnología, que hagan que en un plazo [que estimamos relativamente corto] aparecerán supuestos de hecho que no puedan ser abarcados por los tipos penales tradicionales.

Tecnologías como la inteligencia artificial que hoy se emplean en cosas tan elementales como las casas inteligentes, los vehículos inteligentes, sistemas informáticos para manejar de inventarios, robots para todo tipo de procesos, incluso ya es una realidad que hasta en oficinas legales en nuestro país para la evacuación de consultas legales se emplea inteligencia artificial, sin la intervención persona alguna. Todo eso nos lleva a pensar, que pronto veremos hechos susceptibles de ser abarcados por tipos penales existentes, pero que por ausencia de "una persona" o "sujeto" de una "acción humana" en sentido estricto no pueden ser aplicados al caso concreto.

[30] Es preciso antes señalar que técnicamente no es ninguna estafa, por ausencia de un sujeto pasivo que realice el acto dispositivo, sin embargo se asemeja a la hipótesis de la estafa triangular, la cual supone que el engañado y el estafado son personas diferentes. Sin embargo, en la estafa triangular el engañado tiene la facultad de realizar un acto dispositivo perjudicial para el estafado, de manera que el autor le produce a través de ese engaño, una lesión a su patrimonio y obtiene para sí o para un tercero un beneficio patrimonial antijurídico. En el caso de la aquí denominada "estafa electrónica" lo que el autor hace es "engañar" [utilizamos el término únicamente como una pseudodefinición estipulativa porque claramente no es un engaño, sino una manipulación] a la computadora (que sustituye al sujeto pasivo), y produce con esto que la computadora realice un acto dispositivo perjudicial para un tercero, desde luego, pues para la computadora no puede existir un perjuicio patrimonial en ningún supuesto.

Estas nuevas formas delincuenciales y la experiencia derivada del abordaje pasado de la denominada "Ciberdelincuencia" por medio de la creación de tipos penales paralelos, a tipos penales existentes como forma de combatir esos nuevos fenómenos vgr. Estafa vs Estafa Informática, Violación de correspondencia vs Interceptación de Comunicaciones Electrónicas, Daños vs Sabotaje Informático, y así sucesivamente; pareciera que nos conduce irremediablemente hacia la aquí denominada "polución" del delito informático. Que es la aparición cada vez más frecuente de nuevas formas de delincuencia asociada a nuevas tecnologías, que se combate por medio de la creación de tipos penales paralelos [similares a los ya existentes], que permitan "cerrar las puertas" que los tipos tradicionales dejaron abiertas, al no contemplar el uso de la tecnología como formas de comisión del hecho punible.

Por eso la propuesta que se antoja como tesis central de este aporte, se basa en el empleo del artículo 45 del Código Penal vigente que como vimos, introdujo el empleo de la autoría mediata como forma de comisión del hecho punible al señalar que es autor del hecho punible quien lo **realizare por sí o sirviéndose de otro u otros**.

Como ya se sabe, la interpretación que la doctrina dominante ha dado a la frase, consiste en entender que el servirse de otro u otros, ha sido entendido como emplear para la comisión del hecho punible a uno o más sujetos [como instrumentos] de su acción.

De lo anterior se infiere, que es dable pensar, que si el derecho penal ha podido equiparar a la categoría de objeto o instrumento, la acción humana cuando es dominada por otro [autor] del hecho punible, con mucha más razón y facilidad puede aceptar, que es autor del hecho punible quien lo comete por medio de un instrumento [computadora], que en sentido óntico[31] es un instrumento en sí mismo.

De lo expuesto se deriva la propuesta de *lege ferenda* de reforma del artículo 45 del Código Penal, que supone cerrar la brecha existente y ampliar la punibilidad a nuevas

[31]En el pensamiento de Heidegger, filósofo alemán del siglo XX, referente a los entes, a diferenci a de *ontológico*, que se refiere al ser de los entes.

formas de comisión de hechos penales por medio del empleo de nuevas tecnologías, a saber:

> *Artículo 45.- Es autor del hecho punible tipificado como tal, quien lo realizare por sí o sirviéndose de otro u otros* ***o por medio de un instrumento empleado para tal fin****, y coautores los que lo realizaren conjuntamente con el autor.*

5) Conclusión.

La propuesta de modificación del artículo 45 del Código Penal aquí planteada, presenta tres grandes ventajas con respecto a la situación existente y la crítica esgrimida:

a) Se trata de una modificación de la parte general del Código Penal, que por consiguiente, resulta de aplicación a todos los tipos penales existentes y futuros, tanto del Código Penal como del denominado derecho penal accesorio, esto; sin necesidad de realizar cambio alguno en la legislación vigente y mejor aún, sin necesidad de recurrir a la casuística como hasta la fecha, cada vez que aparece un supuesto fáctico que por algún tecnicismo no puede ser abarcado por un tipo penal existente, a falta de un autor del hecho punible y del empleo de la tecnología para su comisión.

b) Por tratarse de una norma de carácter general, el Legislador no requiere de crear tipos penales específicos y concretos, para sancionar la comisión de delitos, por medios electrónicos, telemáticos y/o informáticos, de forma tal que se elimina la duplicidad de tipos penales (uno general y otro informático vgr. estafa y estafa informática, daños y sabotaje, violación de correspondencia e interceptación de comunicaciones, espionaje y espionaje informático, etc.).

c) Se elimina por completo la falsa creencia de que el delito informático es un delito especial, que requiere de grandes conocimientos científicos y/o capacidades especiales, y que está reservado únicamente para mentes privilegiadas, sino que se acepta de una vez y por todas, que los sistemas informáticos, telemáticos, electrónicos, en una palabra, la tecnología; llegó para quedarse y cada vez es más

común encontrar toda suerte de aplicaciones tecnológicas que si bien es cierto, en su inmensa mayoría han simplificado las labores cotidianas y hacen la vida más cómoda, también lo es; que abren la posibilidad a nuevas manifestaciones criminales, propias de nuestro tiempo y que hacia el futuro se vislumbran como cada vez más elaboradas, por lo que es preferible reaccionar a tiempo que no esperar a que aparezcan para buscar caso por caso una solución en particular.

6) Comentario final.

Esta tesis no es producto de un análisis de la reciente discusión con ocasión de esa denominada polución del delito informático que criticamos, más bien, esta fue nuestra tesis de Maestría presentada en la Albert-Ludwigs-Universität Freiburg (República Federal de Alemania), cuando realizamos estudios en el Institut für Kriminologie und Wirtschatstrafrechts (1997-2000) adscrito a esa casa de estudios, en esa época bajo la dirección de Prof. Dr. Drs h.c. mult. Klaus Tiedemann (q.d.D.g.), quien fue el creador del artículo §263 del StGB (Strafgezetzbuch o código penal alemán).

Recordamos hoy tan fresco como ayer, cuando el asistente científico del Prof. Tiedemann en esa época, el hoy Prof. en la Universidad de Colonia, República Federal de Alemania, Martín Wassmer, nos informó, que para que la tesis pudiera ser aprobada por el señor Tiedemann, debía ser suprimido del texto original esta posición, pues atentaba contra su obra científica de la cual él se sentía muy orgulloso. Algunos nos impulsaron a que escribiéramos nuestro punto de vista, tenemos presentes en esa línea de pensamiento al hoy profesor de la Universidad de Granada, España y muy recordado amigo, el Prof. Dr. Javier Vals Prieto, quien hasta me rogó que lo hiciera mas nunca lo hicimos, fue grande la desilusión por esa especie de "censura científica", que nos duró cuatro lustros. Por eso, hoy 20 años después de aquellos días y en honor a uno de los grandes maestros del derecho penal y procesal costarricense, dejamos plasmadas esas líneas para ser sometidas a la crítica y si es que lo merecen, algún tipo de análisis por parte del foro.

6) Bibliografía.

GUTIERREZ F., M. L. Fraude Informático y estafa (Aptitud del tipo de estafa en el Derecho español ante las defraudaciones por medios informáticos), Ministerio de Justicia, Secretaría General Técnica, centro de publicaciones, Madrid 1991.

BERISTAIN, A. La reforma del código penal alemán en Anuario de Derecho penal y Ciencias penales, 1969, p. 371, tonado de: Dialnet-LaReformaDelCodigoPenalAleman-2784688.pdf

CHINCHILLA S. C. *Delitos Informáticos, Elementos básicos para identificarlos y su aplicación*, San José, Costa Rica, Ediciones Farben, 2004.

CONSEJO DE EUROPA. Recomendación R (89) 9, del Comité de Ministros del Consejo de Europa a los Estados Miembros del 13 de septiembre de 1989, durante la sesión 428 [a], reunión de los Delegados de los Ministros.

CORREA y otros, Derecho Informático, Ediciones Depalma, Buenos Aires, 1987.

FRANKL, V. El hombre en busca de sentido. Editorial Herder. Barcelona. 1979

DAVARA R, M.A. Manual de Derecho Informático, Aranzadi Editorial, 1997.

POPPER, K. En busca de un mundo mejor. Ediciones Paidós Iberoamérica. Barcelona. Buenos Aires. México, 1994.

SALAZAR, A. Delito Informático (Análisis comparativo con el delito de danos y otros tipos del Código Penal costarricense), en Revista de Ciencias Jurídicas, Universidad de Costa Rica - Colegio de Abogados de Costa Rica, Número 88, Setiembre - Diciembre 1998, y Cuadernos de Doctrina y Jurisprudencia Penal, Argentina, Año V, Número 9 A, p. 709-727.

SALAZAR, A. Perspectiva criminológica del crimen por computadora en Revista de Ciencias Jurídicas, Universidad de Costa Rica - Colegio de Abogados de Costa Rica, Número 149, Mayo- Agosto, 2019, p. 133-166.

SALAZAR, A. Una nueva visión del recurso de casación por el fondo en el derecho procesal penal costarricense, en CDJP (Casación), Nº 1 (2001) y en Ciencias

Penales. Revista de la Asociación de Ciencias Penales de Costa Rica, Año 12, N° 17, Marzo, 2000.

SALAZAR, A./GUERRERO, E. Comentario críticos a la reforma del Código Penal que introduce la ley 9048 (Sobre los delitos informáticos en el derecho penal costarricense) localizable en: https://escuelajudicialpj.poder-judicial.go.cr/images/DocsRevista/revistajudicial112.pdf

TIEDEMAN, K.; COSSON, J., Straftaten und Strafrecht im deutschen und französischen Bank- und Kreditwesen, Köln/Berlin/Bonn/München, 1973, p. 25.

TIEDEMANN, K., Poder Económico y Delito, Ariel, 1985.