dicho software:

Cuando se hace esta pregunta nos referimos a las características que ha de reunir el sistema de base datos, desde el punto de vista del usuario, teniendo presente en todo momento que es un producto de software, suponiendo que se dispone del computador adecuado.

Las características deseables se pueden resumir en dos: sencillez de uso y versatilidad.

Cuando decimos sencillez de uso, queremos decir que no se requieren grandes conocimientos iniciales, que se precise poco tiempo para aprender su manejo y que la entrada de datos sea cómoda. Y finalmente cuando se refiere a la versatilidad, se requiere que tenga capacidad de clasificación, búsqueda de datos rápida y que pueda generar informes fácilmente, gráficos etc.

LA INFORMATICA Y EL DERECHO EN COSTA RICA

Juan Diego Castro Fernández
Costa Rica

Costa Rica es una República Democrática, con la particularidad, única en el mundo, de que de conformidad con el artículo décimo segundo de nuestra Constitución Política "Se proscribe el ejército como institución permamente". El nuestro es un "estado de derecho", simentado en la vieja tradición jurídica de nuestro pueblo. El Derecho se estudia en nuestro país desde hace más de siglo y medio a nivel universitario. Ha prevalecido la fuerza de la razón y de la ley frente a la irracional fuerza del fusil. Podemos decir que en todos los costarricenses, hay dentro, un duende de abogado, y la llama inextingible de la libertad y de la paz.

Las computadoras tuvieron su aparición en Costa Rica, al igual que en todos los países latinoamericanos hasta hace muy pocos años, pero hoy en día es innegable la presencia y la importancia de estas máquinas en todos los ámbitos de la vida privada y pública de la nación. Las elecciones nacionales y el Registro Civil se han informatizado. El Estado que es el mayor empleador del país, paga sus salarios mediante giros confeccionados electrónicamente por la computadora de la Oficina Técnica Mecanizada. La banca nacionalizada cuenta con importantes centros de cómputo, así como el Seguro Social, el Instituto Costarricense de Electricidad y las más importantes empresas del sector privado. Asimismo la automatización del Registro Nacional, ha sido un factor que obligó a los juristas a interesarse en el tema de la informática.

La máquina de Konrad Zuse, la "Z3", implementada en 1941 y totalmente destruída en 1944 durante una incursión aérea, era eléctrica y dependía de relés para llevar a cabo los cálculos. El "mark I Automatic Sequence Controlled Calculator" de Howard Aiken, construído en 1944 en la Universidad de Harvard, funcionaba según el mismo principio. De esta manera, un nuevo personaje entraba en el escenario mundial, en computador electrónico. (1).

LEE LOEVINGER, un joven catedrático norteamericano, fue el primer estudioso en darse cuenta de la importancia de esta herramienta electrónica y de la cibernética para el derecho. En 1949, la Minnesota Law Review publicó su ensayo: "JURIMETRICS: THE NEXT STEP" (Jurimétrica: el próximo paso). El próximo paso era "intentar aplicar los métodos científicos en el campo del derecho", es decir, aplicar el procesamiento electrónico de datos en el derecho. (2).

En octubre de 1960, se celebró en Lake Arrowhead, California, la PRIMERA CONFERENCIA SOBRE DERECHO Y ELECTRONICA. Las actas de esta conferencia fueron publicadas en 1962, con el título "THE CHALLENGE OF A NEW ERA" (El Desafío de una nueva era).

En 1962, el escritor francés PHILIPPE DREYFUS, acuñó un término nuevo "informatique" (informática), que a su vez reunía otras dos palabras "información" y "automático".

La Academia Francesa la definió como: "la ciencia del procesamiento racional, esencialmente mediante máquinas automatizadas, de la información considerada como la base del conocimiento y de la comunicación en las esferas técnicas, económicas y sociales".

En 1963, VICTOR KNAPP publicó en Praga su libro "LA APLICABILIDAD DE LA CIBERNETICA EN EL DERECHO". Este libro escrito en checo e influenciado por la metodología marxista no se difundió inmediatamente en Europa occidental o en Estados Unidos. Sin embargo una revista de Alemania del Este, "Staat und Recht", publicó el mismo año, un artículo del Profesor Knapp que llamó la atención de los estudiosos occidentales sobre las ideas contenidas en el libro.

En Europa Occidental, Vittorio Frosini publicó el primer libro sobre la relación entre el derecho y los computadores: "CIBERNETICA, DIRITTO E SOCIETA" (Cibernética, Derecho y Sociedad) Milán, 1968. Este dio lugar a debates entre juristas y sociológos de todo el mundo. (3).

Costa Rica, subdesarrollada, o en vías de desarrollo, que depende fundamentalmente de la exportación de sus productos agrícolas (café, banano, azúcar). País que importa ahora no solo el equipo electrónico, a muy alto precio, sino que siempre ha importado el papel, la tinta, los lapiceros y las máquinas de escribir, así como las imprentas, los televisores, las radios y los teléfonos, hace frente no solo a la profunda brecha de la industrialización, sino también a la de la informatización. No podrá operarse pues, una transferencia mecánica de las tecnologías informáticas de los países llamados desarrollados hacia el nuestro, puesto que la misma realidad socioeconómica nuestra es muy diferente a la de tales sociedades avanzadas, y nuestro derecho, de informatizarse, debe hacerse partiendo de nuestra propia realidad y de nuestras verdaderas necesidades, y no de las necesidades de mercadeo de los vendedores de equipo electrónico, que a veces resulta caro y desactualizado.

"La sociedad tecnológica moderna, caracterizada por su desarrollo e innovaciones rápidas y cuyo símbolo es el computador ha planteado numerosas cuestiones jurídicas que podrían definirse como el problema de la nueva frontera del derecho, un nuevo tipo de experiencia jurídica: el derecho informático.

Ya existe una abundante literatura sobre la amenaza potencial del computador sobre el individuo, el impacto del computador sobre la sociedad, y la necesidad de reglamentar la gestión y la utilización de los bancos de datos que constituyen la fuente del poder informativo. Esta documentación subraya lo difícil que es ejercer un control estatutario sobre la utilización del computador, con miras a "controlar a quienes controlan" —o sea, a quienes se encargan de la gestión de la información basada en el computador. Pero la profesión jurídica aún no se ha dado cuenta suficientemente de la importancia de la informática como fuente de poder, como medio de transformación no solo tecnológica sino también social. Aún existen, numerosas lagunas en el derecho informático y todavía no se ha emprendido ninguna sistematización de los conceptos. (4).

DELITO INFORMATICO

El impacto de la computación se puede observar en todos los niveles sociales. En lo jurídico es de tal magnitud, que podemos decir que con la informatización del derecho, estamos en la época de la visión jurídica en tercera dimensión. Las enormes masas de información jurídica se hacen manejables con una facilidad increíble, y en la medida en que los "thesaurus" jurídicos se perfeccionen, el acceso a la información legal será cada vez más fácil.

Todas las disciplinas jurídicas están afectadas por la informática, y la penal no es la excepción, todo lo contrario, podemos afirmar que es quizá

la rama jurídica, en la que la computación juega un papel muy interesante y particular. Partimos de que "la computadora", como herramienta constituye la generalidad de las veces el instrumento del que eventualmente se puede servir el delincuente para realizar su acción ilegítima, pero sin embargo en cierta medida, con el propio avance de la informática se hará necesario regular con mayor precisión los tipos penales, de modo que las conductas queden más claramente delineadas.

Por supuesto que en nuestro derecho penal positivo no existe aún, figura penal alguna que se refiera directamente al mundo de la informática. Esta situación hace que no exista definición jurídica alguna, en nuestra sistemática penal, sobre delito informático.

Se habla de "delitos cometidos con computadoras", "delitos cibernéticos", pero nos inclinamos por el término "delitos informáticos", entendido en el mismo sentido que en la literatura norteamericana tiene "computer crimes", lo que nos lleva a conceptualizarlo en dos sentidos:

Restringido: "aquel hecho en el que —independientemente del perjuicio que pueda causarse en otros bienes jurídicamente tutelados y que eventualmente puedan concurrir en forma real o ideal— se atacan elementos puramente informáticos. Tales serían los casos del uso indebido del software, apropiación indebida de datos, interferencias en sistemas de datos ajenos, etc."

Amplio: "Acción típica, antijurídica y culpable para cuya consumación se utiliza o se afecta a una computadora o sus accesorios" (5).

ELEMENTOS DEL DELITO INFORMATICO

Elemento Objetivo:

Dado por la acción que la ley tipifica como delito. En el "homicidio" (artículo 111 del Código Penal) "quien haya dado muerte a una persona", en el hurto "el que se apoderare ilegítimamente de una cosa mueble, total o parcialmente ajena" (artículo 208 del Código Penal), en los daños "el que se destruyere, inutlizare, hiciere desaparecer o de cualquier modo dañare una cosa total o parcialmente ajena (artículo 228).

Decimos junto con las juristas argentinas Lilli y Massa: "En los delitos informáticos, la acción no resulta tan clara, dada la diversidad de bienes jurídicos, tutelados, como de formas de perpetrar el delito. Así en algunos casos la acción tiende a afectar elementos componentes de la computadora —tanto el hardware como el software— mientras que en otros casos la computadora solo es utilizada como medio o instrumento para cometer el delito. Por último, puede suceder que sin afectar el hardware o el software de una computadora, ni utilizar la computadora para la perpetración de un hecho ilícito autonómo, el ilícito consista en el uso o utilización indebida de una computadora sin la correspondiente autorización.

Dentro de estos tres grandes grupos estaría encuadrado el elemento objetivo del delito informático —es decir la acción— debiendo el legislador tipificar a través de figuras lo más exactas posibles tales acciones.

Elemento subjetivo:

De acuerdo con el artículo treinta de nuestro Código Penal: "Nadie puede ser sancionado por un hecho expresamente tipificado en la ley si no lo ha realizado con dolo, culpa o preterintención".

Si partimos, de que actualmente y de conformidad con el derecho penal positivo, tendrán relevancia jurídica en nuestro sistema jurídico-penal, únicamente los "delitos informáticos" que se adecúen a los tipos de

nuestro ordenamiento, ya que no existen, en sentido restringido delitos informáticos propiamente dichos.

Veremos entonces cómo podremos estar frente a hechos delictivos, cometidos con, por o en contra de una computadora y sus partes, que para ser delitos deberán necesariamente cuadrar en alguna figura penal, como "daños", "hurto", "estafa", etc.

Nos parece que tales conductas, dentro de este concepto de delitos informáticos, podrán ser atribuidas a sus partícipes tanto a título de dolo, como de culpa.

SUJETOS DEL DELITO INFORMATICO

SUJETO ACTIVO:

El "Delincuente informático" será la persona que realiza la conducta descrita en el tipo penal.

Criminológicamente hablando, estamos en presencia sin lugar a dudas de un clarísimo "delito de cuello blanco", en donde los autores no solo reunen condiciones técnicas o profesionales muy singulares, sino que han logrado un cierto dominio de su "oficio" que les permite ejecutar el delito.

"En este tipo de delitos el obrar delictivo está precedido por la atenta observación del accionar de quién será su víctima o su herramienta: la computadora. Tales sujetos se reclutan en sectores instruídos, con acceso a determinadas oportunidades y conocimientos imprescindibles que les permiten incrementar su riqueza mediante el uso de modernas técnicas a las que tienen acceso por su ocupación o disponibilidad de medios" (6).

RELACION SUJETO ACTIVO/FUNCION O EMPLEO

Los técnicos y profesionales vinculados a la computación, que se han visto involucrados en hechos delictivos, según Lilli y Massa, son:

OPERADORES:

Pueden modificar, agregar, eliminar o sustituir información y/o programas, copiar archivos para venderlos a competidores. Pueden estar envueltos en colusión.

PROGRAMADORES:

Pueden violar o inutilizar controles protectores del programa y/o sistema; dar información a terceros ajenos a la empresa, atacar el sistema operativo, sabotear programas, modificar archivos, acceder a información confidencial.

ANALISTAS DE SISTEMAS:

Es comúnmente el único que conoce la operación de un sistema completo, puede estar en colusión con el usuario, programador y/u operador.

ANALISTA DE COMUNICACIONES:

Es la persona que diseña la seguridad del sistema de comunicaciones por lo que conoce los métodos para violar la seguridad con fines de fraude.

SUPERVISORES:

Tienen conocimiento global de las operaciones y debilidades del sistema de seguridad, pueden manipular los archivos de datos y los ingresos y salidas del sistema. Tienen la posibilidad de modificar, agregar o eliminar información.

PERSONAL TECNICO Y DE SERVICIO:

Generalmente tienen libre acceso al Centro de Cómputo, poseen mayores conocimientos de los sistemas operativos y de base de datos, así como de sus debilidades.

FUNCIONARIOS SUPERIORES:

Tienen conocimiento general de los proyectos por lo que implican una amenaza potencial. Pueden estar en colusión con analistas, programadores, usuarios y/o operadores.

AUDITORES:

Conocen las debilidades del sistema toda vez que implementan las medidas de seguridad, instalando controles preventivos u otros que a posteriori permitan detectar el fraude antes que la persona involucrada pueda escaparse. Pueden actuar en colusión con otro personal.

BIBLIOTECARIOS DE PROGRAMACION:

Como es el responsable del mantenimiento de la documentación de sistemas, pueden vender la documentación a competidores u otros compradores.

BIBLIOTECARIOS DE OPERACIONES:

Constituye una amenaza de alto riesgo, toda vez que puede destruir información mediante la utilización de imanes o identificando como "scratch" (destruir) cintas correspondientes a archivos maestros; copiar información para vender, cambiar etiquetas externas.

PERSONAL DE LIMPIEZA MANTENIMIENTO Y CUSTODIA:

Pueden vender el contenido de los cestos de papeles a competidores u otros compradores, fotografiar documentos dejados sobre los escritorios, sustraer información y/o listados del Centro de Cómputo, sabotear el sistema con explosivos.

USUARIOS:

Tienen la posibilidad de hacerse pasar por otros usuarios, modificar, omitir o agregar información con propósitos fraudulentos; vender información a competidores, y efectuar un uso no autorizado". (7).

SUJETO PASIVO:

Las víctimas de los "delincuentes informáticos" han sido fundamentalmente los Bancos, compañías financieras, aseguradoras, instituciones estatales de servicios públicos, universidades, colegios, grandes empresas.

BIENES JURIDICOS TUTELADOS

"Partiendo de la base que nuestro legislador no ha previsto en absoluto delitos consumados contra medios o con el concurso de medios informáticos, resulta claro que el "delito informático" no existe en nuestro derecho penal positivo, para el cual hasta el presente la computadora es tan irrelevante como un lápiz o una máquina de escribir" (8).

En Costa rica, los delitos que se cometan por medios informáticos o en contra de ellos para ser típicos tienen que adecuarse a alguna de las figuras de nuestro derecho penal positivo, por lo que podemos sostener que prácticamente las computadoras pueden ser instrumento con el que sean cometidos los más importantes delitos de nuestro catálogo penal:

DELITOS CONTRA LAS PERSONAS

La medicina moderna cuenta con las computadoras entre sus más importantes instrumentos de diagnóstico clínico, por lo que es posible que a nivel de "mal praxis" el uso indebido de la computadora represente responsabilidad para el médico, por dolo o por culpa, teniendo frente a nosotros desde un homicidio simple, un homicidio culposo, unas lesiones o hasta lesiones culposas.

DELITOS CONTRA EL HONOR

Con respecto a la dignidad, decoro, honra, reputación al incluirse información falsa de carácter injurioso en un archivo electrónico, que al darse a conocer cause un perjuicio al honor. O bien que en registros electrónicos se conserve información falsa "que ofensa la memoria de una persona muerta con expresiones injuriosas o difamatorias".

Asimismo podría suceder con informaciones falsas contenidas o suministradas por medios electrónicos sobre "hechos falsos concernientes a una persona jurídica o a sus personeros por razón del ejercicio de sus cargos que puedan dañar gravemente la confianza del público o el crédito de que gozan". En otros países existen empresas de gran prestigio que venden información sobre corporaciones a nivel legal, administrativo y financiero, fundamentalmente para efectos comerciales.

DELITOS CONTRA LA INTIMIDAD

Con el desarrollo de los sistemas telemáticos, tales como transmisión de datos en paquetes y el correo electrónico, podríamos encontrarnos frente a delitos de violación de correspondencia (artículo 196, C. Penal) y sustracción, desvío o supresión de correspondencia (artículo 197. Código Penal).

DELITOS CONTRA LA PROPIEDAD

Cuando pensamos en el "hardware", el problema del hurto o del robo

del equipo, es muy simple. Inclusive si pensamos en el hurto de uso, en tiempo de máquina. Pero con respeto al "software", la situación es más compleja, precisamente por la intagibilidad de los programas, porque pueden ser "copiados", sin ni siquiera estar en el centro de cómputo, podría ser hasta desde otro país, a través de los modernos medios telemáticos de hoy día. Estaríamos en presencia de un hurto (simple), o frente a los delitos relativos a los derechos de autor, o de la propiedad industrial. Tema que merece nuestra consideración especial.

La situación llama la atención si nos referimos a las defraudaciones. Hasta qué punto podemos considerar como "artificios o engaños", los medios electrónicos desarrollados por el delincuente informático para entrar al "sistema" y lograr que se acrediten a su cuenta fuertes sumas de dinero, o se le adjudiquen cualquier clase de bienes.

En nuestro país tenemos una sentencia de un Tribunal Superior Penal de San José, en que fueron condenados dos operadores del Centro de Cómputo del Banco Crédito Agrícola de Cartago, que mediante un sistema de "crédito revolutivo" cargaban sus cuentas corrientes de fondos ficticios, pero el asunto se resolvió desde el punto de vista de la falsedad, porque los imputados alteraban los comprobantes escritos de otras cuentas corrientes.

En los Estados Unidos, se conoce un caso famoso de fraude financiero mediante computadora. Es el caso RIFKIN. La víctima fue un Banco de Los Angeles, California, que diariamente realiza transferencias electrónicas de fondos a nivel internacional y por montos que oscilan entre los dos y cuatro billones de dólares".El delito fue calificado como "transferencia electrónica de fondos ilegales". Stanley Mark Rifkin, de treinta y dos años, contratado por el Banco para que estableciera un sistema de "back up" (respaldo) relativo a las transferencias electrónicas de fondos. Dada la falta de instrucciones detalladas Rifkin practicó un relevamiento integral para obtener la certeza de que el sistema de back up contemplara y reuniera todos los elementos necesarios, y además detectó fallas en el sistema en vigencia que le posibilitarían eventualmente practicar una transferencia de fondos ilegal. La idea de Rifkin era adquirir diamantes en Europa, lo que el 25 de octubre de 1978 ingresó a la sala de transferencias utilizando su identificación personal, la que mantenía en su poder, a pesar de haber finalizado su contrato. Saludó a los operadores y les dijo que concurría para verificar el funcionamiento del sistema, permaneció un tiempo en el lugar y confirmó que el sistema era el mismo que él había relevado. Además de las claves previstas, para la instrumentación final de la transferencia, un funcionario debidamente facultado proporcionaba la autorización final, empleando un código especial. Rifkin tomó el código vigente en ese momento, que se cambiaba varias veces por día, pero constaba en un papel adherido a una de las paredes de la sala. Luego de retirarse, realizó una llamada telefónica desde un aparato público, identificándose como el funcionario autorizado, requiriendo la transferencia de diez millones doscientos mil dólares sobre su cuenta bancaria en Nueva York. Posteriormente el dinero debía ser transferido a un banco suizo. Ello así ocurrió y Rifkin viajó a Europa y compró los diamantes. Luego volvió a los Estados Unidos y fue descubierto y detenido. (9).

DELITOS CONTRA FE PUBLICA

En Costa Rica, el Registro Nacional, prácticamente automatizado en su totalidad, la información atinente a la propiedad inmobiliaria, vehicular,

mercantil, etc., está almacenada en soportes magnéticos. Avance incuestionable, que además plantea algunas cuestiones interesantes, máxime ahora que estamos a punto de que el sistema se ha integrado a la red pública, en donde las demás dependencias estatales y los notarios se convierten en sus usuarios, ya no en las terminales del Registro, sino a través de sus microcomputadoras "conectadas" por vía telefónica. Ya no volveremos a presenciar hechos como la sustracción de un folio de un tomo de propiedad, o de una tarjeta de vehículo. Pero ¿podrá algún "delincuente informático" romper el sistema de seguridad y alterar la información registral? Los funcionarios que tengan fe pública, "darán fe" de lo visto en unapantalla de rayos catódicos,o de la información almacenada en medios magnéticos, no visibles como los documentos tradicionales. Al respecto sostiene Klaus Tiedemann,en su obra"Poder Económico y Delito": "el tipo penal de la falsificación de documentos exige que el documento sea la expresión tangible y probatoria de un pensamiento humano. Aunque se cuestione este requisito, los datos y programas de las computadoras no son en ninguna forma documentos, por cuanto los datos ARCHIVADOS ELECTRONICAMENTE no SON RECONOCIBLES VISUALMENTE. Por lo general, además, no permiten individualizar autores" (10).

Así podríamos continuar con la lista de acciones delictivas, que usando de computadoras, se enmarcan dentro de la tipología penal vigente.

CONCEPTO Y MODALIDADES DE LA CRIMINALIDAD MEDIANTE COMPUTADORES.

El Profesor alemán Tiedemann, en su obra antes citada, sostiene:

"Con la expresión "Criminalidad mediante computadoras" se alude a todos los actos antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro) realizados con un equipo automático de procesamiento de datos".

"Gracias a las investigaciones efectuadas desde hace diez años por el INSTITUTO DE CRIMINOLOGIA Y DERECHO PENAL ECONOMICO DE LA UNIVERSIDAD DE FRIBURGO", actualmente se puede ofrecer una recopilación bastante completa de asuntos penales, tanto de la República Federal Alemana como del ámbito europeo, para acreditar la existencia de tal criminalidad".

MANIPULACIONES:

"Estas pueden afectar tanto a la fase de suministro o alimentación (input) de datos, como a la de su salida (out put) y a la de su procesamiento (bajo la forma de manipulaciones en el programa o en la consola)". ..."Los sistemas para el procesamiento de datos operados a distancia... ofrecen una variante especialmente interesante con muchas perspectivas de ulteriores desarrollos, para las técnicas de manipulación aquí descritas: si se puede acceder a la computadora, por ejemplo a través de la red telefónica, mediante una terminal que opera a distancia, el autor puede efectuar la manipulación desde su casa, con su propia terminal y sin necesidad de introducirse personalmente en la empresa perjudicada... La acción y el efecto se verifican por separado, lo cual dificulta sobremanera el descubrimiento del hecho.

ESPIONAJE:

"En el ámbito del procesamiento de datos, el espionaje económico se ve favorecido por el hecho de que las informaciones se encuentran archivadas en un espacio mínimo y pueden ser transferidas sin ningún problema a otro soporte. Además en el centro del uso indebido de datos figura siempre el también llamado hurto de software, o sea el empleo indebido de programas de computación, elaborados generalmente con considerables esfuerzos y que a menudos encierran un valioso "know how" comercial.

BIBLIOGRAFIA

1.- FROSINI, Vittorio. "INFORMATICA JURIDICA Y DERECHO INFORMATICO". Revista Agora, número 6, 1983, página 22. IBI, Roma, Italia.
2.- FROSINI, Vittorio, OP.- cit.- página 22.
3.- Idem.- Página 23.
4.- Idem.- página 23.
5.- LILLI, Alicia Raquel y MASSA, María Amalia.- "DELITOS INFORMATIVOS", Ponencia presentada a las Jornadas Internacionales de Informática al Servicio del Derecho.- Mercedes, Buenos Aires, Argentina, junio 1985.
6.- Idem.
7.- Idem.
8.- Idem.
9.- Idem.
10.- TIEDEMANN, KLAUS.- "PODER ECONOMICO Y DELITO", Editorial Ariel, Barcelona 1985, página 133.
11.- TIEDEMANN, Klaus, OP.- cit.- páginas 126, 127, 128.

SABOTAJE:

"Tanto desde la perspectiva de la envergadura del daño como desde la del modo de realizar el hecho, son dignos de considerar los casos de sabotaje en el procesamiento de datos. También estos resultan favorecidos por la gran concentración de informaciones en un mínimo espacio. La destrucción total de programas y datos —por ejemplo, mediante atentados con incendio, imanes o "programas borradores" especialmente elaborados— pueden poner en jaque la continuidad de toda la empresa".

HURTO DE TIEMPO:

"La utilización indebida de instalaciones de cómputos por parte de empleados desleales o de extraños puede producir pérdidas considerables, especialmente en los sistemas de procesamiento de datos a distancia, al efectuarse cómputos con número de "account" ajenos".

"La criminalidad mediante computadoras 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 jurídicos" (11).

MODUS OPERANDI DE LOS DELINCUENTES INFORMATICOS

El jurista guatemalteco Rodolfo Bolaños Ramírez, en su ponencia presentada al Primer Congreso Iberoamericano de Informática Jurídica, celebrado hace un año en Santo Domingo, República Dominicana, expuso los métodos con que operan estos delincuentes en los Estados Unidos, citando al Profesor Dom B. Parcker:

1.- DATA DIDDLING (datos engañosos). Simple, seguro y común. Manipulación de datos antes o durante su entrada al ordenador.

2. TROJAN HORSE (caballo de Troya) Introducción de un conjunto de sentencias en la codificación de un programa para realizar una función no autorizada. Es el método más común de sabotaje.

3. SALAMI TECHNIQUES. Sustracción de pequeñas cantidades de "activos" de numerosas procedencias. (redondeo de cuentas).

4. SUPERZAPPING. Uso no autorizado de programas de acceso universal.

5. TRAP DOORS. (puertas con trampa) Utilización de interrupciones en la lógica de un programa, en la fase de desarrollo para su depuración, y uso posterior de éstas con fines delictivos.

6. LOGIC BOMBS (bombas lógicas) Programa que se ejecuta en un momento específico o periódicamente, cuando se cumplen determinadas condiciones. (rutinas a posteriori).

7.- ASYNCHRONOUS ATTACKS (ataques asincrónicos). Consiste en aprovechar el funcionamiento asincrónico de un sistema operativo, ya que la mayor parte de los sistemas operativos funcionan asincrónicamente basados en los servicios que pueden realizar para los distintos programas en ejecución.

8.- SCAVENGING (recogida de residuos). Obtención de información "residual" impresa en papel o cinta magnética en memoria después de la ejecución de un trabajo. (tercera o cuarta copia).

9.- DATA LEAKAGE (filtración de datos) Sustracción de datos o copias de datos de un sistema. (duplicar una cinta magnética).

10.- PIGGYBAKING AND IMPERSIONATION (trasiego de personas). Lograr el acceso a áreas controladas, por medios electrónicos o mecánicos.

11.- WIRETAPPING (pinchar líneas de teleproceso). Intervención de las líneas de comunicación para acceder o manipular los datos que son transmitidos.

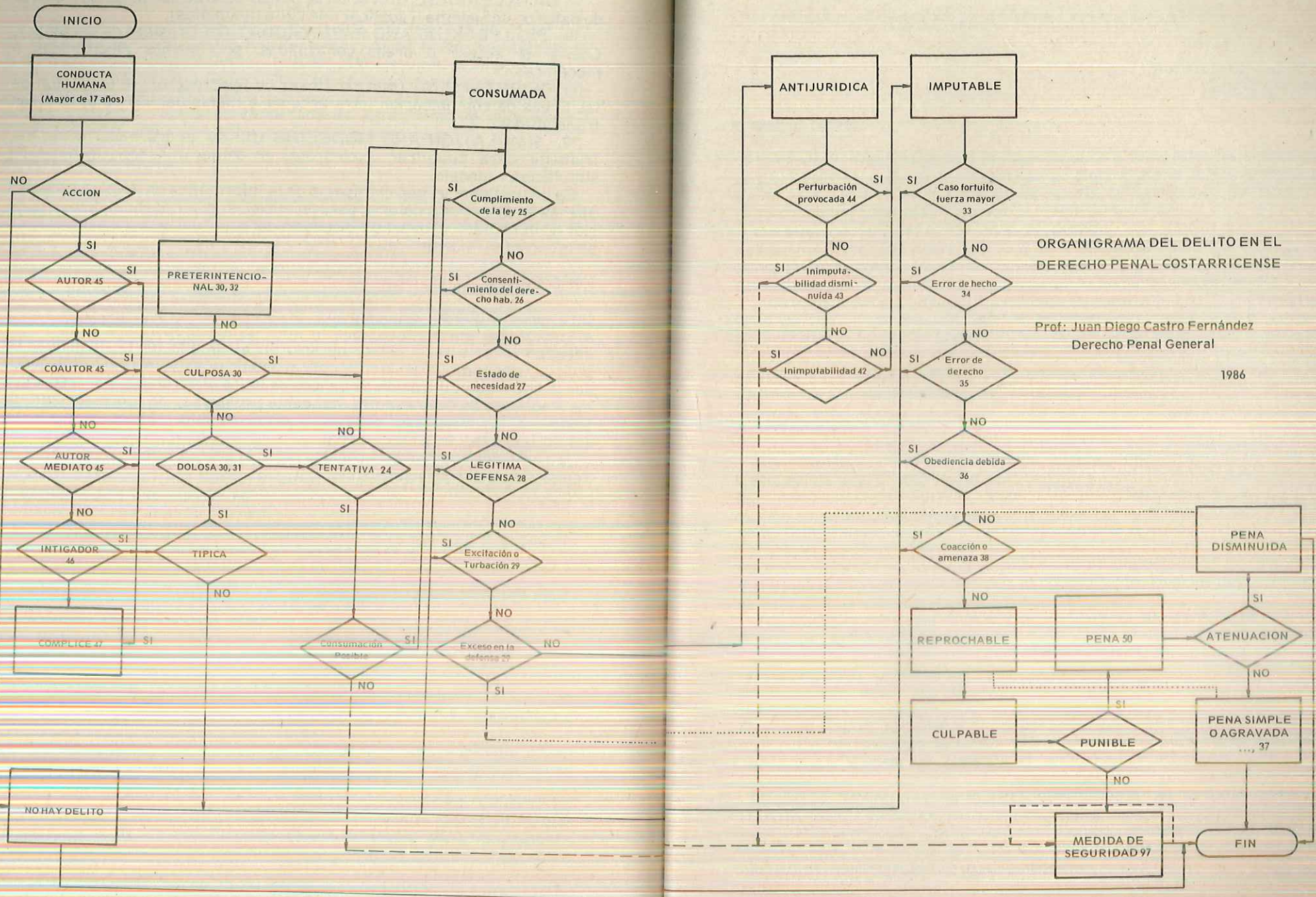
12.- SIMULATION AND MODELING. Utilizar el ordenador como instrumento para planificar y controlar un delito, utilizando técnicas de simulación y modelo.

Es incuestionable, que el impacto de la informática en nuestra sociedad apenas empezamos a notarlo, pero los juristas costarricences debemos iniciar de inmediato el estudio y discusión del papel del derecho democrático en la sociedad informatizada.

INFORMATICA DEL DELITO

Otro aspecto, que por supuesto no es el central de este trabajo, es el anotar al menos, las posibilidades que la informática proporciona a nivel tecnológico a la justicia penal, no solo en el ámbito de la investigación policial, sino también en lo referente al debido proceso mismo, como puede ser la adecuada utilización de bancos de datos electrónicos con respecto a los Registros de Delincuentes, así como programas de procesamiento de textos en los tribunales penales, y archivos informáticos de doctrina, jurisprudencia y legislación penal.

Ya el Poder Judicial está construyendo la base de datos respectiva en el registro Judicial de Delincuentes.



ORGANIGRAMA DEL DELITO EN EL DERECHO PENAL COSTARRICENSE

Prof: Juan Diego Castro Fernández
Derecho Penal General

1986