DELITO INFORMÁTICO:
ESTAFA INFORMÁTICA DEL ARTÍCULO 248.2 DEL CÓDIGO PENAL

Tesis Doctoral que presenta
El doctorando EDMUNDO ARIEL DEVIA GONZÁLEZ,
para la obtención del Grado de Doctor en Derecho
por la Universidad De Sevilla,
bajo la dirección del
Prof. Dr. *Dr. h. c. mult.* MIGUEL POLAINO NAVARRETE

UNIVERSIDAD DE SEVILLA
CURSO 2016 / 2017

A Maximiliano y Edmundo

A mi padre que desde alguna parte nos cuida…

.

“Dime y lo olvido, enséñame y lo recuerdo, involúcrame y lo aprendo”

Benjamín FRANKLIN

“Las organizaciones gastan millones de dólares en *firewalls* y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores”.

Kevin MITNICK – hacker

ÍNDICE

CAPÍTULO II

Consideraciones sobre informática.

Cuestiones relativas a internet, cibercrimen y su regulación

CAPÍTULO III

Fraudes a través de sistemas informáticos: planteamiento del problema

CAPÍTULO IV

Estafa informática en el Derecho comparado. Convenio de Budapest, Alemania, Italia y en Especial referencia al Ordenamiento jurídico de Chile

CAPÍTULO V

Referencias al tipo tradicional o básico de estafa y la estafa informática en España: antecedentes

CAPÍTULO VI

Imputación típica del delito de estafa informática

CAPÍTULO VII

Imputación objetiva en el delito de estafa informática

CAPÍTULO VIII

Naturaleza jurídica y Bien jurídico protegido en la estafa informática

ABREVIATURAS

AEPD /APD	Agencia Española de Protección de Datos
ACE	Abusos de correo electrónico
ADPCP	Anuario de Derecho Penal y Ciencias Penales
AEDI	Asociación Española para la Dirección Informática
AN	Audiencia Nacional
AP	Audiencia Provincial
APWG	Anti-Phishing Working Group
BUE	Boletín de la Unión Europea
Cap.	Capítulo
CCAA	Comunidades Autónomas
CE	Constitución Política de la Monarquía Española de 1978
CERT	Equipo de Respuesta ante Emergencias Informáticas
CSIRT	Equipo de Respuesta ante Incidentes de Seguridad Informática
Cit.	Citada
Cfr.	Confróntese
CGPJ	Consejo General del Poder Judicial
CP	Código Penal

CPU	Unidad Central de Procesamiento (*central processing unit*)
Coord. / Coords.	Coordinador / Coordinadores
CP	Código Penal
DARPA	Defense Advanced Research Projects Agency/ Agencia de Proyectos de Investigación Avanzados de Defensa
Dir. / Dirs.	Director / Directores
DRAE	Diccionario de la Real Academia Española
EEUU	Estados Unidos
Ed.	Edición
FBI	Federal Bureau of Investigation
INCIBE	Instituto Nacional de Ciberseguridad de España
IPTO	Agencia para Proyectos de Investigación Avanzados
IP	Dirección univoca de cada ordenador o maquina conectada a internet
ISP's	Proveedores de conectividad IP
J. G.	Juzgado de Garantía
JPG-JPEG	Joint Fhotographic expert Group (Grupo Conjunto de Expertos Fotográficos)
LECrim.	Ley de Enjuiciamiento Criminal
LSSICE	Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico
LO	Ley Orgánica

LOPD	Ley Orgánica de Protección de Datos de Carácter Personal
LGT	Ley General de Telecomunicaciones
MMS	Mediante telefonía móvil
MP3	MP3 Moving Picture Experts Group
MS	Abreviatura de Microsoft
MS-DOS	Microsoft Disk Operating System (Sistema Operativo de Disco de Microsoft)
NASA	National Aeronautics and Space Administration
Núm. / núms.	Número / números
OECD	Organización de Cooperación y Desarrollo Económico
Op. cit.	Obra citada
Pág. / págs.	Página / páginas
PSI	Proveedor de servicios de Internet
P2P	De par a par
RAE	Real Academia Española
RAT	Remote Access Tool
RIT	Rol interno de tribunal
RD	Real Decreto
RDPC	Revista de Derecho Penal y Criminología
Sig. / Sigs.	Siguiente / Siguientes
SMS	(Short Message Service) Servicio de mensajes cortos

STC	Sentencia del Tribunal Constitucional
STCE	Sentencia del Tribunal de Justicia de la Unión Europea
STS	Sentencia del Tribunal Supremo
StGB	Strafgesetzbuch (Código penal alemán)
SCS	Corte Suprema de Justicia de Chile
SCA	Sentencia de Corte de apelaciones
TC	Tribunal Constitucional
TCP	Protocolos de transmisión de control
TICs	Tecnología de la información y la comunicación
TUE	Tratado de la Unión Europea
TFUE	Tratado de Funcionamiento de la Unión Europea
TJCE	Tribunal de Justicia de la Comunidad Europea
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia
t.	Tomo
UNODC	Oficina De Las Naciones Unidas Contra La Droga y El Delito (United Nations on Drugs and Crime)
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones
URL	Localizador de Recursos uniforme (Uniform Resource Locator)

USB	Bus serial universal
VBS	Abreviatura de Visual Basic Script Edition
Vid.	Véase
Vol.	Volumen
WWW.	World Wide Web
§	Parágrafo alemán

INTRODUCCIÓN

Ha surgido una nueva faceta evolutiva de la comunicación humana[1], que se halla en una urgente necesidad de regulación, puesto que como el derecho es un producto de la inteligencia y del espíritu humano, no podemos permitir que el ciberespacio haya sido confiado sólo a su autorregulación, puesto que el derecho no permanece inmóvil, sino que se desarrolla y fluye, entonces se debe propender a que vaya variando según las circunstancias de lugar y tiempo, debiendo el legislador hallar las instancias necesarias para hacerlo, puesto que las condiciones cambiantes de la vida, deben llevar a que se reflejen también en el derecho vigente.

El siguiente estudio investigativo pretende entregar una revisión sintética pero integral sobre los requisitos típicos del *delito informático,* permitiendo al lector tener una visión general, pero no por ello menos exhaustiva de este tipo de ilícito, de manera tal que se pueda obtener un perspectiva acerca de cuáles son sus antecedentes normativos y las implicancias en el mundo jurídico. Como antesala al delito antes dicho, se aborda con una visión global, pero con un análisis claro al día de hoy, sobre las comunicaciones, informática en general y su relación con el

[1] En el nivel internacional, una de las primeras iniciativas en relación con la problemática de la criminalidad informática fue adoptada por la Organización Internacional de Policía Criminal (Interpol), mediante la realización en 1979 de una conferencia internacional en París, Francia. STEIN SCHOJOLBERG, de la policía de Noruega señalaba que: *La naturaleza de los delitos informáticos es internacional debido al incremento de las comunicaciones telefónicas, satelitales, etc. entre diferentes países. Las organizaciones internacionales deben prestar más atención en este aspecto.* SCHJOLBERG, S, *La historia de la armonización global sobre la legislación de delitos informáticos*, En camino a Ginebra., Noviembre de 2015. [accesible en] http://www.cybercrimelaw.

derecho, antecedentes sobre Internet y el ciberespacio, a su vez se incluye en la investigación una explicación actual sobre las normas internacionales que regulan la ciberdelincuencia, y su relación con la Internet profunda y las llamadas monedas electrónicas, análisis que se considera, necesario para abordar uno de los principales retos jurídicos actuales, a saber la aparición de los delitos cometidos, a través de sistemas de cómputos e Internet.

La investigación culmina, ofreciendo de una forma condensada pero integral un análisis sobre el delito de *estafa informática* del artículo 248 N° 2 del Código Penal Español, intentando dar una visión rápida y obtener la información básica sobre el fraude cometido por medio de sistema de computo y sobre el tipo penal especifico, a la luz de la teoría del delito, con una mirada estrecha frente a la legislación foránea, puesto que frente a cualquier opinión doctrinal que se pueda tener acerca del tema, estos ilícitos desbordan la soberanía de los Estados, convirtiéndose en un tema transfronterizo que requiere de la ayuda y colaboración de todos los gobiernos sin distingo alguno, a fin de propender un debate acerca de reglamentar jurídicamente, lo referente al cibercrimen, ciberdelito o delitos informáticos.

Los gobiernos en el último tiempo se han empeñado en tratar de regular el tráfico de información en Internet y por supuesto el comercio, sin embargo las directrices que han regido las transacciones del mercado en forma física es decir de persona a persona, se han vuelto inadecuadas o insuficientes para la interacción electrónica, por ello se ha dicho o planteado que los esfuerzos y las estrategias para imponer la ley, especialmente el Derecho penal, y que han resultado de forma

exitosa en el mundo real, han tenido poco éxito o han sido inadecuadas en el mundo virtual[2].

Las dimensiones de este fenómeno son de tal magnitud que se puede afirmar que se puede comparar con los cambios históricos en cuanto ella se trata como son, la transición de la comunicación oral a la escritura, posteriormente con la invención de la imprenta, nos lleva a la distribución masiva de comunicación escrita, y hoy en día esto se ve exacerbado, con los avances tecnológicos y en especialmente con la creación de *Internet*[3]. Se han superado las barreras naturales y de espacio, que limitaban la comunicación verbal y escrita, teniendo hoy en día la posibilidad de compartir de modo efectivo una unidad de conciencia sobre nuestro mundo. No obstante las grandes posibilidades que existen con el desarrollo de la informática en este sentido y todo los beneficios que con ello trae, la comunicación instantánea en relación con la interacción social y las comunidades virtuales, han sido criticadas por el posible aislamiento social y el quebrantamiento de la comunicación y vida familiar, puesto que hoy en día existe el anonimato, y se están dejando de lado la interacción personal y real con los individuos. Con Internet y las comunicaciones electrónicas, han traído consigo relaciones de alteridad que también pueden

[2] Por ejemplo una compañía de juegos de Internet de un país determinado, donde el juego de azar está legislad, pero mantiene sus ordenadores situados en antigua, donde los casinos de juego no tiene limitaciones o son legales. *Décimo Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente*, Naciones Unidas, Viena, Conferencia 187/5, 2000, pág. 9.

[3] FROSINI Vittorio, *Informática y derecho*, Editorial Temis, Bogotá, 1988, pág 173 y sigs. Además el autor nos dice, que el cambio de mayor significación en la materia lo constituyó el tratamiento electrónico de información y, con ella, su automatización mediante el ordenador, que constituye una prótesis electrónica de la inteligencia humana, por medio de la cual se pueden identificar seleccionar y comparar la informaciones recibidas a una velocidad semejante a la del pensamiento humano. En efecto, la aparición del ordenador, su rápida reducción de tamaño y su vertiginosa difusión ambientar uno nuevo tiempo, en el que el *espacio informático* determinó que la información se convertiría en una novedosa forma de energía, de poder y de producción en la sociedad de nuestros días. Citado por DELPIAZZO, Carlos E, *Del derecho informático al derecho telemático,* En acervo de la biblioteca jurídica virtual, "estudios en homenaje al Dr. Julio TÉLLEZ VALDÉS" UNAM, (documento sin fecha), México, [accesible en] <www.juridicas.unan.mx>.

transformarse en relaciones jurídicas, que pueden tener múltiples consecuencias, y por supuesto en el ámbito delictual, ante este escenario el Derecho y en especial el Derecho penal, deben pronunciarse acerca de estas nuevas relaciones sociales que piden ser reguladas[4].

El desarrollo del protocolo de internet, caracterizado por la apertura, la interfaz[5] y la capacidad de expansión en el mundo virtual, ha logrado almacenar información sobre los individuos a nivel mundial por parte de todas las organizaciones de cualquier tipo, creando con ello un mercado universal de acceso sin límites, usándose dicho mercado virtual tanto para fines lícitos como ilícitos existiendo percepciones distintas respecto de la regulación de internet. Podemos decir entonces, que la gran mayoría de las facetas de la vida humana moderna, están hoy en día dependiendo de la tecnología de la información. Esta ingeniería, mundial seguido perfeccionando cada día siendo uno de los adelantos más importantes de la última década, llegando entonces a todo tipo de necesidad de las personas, puesto que todos los servicios ya sea de obtención de bienes o servicios, de consulta en línea, televisión radio, o necesidades relacionadas con la defensa nacional militar están supeditados a la conexión de la red mundial. Millones de personas utilizan la tecnología satelital, para conectarse en forma instantánea al resto del mundo, teniendo imágenes del momento de lo que sucede en cualquier lugar, existiendo sistemas permanentes de comunicación global, evolucionando constantemente, lo

[4] HERRERA BRAVO, Rodolfo, *Ciberespacio, sociedad y derecho*, En revista chilena derecho informático, U. De Chile, número 3, Santiago de Chile, 2003, pág. 4.

[5] Parte de un programa que permite el flujo de información entre un usuario y la aplicación, o entre la aplicación y otros programas periféricos, constituido por un conjunto de comandos y métodos que permiten estas intercomunicaciones, con ello se logra interactividad entre usuario y ordenador. También podemos hablar de interfaz a partir del hardware, tomando por ejemplo el monitor, teclado y mouse, siendo estos interfaces entre el usuario y el ordenador. Si hablamos de electrónica, un interfaz sería el puerto por el cual se envían o reciben señales desde un sistema hacia otros. (Interfaz no es sinónimo de interface, este último tiene otro significado en biología, física y química.

que trae consecuencias beneficiosas para toda la humanidad pero también consecuencias no esperadas puesto que también se utiliza con fines delictivos. La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder a casi toda la gama de interrogantes que se planteen a los archivos informáticos. Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

La expansión de la tecnología comunicacional parece haber multiplicado la escala cuantitativa de los fraudes mediante el incremento de las oportunidades que ofrecen para acceder cómodamente, incluso sin contacto directo con la víctima, siendo blancos demasiados atractivos para la actividad delictiva, utilizándose la banca electrónica como área de criminalidad preferente de los grupos destinados a realizar fraudes, con manipulaciones informáticas[6].

Las tecnologías de la información y las comunicaciones, han venido cambiando las sociedades en general, permitiendo una mejora de la productividad en las industrias, la revolución de los procesos laborales, y la velocidad y flujo de capitales; no obstante, el agigantado crecimiento, desencadenó nuevas formas de

[6] GABALDÓN GERARDO, Luis, Fraude electrónico y cultura corporativa, Editorial Universidad Federal de Bahía, pág. 197, Caderno CRH [en línea] 2006, (Mayo-Agosto)] Disponible en:<http://www.redalyc.org/articulo.oa>.

delincuencia, ahora orientadas hacia la informática[7]. En efecto, con los avances tecnológicos, devino el incremento desmesurado del cibercrimen, circunstancia que obliga a los Estados a adoptar un marco punitivo con observancia de los lineamientos constitucionales que nutren el Derecho penal vigente, sin alejarnos del principio de *lesividad* y de *última ratio* propios de un sistema penal que se sustenta de un estado de derecho, a fin de enfrentar, prevenir y erradicar la novísima manera de delinquir.

Esta moderna manera de delincuencia, presente por más de dos décadas, es difícil de conceptualizar de manera plena, al implicar la utilización de tecnologías digitales en la comisión del delito; estar dirigida a las propias tecnologías de las comunicaciones; e incluir la utilización de ordenadores para la comisión del delito, ello por cuanto el ciberespacio brinda nuevas herramientas para la comisión de nuevas formas de delitos tradicionales como el robo, el fraude y la pornografía, entre otros, adquiriendo nueva vida y distintas formas a partir de la intermediación de los medios electrónicos. Se habla de piratería de software, distribución de virus y ataque a determinados sitios web, que se originan y tienen existencia únicamente a partir del uso de las máquinas conectadas en la red. Todas estas especialísimas circunstancias han impedido su imputación de manera adecuada, más aun cuando los operadores de justicia, requieren de un entrenamiento especial, por lo que ven frustradas sus posibilidades de persecución al carecer del conocimiento necesario para avocar y adentrarse en este tipo de actividades delincuenciales.

[7] La creciente utilización de la tecnología informática y de las redes informáticas mundiales y de telecomunicaciones como instrumento esencial para las operaciones financieras y bancarias internacionales contemporáneas puede crear asimismo condiciones que facilitan considerablemente la realización de operaciones delictivas dentro de cada país y entre distintos países, permitiendo a la delincuencia organizada tener acceso a la utilización de dichas técnicas para fines tales como el blanqueo de dinero o para la gestión y transferencia de activos adquiridos ilegalmente. ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Informe del Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente*, pág. 149.

Vale indicar que la mirada que se entrega, no pretende ser especializada en este tipo de debates, sobre todo porque la misma requiere de una tecnicidad propia de una carrera universitaria, por ello pretendo reunir, fundir y sistematizar en el presente escrito investigativo, con mediana claridad, aspectos generales del delito informático, internet, algo sobre el cibercrimen actual para aterrizar la investigación en el fraude en la red y más aún con un mayor detalle en la *estafa informática* regulada en el Código Penal Español. Resulta de importancia recalcar el propósito de la tesis doctoral, que no es otro que exponer de manera didáctica las generalidades y prolegómenos que sobre el delito informático han surgido con ocasión de los avances tecnológicos, la globalización y el uso trasfronterizo de información, partiendo de un análisis bibliográfico de obras nacionales y extranjeras, así como de la revisión de bibliografía virtual, vinculándola con las conductas delictivas informáticas, a fin de ilustrar al lector en torno a la peculiar y actual delincuencia generacional, centrando en el fraude.

Con este desarrollo global de las tecnologías informáticas se ha ido gestando formas de criminalidad nunca vistas, que ya no son la base para la trama de una película de ciencia ficción, sino que han pasado a ser una preocupación de todos los países, pudiendo un individuo con los conocimientos adecuados gestar acciones tendientes a sustraer información, defraudar la banca electrónica, suplantar identidad, o realizar espionaje industrial, comportamientos que llevan hacernos preguntas, como por ejemplo; ¿ cómo ingresó a nuestra privacidad ?, ¿quién es?, y ¿dónde está?. Como contrapartida deben existir profesionales, que puedan entender el actuar de dichos individuos, que posean los conocimientos técnicos necesarios, y el manejo de la evidencia a la luz de la legislación interna y transnacional, toda vez que sin ellos los usuarios quedan a la merced de los ataques virtuales.

La globalización, es decir el fenómeno que se caracteriza por la integración económica, social, cultural y racial en este momento de la historia del mundo, está

alcanzando niveles nunca vistos, sin embargo fruto de ella tenemos hoy en día mejora de la calidad de vida del ser humano, sin dejar de mencionar o desconocer que la brecha entre la pobreza y la riqueza de acrecienta, puesto que el capitalismo a pesar de sus beneficios, como son la facultad indudable de la homogeneización, unificación progresiva la sociedad, masificando, tanto capitales y mercados, también dicho sistema económico trae como consecuencia la ampliación de dicha separación social[8].

Por otro lado el desarrollo de la tecnología de la información y de la comunicación, juega un papel fundamental en el desarrollo de la cultura mundial, haciendo mucho más viable la trasmisión de información entre las personas, siendo el procesamiento y almacenamiento casi instantáneo, generando un proceso inmediato de tiempo y espacio, jamás imaginado, algo que en este preciso momento, es imprescindible para el desarrollo del ser humano. El arquetipo de comunicación,

[8] Desde fines de la década de los ochenta, los negocios, principalmente en Occidente, han tenido que reinventarse debido a que las condiciones de entorno han cambiado de una manera fundamental. Teniendo como marco la creciente apertura de los mercados a nivel mundial o globalización, se han producido varios acontecimientos clave que han inducido cambios estructurales. Primero fue la presión competitiva de los tigres asiáticos, que obligó a muchas empresas, como la General Motors e IBM, a replantearse sus negocios para poder competir. Así nació la reingeniería de procesos de negocios como una manera de formalizar la estrategia de cambio de las organizaciones. Después, en la segunda parte de la década de los noventa, cuando todavía no se estabilizaban las reestructuraciones inducidas por la reingeniería, vino la masificación de internet y la aparición de las empresas *punto-com*, cambiando nuevamente las reglas del juego al crear posibilidades inéditas para la realización de los negocios. El caso paradigmático de esto es *Amazon.com*, el cual mostró la viabilidad del nuevo canal de ventas internet. A partir de entonces, muchos productos tradicionales empezaran a entregarse y venderse por empresas en la *Web*, como libros electrónicos, videos, CD, billetes de vuelo, acciones, seguros, capacitación, educación, etc. induciendo a las empresas de la economía tradicional a repensar sus negocios, viéndose éstas obligadas, en muchos casos, a crear el canal de ventas de internet, como complementario a los tradicionales. Pero el impacto más significativo de internet en las empresas de la vieja economía no ha sido la existencia de un nuevo canal de ventas para los productos tradicionales, sino la posibilidad de replantearse los procesos internos del negocio y las relaciones con los proveedores, como también imaginar maneras no tradicionales de entregar servicios a los clientes, que complementen a las habituales. BARROS V. Oscar, *Ingeniería e-business ingeniería de negocios para la economía digital*, Editorial Lom S. A. Santiago de Chile, 2004, pág. 11.

nos entrega la posibilidad de dar servicios que a otrora, sería impensable de esta manera la educación, como la salud, o la misma gestión de la naciones nace en el momento, sin importar el lugar del planeta en que se encuentre las personas que reciben dicho servicio.

El desarrollo increíble, que se aprecia como extremadamente positivo y eficaz para solución de múltiples inconvenientes para el desarrollo mundial, trae como consecuencia, el aumento del riesgo, poniendo a prueba los principios del Derecho penal. Con ello, en esta nueva realidad creada por los hombres nacen inconvenientes frente a los cuales los operadores jurídicos deben abarcar a la hora de analizar y actuar respecto del mundo de la informática jurídica. Al hablar de informática jurídica se estima que es un entorno más propio de las ingenierías y las matemáticas que de las humanidades, por ello muchas veces el legislador al tener que incorporar tipos legales referente a la materia, no se adentra más a fondo en el nuevo ámbito del conocimiento, puesto que al legislar sólo debe existir criterios económicos sino que también sociales, culturales e incluso filosóficos, puesto que de lo que hablamos no sólo es de la regulación de un sector más del acontecer social, sino que hablamos de todo un mundo nuevo, esencialmente dinámico, revolucionario, con sus propios rasgos distintivos de interacción y comportamiento. Ahora bien, en este espacio, se han realizado intentos nacionales e internacionales para poder regularlo, pero han sido totalmente insuficientes, porque a pesar de los múltiples esfuerzos los involucrados ven como los cibernautas, aprovechan esta falta de regulación para actuar de manera ilícita, no pudiendo ser objeto de investigación o sanción alguna.

Así, el actuar de ciertos individuos de la sociedad, que encuentran inmersos en el ciberespacio, con distintas denominaciones como serian por ejemplo hackers y crackers, han tomado comportamientos que pueden ser considerados, por ciertas legislaciones como, como poco adecuados, irregulares o derechamente al margen de la ley, actuares que por distintas razones muchas veces, no pueden ser perseguidos

por la poca regulación o la inexistente regulación, haciendo en esta investigación una aproximación. La normativa internacional que han podido desarrollar los distintos países, o las distintas legislaciones en la lucha contra los delitos informáticos transnacionales, se están abocando a ciertas áreas del mundo informático, donde no existe control y que cada vez más aumenta número de usuarios capaces de ingresar en total anonimato, lo que dificulta aún más la posible persecución de los delitos que se cometan en este medio, existiendo versiones contrapuestas acerca de los derechos en juego, como son la intimidad y el anonimato al momento de navegar por internet en contra posición de la seguridad colectiva.

El naciente campo de la acumulación de sistema de datos, ha generado en el mundo las empresas, tanto públicas como privadas un interés sin precedente, sin embargo ello también recibe delincuente tiene pleno conocimiento de la importancia de toda esta información puesto que lo ataques a los sistema información manipulando y obteniendo claves de acceso se puede realizar con resultados altamente satisfactorios y lucrativos, existiendo probabilidades altísimas de poder tener un fin de lucro ilícito sin ser descubierto. La informática tiene todas las características necesarias, para pueda usarse como medio para cometer delitos, gran cantidad de datos y fácil manipulación.

Por último, según lo razonado anteriormente es necesario entregar una reflexión acerca de la forma en que todos vemos el mundo real en contrapartida del mundo virtual, relacionado directamente como la sucia entiende el mundo que está reglamentado por lo jurídico. Todo esto tiene relación, con la forma en que las personas ven y utilizan la tecnología de la información, puesto que sin necesidad de alguna intrusión previa, o asistencia a cursos programados, toda persona utiliza instintivamente cualquier tipo de programa de cómputo, entendiéndose enviar correos electrónicos, enviar fotografías, o usar la banca electrónica para realizar transacciones diariamente, sumándose ello la exposición desde muy temprana edad a

todos los recursos de multimedia ya la navegación virtual, compitiendo con interacción personalizada, haciendo nebulosa la realidad.

Reflexionando respecto a ello, tan compleja la tecnología de la información, como se dijo anteriormente vinculada a la matemática o a la ciencia, también tan fácil de acceder a ella como se dijo, por ello existe la tendencia por parte de las autoridades que al percibir esta tecnología tan fácil de ser utilizada que también, se estima que no es necesaria explicación suficiente respecto de cómo se cometen este tipo de delitos, utilizando los medios informáticos[9].

De esta manera, antes de comenzar vale ejemplificar una situación cotidiana: si decido ingresar a la oficina de mi profesor guía de tesis, con el fin de sustraer su más reciente obra de derecho penal, ni acción puede ser perfectamente visible, sino tomó los resguardos para que no me sorprendan, por ello, un guardia de seguridad me pueden detener debido a que existiría una flagrancia del delito de robo que acabo de cometer. En este caso no es necesario un peritaje para determinar el valor comercial de la obra sustraída, puesto que sólo basta con determinar el precio con que la obra ha sido vendida en el mercado. Para determinar las consecuencias jurídicas del delito, con estos elementos (flagrancia y valor de la cosa) que son visibles, tangibles, el juez determinará cuál ha sido el delito y mi sanción.

[9] La teoría de la actividad rutinaria (RAT), también puede ofrecer perspectivas de los motores subyacentes del delito cibernético. Según la RAT el riesgo de cometer un delito aumenta con la convergencia de: (i) un perpetrador motivado, (ii) un blanco adecuado, y (iii) la ausencia de un guardián competente. En el caso del delito cibernético, los delincuentes pueden acceder a un gran número de blancos gracias al mayor uso de servicios en línea, como los servicios bancarios, comerciales, y el intercambio de archivos, lo que hace que los usuarios sean vulnerables al fraude y a los ataques mediante phishing. 41 La aparición de redes sociales en línea, como Twitter y Facebook, también ofrece millones de víctimas potenciales de fraude. UNODC (United Nations on Drugs and Crime), Estudio exhautivo sobre le delito cibernético Oficina De Las Naciones Unidas Contra La Droga y El Delito, Naciones Unidas, Nueva York, 2013, pág. 10.

Ahora bien, si traspasamos esta situación hipotética al mundo virtual, donde hoy en día gran parte de las personas permanece desarrollando sus actividades diarias, deberíamos analizarlo de otro punto de vista: si decido ingresar a la oficina en profesor guía de tesis, y realizo la copia de su obra más reciente que se encuentra en su ordenador y la ingreso en mi unidad flash[10], en principio la acción ya no es visible, ya además aparentemente no quedan huellas o rastros de mi ingreso, además la flagrancia sería cuestionada alargándose considerablemente el procedimiento; por otro lado para darle valor a la información que se sustrajo se requerirá entonces un peritaje, tanto para determinar si accedí al ordenador correspondiente, es decir cuando lo hice y como lo dice ya además cuáles son las acciones que realice estando dentro del equipo u ordenador correspondiente, y segundo peritaje para determinar el valor de la información extraída[11].

Así las cosas, ambas conductas son realizadas bajo el mismo tipo penal, es decir robo, pero a pesar que a simple vista se puede pensar una fácil solución, el problema radica en la dificultad, que existe en la segunda conducta, es con el componente de lo tangible y lo intangible. Con este ejemplo podemos decir entonces, que independientemente de la pericia que se realicen para reconocer que tipo de delito y posteriormente la sanción aplicar, existen otros puntos que complejidad más la tarea tanto del legislador como del juzgador, puesto que existen acciones que son reconocidas como delitos, y además en la vida real tendría

[10] Tipo de memoria no volátil que suele ser usadas en celulares, cámaras digitales, reproductores portátiles, discos rígidos, etc. Pueden borrarse y reescribirse. Además permiten que múltiples posiciones de memoria sean escritas o borradas en una misma operación mediante impulsos eléctricos. Por esta razón, este tipo de memorias funcionan a velocidades muy superiores cuando los sistemas emplean lectura y escritura al mismo tiempo. Resistentes al polvo y rasguños y, en teoría, pueden guardar información durante 10 años y permitir hasta 100 mil ciclos de escritura y borrado, siendo los más usados los dispositivos de memoria USB, también llamados pendrive.

[11] MUÑOZ TORRES, Ivonne, Delitos informáticos, diez años después, 1ª edición, Editorial Ubijus, México, pág 3.

características fácil de determinar, pero en el mundo virtual, se debe discernir además del tipo delictivo, a que otras figuras propias de otras ramas del Derecho penal, corresponde el hecho.

CAPÍTULO I

Sobre el Delito informático o ciberdelito

I. Planteamiento

Con la Internet comercial y la expansión de la web aparecen nuevos peligros y amenazas para la seguridad las personas y los sistemas a partir de la multiplicidad de oportunidades tecnológicas que ofrece este medio. En el año 2011, al menos 2.300 millones de personas, el equivalente a más de un tercio de la población total del mundo, tenía acceso a Internet. Más del 60 por ciento de todos los usuarios de Internet se encuentran en países en desarrollo, y el 45 por ciento de todos los usuarios de Internet tienen menos de 25 años de edad. Para el año 2017, se calcula que las suscripciones a banda ancha móvil llegarán al 70 por ciento de la población total del mundo y para el año 2020, el número de dispositivos interconectados por la red (el Internet de los objetos) rebasará a las personas en una proporción de seis a uno, transformando las concepciones actuales de lo que es Internet. En el mundo hiperconectado del mañana, será difícil imaginarse un delito informático, y quizás cualquier otro delito que no involucre evidencia electrónica vinculada con la conectividad del Protocolo de Internet (IP)[12].

El proceso de la tecnología informática ha proporcionado eficaces mecanismos de tratamiento y almacenamiento de datos, al propio tiempo que ha

[12] UNODC (United Nations on Drugs and Crime), Estudio exhautivo sobre le delito cibernético Oficina De Las Naciones Unidas Contra La Droga y El Delito, Naciones Unidas, Nueva York, 2013, pág. 18.

abierto la brecha a nuevas formas de incursión en la esfera jurídica de los ciudadanos, a través de la llamada criminalidad informática, que en un principio estaba limitada a las modalidades delictivas tradicionales como ocurre en el caso de la estafa informática, sin embargo con la sofisticación de dichos delincuentes, se han incrementado las dificultades para la detección de estas conductas y además se ha ampliado el abanico devine jurídicos susceptibles ser dañados[13].

Uno de los fenómenos más novedosos de la nueva tecnología, ha sido la necesidad regula los comportamientos ilícitos en dicho campo, por ello desde hace unas décadas, los estados nacionales y la propia comunidad internacional, como tal, viendo la respuesta punitiva, mediante diversas técnicas jurídicas, a las infracciones consideradas más graves, en relación al derecho informático, de esta manera son tres los instrumentos principales que han abordado la materia a saber, las leyes especiales; introducción de nuevos delitos en el Código penal y las normas internacionales[14].

Para abordar el tema de los delitos informáticos, es de suma importancia delimitar el campo de acción de estas figuras, vale decir definir lo que se entiende por delitos informático, cuales son las conductas, que son constitutivas de los mismos, diferenciándolo de los delitos comunes o de otra especie. El fenómeno de la ciberdelincuencia, no sólo es abordado por los diferentes organismos gubernamentales y fuerzas de seguridad de diferentes países sino también por organismos internacionales, con el objetivo de fortalecer la cooperación entre países y la armonización penal de los delitos informáticos. CAMACHO LOSA, se pregunta *¿y*

[13] ORTS BERENGUER, Enrique / ROIG TORRES, Margarita, *Delitos informáticos y delitos comunes cometidos a través de la informática*, Editorial Tirant lo blanch, Valencia, 2001, pág. 13.

[14] DE URBANO CASTRILLO, Eduardo, *Delincuencia informática, tiempos de cautela y amparo, Las estafas*, Capitulo X, 1ª Edición, Editorial Aranzadi, Pamplona, 2012, pág. 17 y sigs.

por qué la informática habría de ser diferente?, puesto que en todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito, y desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia, allí donde hay hombres, antes o después surge el delito, y si en los primeros tiempos de la informática no se tiene constancia de ningún hecho que pueda ser considerado como punible, quizás sea debido a la escasa difusión de una técnica todavía incipiente y, en consecuencia, al reducido número de personas que trabajaban en ella[15].

Cada vez con más fuerza se incorpora a nuestra vida cotidiana el uso de las nuevas tecnologías, convirtiéndose en algo habitual, no exclusivo de determinadas profesiones. Esto conlleva a la utilización de este nuevo medio para cometer delitos, transformándose en un fenómeno creciente de riesgo y perjuicio[16], quedando muchos tipos penales como insuficientes. Desde esta perspectiva se reflexiona sobre la falta de un concepto único de delitos informáticos; además problemas de interpretación de los tipos penales en relación a las modalidades de fraude; la

[15] CAMACHO LOSA, Luis, *El delito informático*, Editorial Madrid, 1ª edición, Madrid, 1987, pág. 13.

[16] Al respecto manifiesta Rovira Del Canto, "Hemos apuntado el hecho que el desarrollo y expansión de las modernas tecnologías, entre ellas la informática, está estrechamente vinculad a la creciente significación de la información en la sociedad postindustrial. El desarrollo de la sociedad tecnológica se constituye, por tanto, en la segunda mayor influencia en el cambio de perspectivas de la actual evolución social. Durante las últimas dos décadas, los sociólogos y los juristas han estado debatiendo el impacto social de la tecnología moderna, y hasta qué punto determinados cambios de la tecnología general son válidos también en el campo de la tecnología informática, bajo lo que se ha venido denominando como la *Sociedad de Riesgos.* La gran mayoría de la doctrina especialista o no en la materia, ha considerado pues que la criminalidad informática queda comprendida dentro de la compleja problemática propia de una «sociedad de riesgos, y en cuatro ámbitos diferentes de necesitada regulación: la protección de los derechos de la personalidad, la lucha contra la criminalidad económica específicamente relacionada con el procesamiento electrónico de datos, la protección de la propiedad intelectual, y la reforma del proceso penal. ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Editorial Comares, Granada, 2002, pág. 18 y 22.

necesidad o no de un tratamiento autónomo de estos delitos, así como las dificultades de su investigación y prueba. El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, o sabotajes. Sin embargo, debe destacarse las técnicas informáticas delictuales que han creado nuevas posibilidades del uso indebido de los ordenadores lo que ha llevado a la necesidad de regulación por parte del Derecho penal actual.

Este nuevo mundo virtual lleno de datos, que se ha construido a partir del uso de las TICs[17], corre el peligro de ser alterado mediante conductas antisociales y delictivas. Éste fenómeno ha sido advertido por juristas y legisladores, quienes han realizado algunos esfuerzos por establecer los denominados delitos informáticos. En efecto, las conductas antisociales y delictivas que resultan de la implementación de los sistemas de información en la vida cotidiana se traducen en prácticas que dependen del uso de la tecnología, como un medio ideal para su ejecución, dada la vulnerabilidad del control de la información del mismo.

Refiere *Rovira del Canto*, que ya no se puede hablar de la existencia de meros abusos informáticos derivados del uso y utilización de los sistemas informáticos y de telecomunicaciones, sino también de comportamientos ilícitos informáticos derivados de la propia sociedad global del riesgo informático y de la información, y que, en cuanto adquieren la suficiencia entidad y gravedad como para constituir ataques serios a intereses jurídicamente protegidos ilegibles, tradicionales y nuevos,

[17] Tecnología de la Información y Comunicación se encargan del estudio, desarrollo, implementación, almacenamiento y distribución de la información mediante la utilización de *hardware* y *software* como medio de sistema informático. Las tecnologías de la información y la comunicación son una parte de las tecnologías emergentes que habitualmente suelen identificarse con las siglas TIC y que hacen referencia a la utilización de medios informáticos para almacenar, procesar y difundir todo tipo de información o procesos de formación educativa. [accesible en] <http://www.lawebdelprogramador.com>.

que deben ser contrarrestados con medidas que superen los meros ámbitos de la autorregulación, el derecho económico y del derecho civil, requiriendo la intervención del Derecho penal, se constituye en lo que podemos denominar delitos informáticos[18].

El proceso de creación del derecho, a pesar de su complejidad al momento de aplicarlo tomando en consideración las nuevas posturas de la doctrina y la evolución y expansión del Derecho penal, cuando hablamos de crear propiamente tal podemos indicar que es relativamente simple, ya que se basa en una actividad selectiva, puesto que la norma elige situaciones de la vida real y les atribuye una consecuencia jurídica, dicha norma previene los conflictos que se producen en la convivencia, señalando para cada uno de ellos, el interés prevalente, de modo que cada ciudadano sabe a qué atenerse en caso de disputa, por ello mediante normas prohibitivas imperativas el derecho establece en definitiva, quien tiene la razón en cada caso[19].

La aparición y difusión de las nuevas tecnologías en la convivencia diaria de los ciudadanos hace que, en muchas ocasiones, los conceptos jurídicos tradicionales resultan poco idóneos para interpretar las nuevas realidades, resultando que se han utilizado el medio informático como instrumento para la comisión de un delito y la tecnología informática y su programa como bien jurídico a proteger por el Derecho penal puesto que se dice que pocas épocas de nuestra historia han soportado una disociación más radical entre los avances tecnológicos y su consecuente proyección sobre la convivencia social por una parte y, por otra, los conceptos jurídicos destinados a regularlos, por ello mientras la dogmática tradicional ha elaborado

[18] ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Editorial Comares, Granada, 2002, pág. 68.

[19] FLORES PRADA, Ignacio, *Criminalidad informática aspectos sustantivos y procesales*, Editorial Tirant Lo Blanch, Valencia, 2012, pág. 15.

durante siglos conceptos como por ejemplo el acto jurídico sus consecuencias hoy en día la doctrina encuentra dificultad para delimitar los efectos de una voluntad consciente y libre proyectada por sobre un programa informático[20].

Los operadores jurídicos al momento de ingresar al mundo de la informática, el primer obstáculo que deben sobrellevar, es el poco conocimiento que se tiene sobre el área, debido a que, en general, se considera a éste un entorno más propio de las ingenierías y las matemáticas que de las humanidades, puesto que tanto jueces, fiscales, defensores abogados en general, no se enfocan en este ámbito. Es común apreciara en la bibliografía, que existe un tratamiento amplio respecto de las características de los delitos informáticos, y sólo centrándose en su análisis legal, no tomando en consideración sus aspectos propios, en el espacio globalizado, y con relación a los ámbitos sociales, culturales e incluso filosóficos. El estatus jurídico, que se le debe entregar a este tipo de delitos, nos lleva obligadamente a pensar que se hace necesario entregar un estatuto jurídico distinto, que sea eficaz y responda a los cambios vertiginosos de la materia, sin que la misma sea un impedimento para que los delitos de esta clase sean juzgados, adecuándose a la realidad que se transforma día, día, mirando el internet desde un punto jurídico, como el nuevo campo donde juegas los distintos operadores, los que tienen una forma de pensar distinta a lo tradicional, a la cual estamos acostumbrados. No sólo se debe describir las conductas, sino que se debe buscar que es lo que motiva dicha conducta, para así poder entregar, las definiciones coherentes con el delito.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aun cuando no existe una definición con carácter universal,

[20] ÁLVAREZ CIENFUEGOS, José, *Informática y derecho penal. Los delitos relativos a la informática*, 1ª Edición, Editorial Ministerio de Justicia, Secretaría técnica, Centro de publicaciones, Madrid, 1996, pág. 195.

se han formulado conceptos funcionales atendiendo a realidades nacionales concretas. Las innovaciones tecnológicas apoyadas en la informática y las redes de comunicación mundial[21], así como su expansión en la última década, han derivado en un nuevo paradigma sociológico nominado *sociedad de la información o del conocimiento*[22], por ello se habla de una nueva revolución industrial, basada en información que se puede procesar, almacenar, recuperar y comunicar de forma ilimitada independiente del tiempo la distancia, sosteniendo este nuevo sistema social en la prestación de servicios, dejando de lado de alguna manera la economía del capital y el trabajo para ahora hablan de conocimiento teórico[23].

ANARTE BORRALLO, plantea que la exposición de motivos del Convenio Sobre Ciberdelincuencia hace énfasis en la digitalización, la convergencia y la

[21] El ejemplo paradigmático y motor de la sociedad del conocimiento es Internet. Su modelo de red es también la estructura que mejor simboliza esta sociedad. Como dice KEVIN KELLY: "El átomo es el pasado. El símbolo de la ciencia para el siglo próximo es la red dinámica…La red canaliza el poder desordenado de la complejidad...La red es la única estructura que permite un crecimiento sin prejuicios o un aprendizaje sin guía... La red es la organización menos estructurada de la que pueda decirse que tenga estructura. De hecho, una pluralidad de elementos divergentes sólo pueden guardar coherencia en una red. Ninguna otra disposición, como cadena, pirámide, árbol, círculo, cubo, puede contener a la diversidad auténtica funcionando como un todo". MAGALLÓN SANZ, José María, *Sociedad del conocimiento*. En revista de política, cultura y arte, Número 070, Madrid. Julio 2000.

[22] Podemos definir la sociedad del conocimiento como aquélla en que los ciudadanos disponen de un acceso prácticamente ilimitado e inmediato a la información, y en la que ésta, su procesamiento y transmisión actúan como factores decisivos en toda la actividad de los individuos, desde sus relaciones económicas hasta el ocio y la vida pública. La sociedad del conocimiento surge como consecuencia de los cambios que inducen en la sociedad una serie de innovaciones tecnológicas desarrolladas en tres sectores convergentes, como son la informática, las telecomunicaciones y en especial con internet y los medios de comunicación, y algunos autores incluyen además la ingeniería genética. MAGALLÓN SANZ, José María, *Sociedad del conocimiento.* En revista de política, cultura y arte, Número 070, Madrid. Julio 2000.

[23] ANARTE BORRALLO, Enrique, *Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la información,* Derecho y conocimiento, Vol. 1, facultad de derecho, de la Universidad de Huelva, España, 2001, pág. 191.

globalización de redes informáticas[24], y reflexiona acerca de lo indicado en dicho convenio (nota al pie número 7), señalando que se asemeja a ciertos aspectos de la

[24] Suscrito en Budapest el 23 de noviembre de 2001 y auspiciado por el Consejo de Europa: (a) El sistema depende directa e intensamente de tecnologías avanzadas de la información, basadas primordialmente en la automatización y en la digitalización. Con todo, su aplicación no sólo tiene lugar en entornos socioeconómicos *sofisticados*, sino en el ámbito cotidiano e incluso doméstico, lo que permite augurar que los impactos también repercutirán, aunque lógicamente con grados y modos diversos, en casi todas las formas delictivas y en casi todas las instancias y mecanismos del control del delito. (b) Estas tecnologías proporcionan una capacidad *ilimitada* de almacenaje, sistematización y accesibilidad de la información, que se ve acrecentada gracias a conexiones en red, principalmente internet, que permite el acceso a todos los contenidos disponibles en cualquier punto de la red. (c) Esto mismo además posibilita ilimitadas comunicaciones e intercambios de información, que se llevan a cabo de forma relativamente sencilla y descentralizada, por sujetos que actúan con bastante autonomía. En realidad, los intercambios pueden ser de muy diverso tipo: personales, comerciales, académicos, de ocio, etc., en tanto que la naturaleza virtual del sistema los posibilite. (d) Se subraya también que cada sujeto interviniente puede ser, a la vez emisor y receptor de información. Y, asimismo, que en ese sistema de comunicación e intercambio virtual los usuarios actúan, de forma más clara que para el resto de contactos sociales modernos, como sujetos anónimos. Con ello, en la sociedad de la información se realiza de forma paradigmática, uno de los aspectos de la sociedad del riesgo que la dogmática penal funcionalista más ha destacado, su anonimato, una característica que ya la *Escuela de Chicago* identificó, como el rasgo más patético de la existencia metropolitana. De este dato interesa tanto su dimensión individual, en el sentido de que el *ciudadano electrónico* puede aspirar a múltiples contactos sin ser identificado más que por su perfil informático o internauta, como la relativa al control social, en tanto que replantea las posibilidades y medios, a través de los cuales la sociedad y las agencias correspondientes aspiran a ejercerlo. Junto a ello, cabe indicar que también en otros rasgos comunes del patrón de conducta tecnológica -a saber, su virtualidad y su ambigüedad o ambivalencia o la crisis de la teoría de la acción humana, considerada como comportamiento racionalmente conducible- se advierten aspectos que pueden alcanzar especial interés jurídico-penal. En efecto, en la medida en que lo distancian del arquetipo de conducta penalmente relevante, esto es, la conducta comisiva intencional y directamente dañina del bien jurídico protegido individual, parece que se facilita la expansión de modelos de imputación *extraordinaria*, que se basan fundamentalmente en la no evitabilidad y están más cerca de las directrices que rigen las reglas de la autoría mediata, la omisión, la *actio libera in causa* o de la estructura de los delitos de peligro contra bienes jurídicos colectivos, etcétera. (e) Se produce asimismo una estrecha convergencia de las tecnologías informáticas con las telecomunicaciones, que se impulsan mutuamente generando sistemas telemáticos integrados e híbridos. Todo ello en un contexto de renovación muy acelerado. (f) En las caracterizaciones precedentes está ya implícito otro aspecto sustancial de la sociedad de la información: su carácter transnacional o, si se prefiere, global, que relativiza no sólo la significación conductual de las magnitudes espacio tiempo, sino también el valor de las fronteras estatales, jurídicas e incluso culturales. Más aún, como dice RODOTÁ, la globalidad de la red no se refiere solamente al hecho de que se extiende por el planeta entero, realmente hoy es la forma extrema de globalización. (g) Se comprende por todo ello que se destaque la fascinación que rodea a las transformaciones indicadas, que se han convertido en objetivo prioritario del interés socio-económico, político, científico o mediático, etcétera. En ello se realiza la Sociedad de la Información como Sociedad del espectáculo, donde éste también es un producto de consumo. Lo anteriormente analizado explica ANARTE

llamada *sociedad del riesgo,* mencionando lo que lo que indica SILVA SÁNCHEZ[25], en el sentido el mejor ejemplo de lo antes dicho es al ciberdelincuencia pudiendo calificarlo en un contexto sociológico en cuanto a los delitos cibernéticos, como *sociedad global del riesgo* o *sociedad del riego informatizada.* De acuerdo lo anterior, los nacientes *Principios Especiales Del Derecho De Internet,* y su surgimiento como nueva rama del derecho ponen a los estudiosos del Derecho penal, en la necesidad de darle cuerpo a estos principios especiales nuevos, como son el principio de la firma electrónica y el documento electrónico; protección de datos personales; principios atributivo del nombre de dominio; principio de neutralidad de la red; el principio de libre accesibilidad internet y la protección de la privacidad en la misma, entre otros variando según la legislación vigente en cada país y las normas internacionales que regulan la materia[26]. Por otro lado, existen factores que vienen a condicionar la existencia de este nuevo derecho de Internet, como las de índole tecnológica puesto que Internet se encuentra sometida distintas

---

BORRALLO, que se han puesto de manifiesto algunas ideas que evidencia la validez del intento de explicar las claves epistemológica no exenta de contradicciones del llamado Derecho penal de riesgo, relacionado entonces con la respuesta jurídico penal ante la delincuencia propia de la sociedad de la información de además de los postulados político-criminales idiomáticos que invocan los estudiosos del derecho penal del riesgo, para poder seguir desarrollando la posible rama del derecho denominada Derecho penal de la social información. ANARTE BORRALLO, Enrique, *Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la información, Derecho y conocimiento,* Vol. 1, Facultad de derecho, de la Universidad de Huelva, España, 2001, pág. 192. (De esta manera lo que se pretende entonces, es vincular lo indicado por el autor con los nacientes *principios especiales del Derecho de Internet).*

[25] En todo caso, a la vista de lo acontecido en los últimos años, resulta ineludible la puesta en relación de la sensación social de inseguridad frente al delito con el modo de proceder de los medios de comunicación. Estos por un lado, desde la posición privilegiada que ostentan en el seno de la sociedad de la información y en el marco de una concepción del mundo como aldea global, trasmiten una imagen de la realidad en la que lo lejano y lo cercano tienen una presencia casi idéntica en la representación del receptor del mensaje. SILVA SÁNCHEZ, Jesús María, *La expansión del Derecho penal, aspectos de la política criminal en las sociedades postindustriales*, 3ª Edición, Editorial Edisofer, España, 2011, pág. 28.

[26] CANTWELL, Francisco, *Los principios especiales del derecho de internet*, Editorial El Jurista, Santiago de Chile, 2015, pág. 11.

legislaciones que están relacionadas con las telecomunicaciones de cada nación, pero en el caso de la Unión Europea existe normativa que armoniza la regulación de este derecho en dicho territorio, además de ello también debe mencionarse el factor de índole político, puesto que Internet tiene como característica que elimina los límites gráficos del Estado siendo el espacio virtual mundial y por último en necesario señalar el factor de índole jurídico puesto que existen innumerables regulaciones tanto en cada país como a nivel internacional por ello será necesario que se unifique de alguna manera dicha materia y con ello poder hacer frente tanto a las necesidades del comercio, la delincuencia Cibernética[27].

II. Antecedentes históricos

Hace tiempo que ya se inició la etapa de la llamada revolución cibernética, en la que una segunda revolución industrial ha instaurado una nueva filosofía de la tecnología de la organización de trabajo, mediante la creación continua de sistemas automatizados de información y control[28].

En la década de los setenta ya se anunciaba el fin de la vida privada frente al desarrollo de técnicas y herramientas que hicieron posible la comunicación masiva y la vigilancia de las personas a través de dispositivos que implican una intromisión

[27] GARCÍA MEXÍA, Pablo, *Principios de derecho internet*, 2ª edición, Editorial Tirant lo Blanch, Valencia, España, 2005, pág. 188.

[28] MORÓN LERMA, Esther, *Internet y derecho penal: hacking y otras conductas ilícitas en la red*, 2ª edición ampliada, Editorial Aranzadi, Navarra, 2002, pág. 25.

directa en el desarrollo normal de sus vidas[29]. Con el inicio de las comunicaciones utilizando ordenadores o computadoras durante los años 60, diferentes tipos de conductas indebidas o ilícitas comenzaron aparecer entre los usuarios conectados a los centros académicos y laboratorios de investigación de aquel entonces.

Con el internet comercial y la expansión de la web aparecen nuevos peligros y amenazas para la seguridad de las personas y los sistemas a partir de la multiplicidad de oportunidades tecnológicas que ofrece este medio para la comisión de delitos a escala global. Dentro del ámbito estrictamente jurídico, el hecho de que aún subsistan múltiples posturas doctrinales que pretende explicar el fenómeno de la criminalidad informática desde distintas ópticas, ocurre que la postura mayoritaria tradicional tiende a negar la existencia del delito informático como un nuevo delito independiente, sólo aceptando la existencia de una pluralidad de ilícitos con una única nota común, a saber la vinculación con los ordenadores, además tomarle en cuenta como meros delitos tradicionales sólo pensando en que representan más que un nuevo *modus operandi*, debiendo superarse las nociones conceptuales elaboradas

[29] El Juez William Douglas decía ya en 1966 en su voto disidente de la sentencia dada por la Suprema Corte de los Estados Unidos en el caso de Osborn v. United States, que "estamos entrando rápidamente en la era en que no habrá privacidad, en la que todos estarán sujetos a vigilancia todo el tiempo, en la que no existirán secretos para el gobierno. […] Las fichas de todos los ciudadanos aumentan en número y tamaño. Ahora las están pasando a ordenadores de forma tal que por el simple gesto de apretar un botón, todos los miserables, los enfermos, los no populares y las personas de la nación que se aparten de lo uniforme puedan ser instantáneamente identificados. Estos ejemplos demuestran que por todas partes la privacidad y dignidad de nuestros ciudadanos están siendo reducidas, a veces a través de pasos imperceptibles. De forma individual, cada paso puede ser de poca importancia. Pero cuando se ve como un todo, comienza a emerger una sociedad muy diferente a cualquiera que hemos visto una sociedad en la cual el gobierno puede entrometerse en las regiones secretas de la vida del hombre a voluntad. […]"Voto disidente del juez William DOUGLAS. Caso *Osborn v. United States*, 385 U. S. 323, 1966. Este caso se versó sobre el uso de un dispositivo de grabación y las condiciones previas de la vigilancia electrónica ilegal. BARINAS UBIÑAS, Désirée, *El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada*, En revista electrónica de Ciencia Penal y Criminología, número 15-09, 2013, pág. 3, [accesible en], <http://criminet.ugr.es/recpc/15/recpc15-09.pdf>.

de la fecha, como por ejemplo sería la equiparación de la delincuencia informática con la financiera[30].

La tecnología información y de las comunicaciones en las últimas décadas han influido en múltiples ámbitos de la sociedad, trayendo consigo distinta forma de vida de trabajo para todas las personas, puesto que en hoy en día existe un almacenamiento y procesamiento de gran cantidad de información, que trae consigo múltiples beneficios tanto para los gobiernos, economía y las personas en general. Toda la forma de procesar esta gran cantidad de información, trae también consigo distintas afectaciones, teniendo que los legisladores, en forma rápida tener que enfrentar los problemas que afectan el Derecho. Así las cosas los peligros generados, a través del abuso de las nuevas tecnologías principalmente fueron vistos como posibles peligros a los derechos de la personalidad, situación que condujo a diferentes países a que los años 70 las leyes orientaran a la protección de los datos personales, y a partir de dicha década el centro de la discusión de estos delitos, pasó al ámbito económico con contenido informático, variando la situación en los años 80 donde se comenzó a hablar, de *espionaje informático, hacking, difusión de virus informático y piratería del software*[31].

Desde mediados del 80 comenzó en varios países la discusión sobre los problemas procesales-penales presentados en relación con la comisión de estos tipos de delitos y el creciente ingreso de las tecnologías de la información y la comunicación, lo cual originó a su vez reformas dichas materias, con ello en los años 90 se centró la discusión en la criminalidad informática, en torno a la difusión

[30] ROVIRA DEL CANTO, Enrique, *Delincuencia Informática y Fraudes Informáticos*, Editorial Comares, Granada, 2002, pág. 65 y sigs.

[31] MAZUELOS COELLO, Julio, *Modelos de imputación en el Derecho penal informático*, En revista de Derecho Penal y criminología, Vol. 28, número 85, U. de Externado Colombia, 2007, pág. 39.

de contenidos antijurídicos en internet, como son, racistas, pornográficos, o de aspecto violento, naciendo discusiones acerca de si el contenido antes señalado podía o no, ser considerado delito informático[32].

En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE)[33], inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional de las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales. La OECD designó un comité de expertos para discutir el crimen relacionado con los ordenadores y la necesidad de cambios en los códigos penales, con dicho dictamen de esta organización, recomendó a los países miembros la modificación de su legislación penal, de forma que se integraran los nuevos delitos informáticos. Posteriormente el Consejo de Europa emitió recomendación el 13 de septiembre 1989, en la cual se presentó una lista mínima de los delitos que debían necesariamente agregarse a las legislaciones de cada país miembro, junto con una lista opcional. También se llegó a discutir sobre estos temas

[32] SIEBER, Ulrich, Computerkriminalität und informationsstrafrecht Entwicklungen der internationalen Informations- und Risikogesellschaft, in: Computer und Recht, Heft 2/1995, S. 100-113. (La delincuencia informática y el derecho penal de la Información. Desarrollos la información internacional y la sociedad del riesgo, En: Informática y Derecho, Nº 2/1995, pág. 100-113. Nota al pie de, MAZUELOS COELLO, Julio, *Modelos de imputación en el Derecho penal informático*..op. cit. pág. 40.

[33] Se remonta a Europa en ruinas después de la guerra. Decidido a no repetir los errores de sus predecesores en las secuelas de la Primera Guerra Mundial, los líderes europeos se dieron asegurar una paz duradera con la idea de estimular la cooperación y la reconstrucción. La Cooperación Económica Europea (OECE) se estableció en 1948 para administrar el Plan Marshall financiado por los Estados Unidos para reconstruir un continente devastado por la guerra. Al elevar la conciencia de los gobiernos europeos a la interdependencia de sus economías, OECE abrió el camino a una era de cooperación que cambiaría la faz del continente. Con el éxito de la OECE y la posibilidad de extender su trabajo a nivel mundial, Canadá y los Estados Unidos se unieron a sus miembros en la firma del Convenio de la OCDE el 14 de diciembre de 1960. El organización para la Cooperación y el Desarrollo Económico, nació oficialmente 30 de septiembre de 1961, fecha de entrada en vigor de la Convención, agrupa a 35 países miembros y su misión es promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo. [accesible en], <www.oecd.org>.

en el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado de Montreal en 1990, en el Octavo Congreso Criminal de las Naciones Unidas celebrado en el mismo año.

En 1992 la Asociación Internacional de Derecho penal, durante el coloquio celebrado en *Wurzburgo* (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el *principio de subsidiariedad*. En 1996, se estableció por el Comité Europeo para los Problemas de la Delincuencia, un nuevo comité de expertos para que abordaran el tema de los delitos informáticos.

A nivel universal con la irrupción de las nuevas tecnologías de la información nacieron soluciones globales, como son el manual de las Naciones Unidas para la prevención y control de delitos informáticos de 1977[34], el cual viene siendo el antecesor o precedente del convenio sobre si el Cibercrimen aprobado en Budapest en el año 2001[35], y en cuanto a la Unión Europea, y con el movimiento de armonización del derecho penal, se crearon las directivas y decisiones marco tomando un giro más decisivo con la firma del tratado de Lisboa del 13 de diciembre

[34] Estados Unidos de Norteamérica, la primera propuesta de legislar con este respecto, se presentó en 1977 por el senador RIBICOFF en el Congreso Federal.

[35] El veintitrés de noviembre 2001, el Consejo de Ministros de Europa, compuesto por los ministros del interior de los estados que conforman la Unión Europea, conjuntamente con Estados Unidos, Sudáfrica, Canadá y Japón, firmaron en Budapest, la convención sobre delitos informáticos, cuyos objetivos fundamentales fueron los siguientes: armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático; proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas; establecer un régimen dinámico y efectivo de cooperación internacional. CASSOU RUIZ, Jorge, *Delitos informáticos en México*, En revista del Instituto de la judicatura Federal, Número 28, México, 2008, pág. 227.

de 2007, donde se optó por la directiva en vez de por la decisión marco, a fin de conseguir mayor eficacia para avanzar en la armonización de disposiciones relativas a la infracciones con dimensión transfronteriza de especial gravedad, entre las que se encuentra la delincuencia informática.

En cuanto a las leyes especiales para regular la materia, primero que todo se regularon de esta manera en Francia, Gran Bretaña, Estados Unidos de Norteamérica, Holanda, Chile, y Venezuela, pudiendo indicar que en el caso de Latinoamérica la ley chilena data de 1993 y en Europa la ley relativa al fraude informático, de Francia de 1988 y la *computer misuse de 1991, de* Gran Bretaña. En cuanto a introducir delitos nuevos que aborde la criminalidad informática en el Código penal podemos indicar que lo ha hecho España, Portugal, Austria, Italia y en Alemania ha combinado tanto una ley especial la cual es de 1986, (Ley contra la criminalidad económica), agregando artículos a su Código penal que contiene referencia los delitos informáticos, y en el caso de América tenemos que en la misma situación se encuentra Argentina y México[36].

A mayor abundamiento, respecto del anterior en Francia hasta 1988, Australia, Canadá, Estados Unidos de Norteamérica, Inglaterra y Japón soportó, por sancionar determinadas conductas relativas a la actividad informática, sin considerar si tales conductas lesionan o ponen en peligro algún bien jurídico ya protegido por la legislación penal general, como la propiedad, el honor, la intimidad y otros. Después del año 1988[37] en Francia[38], Italia, España, Alemania y Suiza, las figuras penales

[36] DE URBANO CASTRILLO, Eduardo, *Delincuencia informática, tiempos de cautela y amparo, Las estafas*, Capitulo X, 1ª Edición, Editorial Aranzadi, Pamplona, 2012, pág. 18.

[37] De esta manera ocurrió en Francia en el año 1988 con la llamada Ley GODFRAIN; en Italia mediante la Ley 547, de 23 de diciembre de 1993; en España, con el nuevo Código penal de 23 de noviembre de 1995; en Alemania, mediante la segunda ley contra la criminalidad económica, de 15 de mayo de 1986; y Suiza, mediante la ley Federal de 17 de junio de 1994. ÁLVAREZ FORTTE, Héctor, *Los delitos informáticos*, Corpus Iuris, Revista jurídica regional N° 9, Chile, 2009, pág. 104.

relativas informática fueron comprendidos por la vía de introducción de modificaciones en el ordenamiento penal general, de manera tal de abarcar aquellas conductas que, por vía de la informática, podían afectar bienes jurídicos ya protegidos en el ordenamiento penal general. En definitiva, existen dos corrientes respecto del tratamiento de este tipo de delitos, puesto que una corriente postula el tratarlos delito informático como una nueva rama del derecho penal, modelo fenomenológico. Y por otro lado existe la corriente que intenta integrar el tema de los delitos informáticos en el campo ya regulado por el Derecho penal, introduciendo sólo modificaciones o ampliaciones legislativas necesarias en los tipos penales tradicionales, de manera tal de poder comprender en ellos la ejecución de los tipos por medio de mecanismos informáticos. Vale decir la primera corriente se centra en el *fenómeno de la criminalidad* y la segunda en el *bien jurídico protegido*[39].

En el último tiempo, el término denominado globalización ha tenido una tendencia ser entendido y caracterizado por sus éxitos sociales, económicos y políticos sin embargo se ha dejado de lado el otro lado de la moneda en el sentido su efectos negativos, puesto que la globalización ha generado un medio ambiente propicio para formas de delincuencia nuevas y extensas, puesto que la el cambio estructura del comercio y las finanzas y las comunicaciones información han fomentado este medio ambiente en el que el delincuente no sólo está centrado dentro de las fronteras de sus respectivos países sino que por el contrario el medio Internet le ha dado la posibilidad de saltar de una nación a otra sin control.

[38] *Godfrain, Loi, Relative à la fraude informatique,* [accesible en] <http://www.spi.ens>.

[39] ÁLVAREZ FORTTE, Héctor, *Los delitos informáticos*…op. P cit. pág. 106.

Antes, de la reforma de 2010 la regulación de delincuencia informática previsto en el código penal se caracterizaba por la inexistencia de un título específico, y en el Código penal de 1995, no existe un capítulo específico dedicado a los delitos informáticos, por ello no se cuenta con un título propio para un tratamiento especial, existiendo hoy en día una dispersión de normas respecto a los distintos delitos informáticos, encontrándose dispersos en el Código penal como son los artículos 186.197, 211.385.5, 248.2 y 3, 256, etcétera, y es más tampoco están ordenados de acuerdo lo diré jurídicos que protegen[40].

III. Delito informático, acercamiento conceptual

Los primeros inconvenientes que existen al momento de analizar los delitos informáticos es su conceptualización, puesto que no resulta fácil que debe entenderse por delito informático y cuáles son las conductas que pueden considerarse incluidas en el mismo, la doctrina no encontrado un concepto unitario

[40] En el Código Penal español se recogen, como delitos informáticos, los siguientes: artículos 186-189 sobre pornografía infantil; artículo 197.2 sobre espionaje informático; artículo 211 so injurie calumnias a través de la red; artículo 385.5 sobre robo utilizando sistemas de guarda criptográfica; artículo 248.2 sobre estafa informática; el artículo 256 sobre ubicación abusiva de equipos terminales de telecomunicaciones; artículo 264.2 sobre sabotaje o daños informáticos; artículo 270 sobre propiedad intelectual; artículos 273-275 sobre delitos contra la propiedad industrial; artículo 278.1 sobre secreto de empresa; artículo 286 sobre uso ilegal de equipos, programas y servicios informáticos; artículo 402 sobre usurpación de funciones públicas por correos electrónicos; artículos 417-418 y 423 sobre infidelidad en la custodia de documentos y violación de secretos; artículo 560.1 sobre ataques a líneas o instalaciones de telecomunicaciones o correspondencia postal y artículos 598 y 603 sobre descubrimiento y revelación de secretos relativos a la defensa nacional. DE URBANO CASTRILLO, Eduardo, *Delincuencia informática, tiempos de cautela y amparo, Las estafas*, Capitulo X, 1ª Edición, Editorial Aranzadi, Pamplona, 2012, pág. 20. Código Penal y Leyes penales especiales, 18ª Edición, Editorial Aranzadi, (concordado por, VALLE MUÑIZ José), Pamplona, 2012, 87 y sigs.

delito informático y existen muchas discrepancias en torno a ello, afirmando algunos que no puede existir una definición del mismo.

Determinar que se entiende por criminalidad informática y concretamente por delito informático no es una tarea sencilla, sobre todo si se tiene en cuenta que ambas expresiones no han sido aceptadas en general por la doctrina, más aún si el término delito informático resulta problemático a pesar que se utilizado con frecuencia tanto por la jurisprudencia como la doctrina[41]. Ahora bien, ante imposibilidad de alcanzar un concepto jurídico-penal, preciso, en vez de hablar de delito informático, existe la tendencia a referirse como *delincuencia informática*, expresión más adecuada para identificar un objeto relativamente impreciso[42]. En el mismo sentido ROMEO CASANOVA, indica que la caracterización, tanto criminológica como dogmática, de los delito informático no es sencilla, pues estos mismos han experimentado una evolución y, hasta cierto punto, transformación, por ello son diversos los problema jurídico-penales que se han ido planteando, puesto que con la expresión delitos informáticos antes solía indicarse que se refería a una pluralidad de conductas[43].

Para desarrollar la definición de este tipo de delitos en necesario primero que todo, realizar una diferenciación de manera tal de poder distinguirlos de otros delitos

[41] ALASTUEY DOBÓN, Mª Carmen, *Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial,* Informática y Derecho (director) CARRASCOSA LÓPEZ, Valentín, Área De Derecho Penal, Facultad De Derecho De La Universidad Zaragoza, Editorial Aranzadi, España, 1994, pág, 453.

[42] ANARTE BORRALLO, Enrique, *Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información*, En revista de Derecho y conocimiento, Vol. 1, facultad de derecho, de la Universidad de Huelva, España, 2001, pág. 198.

[43] ROMEO CASABONA, Carlos M, *De los delitos informáticos al cibercrimen*. En El Cibercrimen, nuevos retos jurídicos-penales, nuevas respuestas Político-Criminales, Editorial Comares S. L., Granada, 2006, pág. 5.

que no son parte del ámbito de la informática[44]. Así, de esta manera es necesario recalcar, que este tipo de delitos se cometen con una máquina, *el ordenador*, siendo el instrumento primordial para cometer estos ilícitos, debiendo hacer presente la distinción, que el instrumento mencionado se puede utilizar para cometer delitos tradicionales, utilizándolo como herramienta o aprovechándose del mismo. No estamos en presencia de un delito informático, cuando se descerraja o abre un dispensador de dinero automático, o cuando se toma parte de un ordenador y se utiliza como elemento contundente para atacar a una persona causándole lesiones, estos son delitos comunes.

El fenómeno de la cibercriminalidad no sólo es abordado por los diferentes organismos gubernamentales y fuerzas de seguridad de diferentes países, sino también por organismos internacionales, con el objetivo de fortalecer la cooperación entre países y la armonización penal de los *delitos informáticos*. Cada vez con más fuerza se incorpora a nuestra vida cotidiana el uso de las nuevas tecnologías, convirtiéndose en algo habitual, no exclusivo de determinados profesiones. Esto

[44] Con la expresión delitos informáticos, existía pluralidad de conductas según la doctrina de hace algunos años, es decir las que forma grave atentan a determinados bienes de titularidad individual, tanto personas físicas como jurídicas, referente a una actividad informática específica exclusiva y además telemática, señalándolos como una tipología técnico criminológica, la cual es de acceso, alteración, ocultación o destrucción no autorizados o no consentido de los datos almacenados en un sistema informático. Además la reproducción completo parcial de datos contenidos en un sistema informático, así como la distribución o comercialización de los mismos. Antes de las reformas del Código Penal español referente a la materia, se incluían también utilización ilegítima de equipos y redes informáticas o telemáticas. Por otro lado, los elementos y sistemas se entendían como un mero instrumento, sin embargo la figura de este tipo de delito es su peculiaridad con misiva, la cual es su elevada agresividad multiplicadora de efectos lesivos. En estos últimos estaríamos en presencia de delitos contra la intimidad y los datos de carácter personal y también podrían incluirse algunos delitos contra el patrimonio como sería el fraude informático ya la vez los daños. Igualmente existía conductas donde la agresión se dirigía hacia el *software* o el *hardware.* Por ello con tan variada manifestación delictiva, la legislación anterior era muy limitada sin embargo los autores en ese momento los llamaban delitos informáticos en general, hoy en día habría que distinguir el Ciberdelito y el cibercrimen. ROMEO CASABONA, Carlos M, *De los delitos informáticos al cibercrimen*. En El Cibercrimen, nuevos retos jurídicos-penales, nuevas respuestas Político-Criminales, Editorial Comares S. L., Granada, 2006, pág. 6.

conlleva la utilización de este nuevo medio para cometer delitos, transformándose en un fenómeno creciente de riesgo y perjuicio, quedando muchos tipos penales como insuficientes. Desde esta perspectiva se reflexiona sobre la falta de un concepto único de delitos informáticos, los problemas de interpretación de los tipos penales, la necesidad o no de un tratamiento autónomo de estos delitos, así como las dificultades de su investigación y prueba.[45]

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho. Este nuevo mundo virtual lleno de datos, que se ha construido a partir del uso de las TICs, corre el peligro de ser alterado mediante conductas antisociales y delictivas. Éste fenómeno ha sido advertido por juristas y legisladores quienes, han realizado algunos esfuerzos por establecer los denominados delitos informáticos. [46]

En efecto, las conductas antisociales y delictivas que resultan de la implementación de los sistemas de información en la vida cotidiana se traducen en prácticas que dependen del uso de la tecnología, como un medio ideal para su ejecución, dada la vulnerabilidad del control de la información del mismo. Con el inicio de las comunicaciones mediadas por computadoras durante los años 60, diferentes tipos de conductas indebidas o ilícitas comenzaron a aparecer entre los usuarios conectados a los centros académicos y laboratorios de investigación de

[45] ADÁN DEL RIO, Carmen, *La persecución y sanción de los delitos informáticos*, En revista Española Eguzkilore, Número 20, San Sebastián, 2006, pág. 151.

[46] NANDO, LEFORT, Víctor, *El lavado de dinero, nuevo problema para el campo jurídico,* 2ª edición Editorial Trillas, México, 1999, pág. 96.

aquel entonces. La Organización de Cooperación y Desarrollo Económico promovió recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, puesto que con internet comercial y la expansión de la *web* aparecen nuevos peligros y amenazas para la seguridad de las personas y los sistemas a partir de la multiplicidad de oportunidades tecnológicas que ofrece este medio para la comisión de delitos a escala global.

A) Aclaración del concepto

Terminando los años 80, algunos autores con el avance las tecnologías comenzaron a utilizar la definición de delito informático, cuya denominación importada del término anglosajón *computer crime*[47], a pesar que el Código Penal español no menciona ningún tipo de delito en materia tecnológica o informática, sin embargo la expresión fue muy criticada y abandonada puesto que autores como *Correa* en Italia o *Tiedemann* en Alemania[48], comenzaron a conceptualizarla de

[47] Agrega GUTIÉRREZ FRANCÉS, que la literatura de la lengua española, se ha venido imponiendo la expresión delito informático, fórmula sencilla y de gran arraigo en el lenguaje coloquial, con la que se ha pretendido traducir, sin circunloquios, la también como depresión anglosajona *computer crime*, y que a pesar de las ventajas del término y su indudable plasticidad, hemos de reconocer, no obstante, que desde un punto de vista técnico no resulta muy afortunado. GUTIÉRREZ FRANCÉS, María Luz, *Fraude informático y estafa*, 1ª Edición, Editorial Ministerio de Justicia, Secretaría técnica, Centro de publicaciones, Madrid, 1996, pág. 51.

[48] BARRIO ANDRÉS, Moisés. *El régimen jurídico de los delitos cometidos en internet en el derecho español tras la reforma penal de 2010*, En Delincuencia informática, Tiempos de cautela y amparo, Editorial Thomson Reuters Aranzadi, Navarra, 2012, pág. 33.

acuerdo al bien jurídico protegido de la legislación naciente respecto a la materia[49]. A su vez ROMEO CASANOVA, refiere que con la expresión delitos informáticos, suele aludirse a conductas que atentan de forma grave a determinados bienes del individuo, pero también de persona jurídica que presentan una configuración específica y exclusiva de la actividad informática y telemática, una tipología técnico-criminológica, que se caracteriza por acceso, alteración, ocultación o destrucción no autorizados de los datos almacenados en un sistema informático; reproducción completo parcial de datos contenidos en un sistema informático; creación de un fichero clandestino; venta de ficheros informáticos; sustracción del tiempo de sistemas informáticos o telemáticos, etcétera, por ello el autor demuestra varios supuestos en que los instrumentos para cometer los hechos son castigados por el Código Penal , sin embargo tiene que tomarse en consideración la característica principal del delito es decir la forma con misiva, por ello también menciona los delitos contra la intimidad y patrimonio, donde el último estaríamos en presencia el fraude informático o otras conductas en el que el bien jurídico agredido sería por ejemplo el software o el hardware, por ello no sería exacta la referencia un supuesto *delito informático*, puesto que debe existir la especialidad que exige el tipo, por ende los medios con mis hijos el bien jurídico protegido nos lleva a entender los delito

[49] CAMACHO LOSA, en 1987 ya explicaba las debilidades de referirse al delito informático, sin hacer distinciones respecto al tipo de ilícito. "En una primera aproximación podríamos definir el delito informático como toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata la víctima, en cuya comisión interviene necesariamente de forma activa dispositivos habitualmente utilizados en las ideas informáticas. No considero que deban incluirse dentro de este concepto aquellos hechos en los que los dispositivos informáticos son objeto de un delito de los tipificados en el Código Penal, como en el caso de la sustracción de material hardware, ya que este tipo de hechos no reúne las características diferenciadoras del delito informático, y su relación con la informática es un mero accidente. CAMACHO LOSA, Luis, *El delito informático*, Editorial Madrid, 1ª edición, Madrid, 1987, pág. 25.

informático como una pluralidad de ellos y no sólo uno[50]. A pesar que con la expresión delito informático, podemos encontrar varias ventajas como sería la flexibilidad del mismo concepto para adaptarse las distintas técnicas de delincuencia informática, desde un punto de vista técnico no es preciso, puesto que el sustantivo delito tiene una significación específica para la doctrina que estudia el Derecho penal, independientemente de las distintas posiciones que cada uno de los autores toma respecto de la teoría del delito, por ello para que una conducta sea técnicamente un delito al menos se necesita la tipificación en la ley penal vigente y además el ámbito de la informática es demasiado complejo como para englobar todas las conductas que existen con un solo término llamado delito informático, es una pluralidad de delitos[51].

1. Delito cibernético

La Real Academia Española, entrega la definición de *cibernética*[52], como el estudio de las analogías entre los sistemas de control y comunicación de los seres

[50] ROMEO CASANOVA, Carlos, *Delitos informáticos*, En enciclopedia Penal básica, (director) LUZÓN PEÑA, Diego, Editorial Comares, Granada, 2002, pág. 518.

[51] GUTIÉRREZ FRANCÉS, María Luz, *Fraude informático y estafa*, 1ª Edición, Editorial Ministerio de Justicia, Secretaría técnica, Centro de publicaciones, Madrid, 1996, pág. 52.

[52] La palabra Cibernética proviene del griego *kibernetes* y significa piloto o el arte de pilotear un navío. MATEOS, MUÑOZ, Agustín, *Compendio de etimologías Greco- Latinas del Español*, Editorial Esfinge, Cuadragésima sexta edición, México, 2007, pág. 299.

vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología[53].

De acuerdo lo anterior se puede indicar que *delito cibernético*, se refiere al que tipifica acciones que realiza una persona similares a aquellas que lleva a cabo una máquina, podemos decir entonces que la cibernética se refiere a una comparación que se realiza entre las funciones de comunicación similares entre humanos y máquinas, por ende estaríamos en presencia de cualquier acto del ser humano que se realiza en forma ilegal y que tiene por fin afectar las comunicaciones transmitidas a través de las tecnologías de la información y comunicación. De acuerdo lo anterior no existiría una categoría autónoma de delito cibernético, puesto que el código Penal español de 1995 no introducido este tipo de delito llamándolo de esa forma, puesto que si se argumenta en forma contraria estaríamos creando una nueva categoría que no existe, por ello es más propio referirse a delincuencia informática.

Ahora bien, desde el punto de vista de la legislación española podemos ejemplificar lo anterior con un ataque de denegación de servicios DDoS (siglas en inglés Distributed Denial of Service), ataque distribuido denegación de servicio, es decir que se ataca al servidor desde muchos ordenadores para que deje de funcionar. Teniendo la vista la redacción del *artículo 264 del Código Penal*[54], se puede

[53] Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa calpe, Madrid, 2005, pág. 546.

[54] Articulo 264 Código Penal: 1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, o programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años. 2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años. 3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso,

englobar los casos de denegación o servicios en dicho artículo, puesto que al suponer el resultado la interrupción del funcionamiento de un sistema informático ajeno, que deja asimismo inaccesible los dato informáticos que el mismo sistema contiene.

2. Delito electrónico

La Real Academia Española, indica que *electrónica* es el estudio y aplicación del comportamiento de los electrones en diversos medios, como el vacío, de los gases y los semiconductores, sometidos a la acción de los campos eléctricos y magnéticos[55]. Por otro lado, el mismo diccionario nos dice que se entiende por *fotones* e indica cada una de las partículas que, según la física cuántica, constituyen la luz y, en general, la radiación electromagnética[56]. Al referirnos a esta definición podemos tomar estos dos conceptos para poder saber a qué se refiere el delito electrónico, y para ello vale señalar que los fotones antes referidos son las partículas

---

la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: 1º. Se hubiese cometido en el marco de una organización criminal. 2º. Haya ocasionado daños de especial gravedad o afectado a los intereses generales. 4. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrán las siguientes penas: a) Multa del doble al cuádruple del perjuicio causado, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años. b) Multa del doble al triple del perjuicio causado, en el resto de los casos. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33. VALLE MUÑIZ, José Manuel, *Código penal y Leyes penales especiales*, 18° edic., Editorial Thomson Reuters Aranzadi, Pamplona, 2012, pág. 178.

[55] Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa calpe, Madrid, 2005, pág. 871.

[56] Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa calpe, Madrid, 2005, pág. 1082.

elementales que son responsables de portar todas las formas de radiación electromagnética, y por ende generan impulsos eléctricos, lo que lleva a *transmitir señales* entre los mismos, generando lo que nos interesa en este concepto, lo cual es el *flujo de información entre los sistemas*[57].

De acuerdo a lo anteriormente analizado el *delito electrónico* puede definirse como aquel que se caracteriza por cualquier acto humano con contenido ilegal cuando mismo acto se realiza con el fin de perturbar el flujo electrónico de datos, afectando con ello el normal funcionamiento de internet, como también de los sistemas de información su funcionamiento y desarrollo.

Desde el punto de vista de la legislación española, podemos ejemplificar un delito electrónico como en el caso de un ataque que se lleva a cabo en contra de las instalaciones físicas de las cuales depende una red de telecomunicaciones. Ahora bien, brevemente podemos indagar si el ejemplo anterior se encuadra en la hipótesis del artículo 264.2 del Código Penal español[58], sin embargo el artículo al señalar *cualquier medio*, se ha dicho que se incurre en un error puesto que no podemos hablar sólo de cualquier medio, puesto que tiene que ser un medio idóneo, para producir lo que exige la norma cuyo resultado sea grave, además el término

[57] Al respecto la autora hace la misma unión de conceptos, he indica que al conjuntar estas dos acepciones se puede establecer lo que se entiende por delito electrónico. MUÑOZ TORRES, Ivonne, *Delitos informáticos, diez años después*, 1ª edición, Editorial Ubijus, México, 2009, pág. 15.

[58] Artículo 264 Código Penal: 2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años. Modificado por LO 15/2003. Nuevamente reformado por LO 5/2010 y renumerando el único párrafo anterior y añadiendo el apartado 2. VALLE MUÑIZ, José Manuel, Código penal y Leyes penales especiales, 18° edición, Editorial Thomson Reuters Aranzadi, Pamplona, 2012, pág. 178.

cualquier medio, limita la obstaculización o la introducción, que sólo podrá ser introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos. Por ello se dicho que lo que se castiga principalmente, es al que cometiendo las acciones del artículo 264.1 del Código Penal, además, interrumpa u obstaculice un sistema informático, con el requisito de doble gravedad, por ello tomando en consideración lo que indica el artículo 264.1, en el cual es posible producir daños sobre datos, programas informáticos o documentos electrónicos, desarrollado dicho ataque directo al hardware, donde estaban contenidos esos datos, se puede deducir que la interrupción u obstaculización pueden llevarse a cabo por medios físicos o ataques físicos al sistema informático, y por ello dichos daños como consecuencia producen la interrupción u obstaculización del sistema informático general. Por último vale indicar que el daño del artículo 264.2 puede ser un daño no tangible el llamado *daño funcional* y no valorable económicamente, lo que no obsta para entender cometido el ataque a la propiedad del sistema o programa informático, pero la amplitud que se deriva del tenor literal debe ser moderada razonablemente, al menos en la aplicación del tipo agravado, puesto que el tipo penal no requiere la producción de un perjuicio económicamente evaluable por lo que se concibe básicamente como un delito contra la libertad de disposición de su titular. Es posible concebir un daño sobre una cosa inmaterial aunque no sea económicamente evaluable con tal, que lesione el poder de disposición inherente al derecho de propiedad[59].

[59] CHOCLÁN MONTALVO, José, *Delincuencia Informática, Problemas de responsabilidad, Infracciones patrimoniales en los procesos de transferencia de datos*, (director) MORALES GARCÍA, Oscar, Cuadernos de Derecho Judicial IX-2002, Consejo General del Poder Judicial, Madrid, 2002, pág. 277.

3. Delito telemático

La Real Academia Española, indica que *telemática*[60], es la aplicación de las técnicas de la telecomunicación y de la informática a la transmisión de información computarizada[61]. Basándose en lo anterior, el *delito telemático,* podría definirse como cualquier acto del hombre que encuentre destinado o realizado con el fin de perturbar las telecomunicaciones o las tecnologías de la información, cuya consecuencia sea la interrupción de la trasmisión de información que esté depositada en un sistema de información[62].

En la exposición de motivos de la reforma 5 /2010, expone en relación al artículo 264 del Código penal, que la acción típica existe en dos ámbitos claramente diferenciados, siendo el primero el de la información y el segundo el de los sistemas, ambos informáticos considerando entonces el legislador, más grave el segundo. En lo que respecta a la definición estudiada de delito telemático podemos subsumir en lo que respecta a los sistemas las situaciones en las que la alteración no recae la

[60] La palabra «telemática» proviene de la fusión de los términos *telecomunicación* e *informática*. También es usado en ocasiones el término *teleinformática*, término que nació en la disciplina de telecomunicación para designar el control remoto de sistemas informáticos, aunque no describe la telemática como tal. El término telemática se acuñó en Francia (*télématique*). En 1976, en un informe encargado por el presidente francés Aléry GISCARD D´ESTAING, al inspector general de Finanzas en 1976, Simón Nora el cual elaboró junto a Alain MINC (conocido como informe Nora-Minc y distribuido por el título: Informatización de la Sociedad), en el que se daba una visión increíblemente precisa de la evolución tecnológica futura. NORA, Simón / Alain, MINC, *La informatización de la sociedad*, Fondo de Cultura Económica, México, 1982, pág. 17.

[61] Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa calpe, Madrid, 2005, pág. 2148.

[62] Al respecto la autora hace alusión al concepto de telemática que entrega la RAE, el cual no se encuentra en desuso y que es probablemente idóneo al tema en análisis puesto que involucra las tecnologías de la información y las telecomunicaciones. MUÑOZ TORRES, Ivonne, *Delitos informáticos, diez años después*, 1ª edición, Editorial Ubijus, México, 2009, pág. 17.

información, sino en el sistema que lo soporta, como las que impiden de forma normal o temporal su utilización, por ejemplo el bloqueo de servidores o páginas web, o también el envío masivo de mensajes de correo electrónico con el objeto de proteger el sistema[63].

4. Delitos computacionales

La Real Academia de la lengua española refiere que *computacional*[64], es dicho de un estudio o de un proceso, que se adapta ser tratado mediante, computador. A su vez, el mismo diccionario nos entrega la definición de *computador*[65], señalando que es una máquina electrónica, analógica o digital, dotada de una memoria de gran capacidad y de método de tratamiento de la información, capaz de resolver problemas matemáticos y lógicos mediante la utilización

[63] Distingue al respecto GONZÁLEZ RUS, como expresión sino anima se ha utilizado *sabotaje informático*, y que empleado en ocasiones anteriores, y que MATELLANES RODRÍGUEZ, califica como tal la destrucción o inutilización del soporte lógico, esto es, de datos o programas contenidos en un ordenador, lo que confirma la identidad de contenido y sentido que se asigna a ambas denominaciones. Entendidos así, pues, no constituye sabotaje informático la destrucción de elementos físicos de un equipo informático en los que no se contienen datos (monitor, impresoras, disco almacenamiento vacío, etcétera), ni tampoco, en rigor, la simple alteración del funcionamiento el sistema informático que afecta el procesamiento de la información, pero que se produce afectando únicamente los elementos físicos del equipo y con el fin de impedir la o dificultar la, inutilización de un microprocesador, que imposibilita o ralentiza el tratamiento del información, deterioro de la memoria RAM etcétera. GONZÁLEZ RUS, *Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (artículo 264.2 del Código Penal)*, En la ciencia del derecho penal ante el nuevo siglo, 1ª edición, Editorial Tecnos, Madrid, 2003, pág. 1282.

[64] Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa Calpe, Madrid, 2005, pág. 608.

[65] Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa Calpe, Madrid, 2005, pág. 609.

automática de programas informáticos. Es dable se presente que el diccionario de la Real Academia de lengua, al referirse a la palabra *ordenador*, concepto utilizado en España y otros países para referirse al computador, dicho diccionario nos entrega una definición del mismo casi idéntica[66].

Entonces al tomar en cuenta los conceptos antes indicados, se tiene que tener en consideración primero que todo que lo principal es una computadora u ordenador. Además de ello debemos tomar en consideración lo que se entiende por *sistema de información,* el cual se define como aquel generalmente automatizado, que tiene por finalidad exclusiva y excluyente el almacenamiento, el procesamiento, la recuperación y la difusión de la información contenida en documentos de cualquier especie[67]. Es así, que el sistema de información cuenta con cuatro características principales, a saber entrada de datos, procesamiento de datos, almacenamiento de datos y salida de datos, todos ellos bajo el supuesto de cálculos matemáticos que procesa la computadora u ordenador.[68]

Podemos definir entonces, *delito computacional*, que tipifica cualquier acto humano como ilegal, cuando dicho acto tiene o ha tenido por fin atacar, perturbar o afectar cualquier operación de una computadora u ordenador, el cual trae como consecuencias, la introducción o afectación de cualquiera de las fases o etapas del procesamiento de datos.

---

[66] *Ordenador:* máquina electrónica dotada de una memoria de gran capacidad y de métodos de tratamiento de información, capaz de resolver problemas aritméticos ilógicos gracias a la utilización automática de programas registrados en ella. Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa Calpe, Madrid, 2005, pág. 1628.

[67] Asimismo se definen como junto u ordenación de elementos organizados para llevar a cabo algún método, procedimiento o control mediante el proceso de información. Diccionario informático, [accesible en], <http://www.lawebdelprogramador.com>.

[68] MUÑOZ TORRES, Ivonne, *Delitos informáticos*…op. cit., pág. 16.

5. Delito informático

Según se ha venido estudiando el tema, existen variados elementos que se conjugan entre sí, para entregar una definición general de delito informático, pudiendo nombrar de modo general, el bien informático en sí, que, visto forma física, será el ordenador o un servidor; los datos contenidos en un repositorio[6970], y la información en sí misma[71]. Ahora bien, vale señalar que lo que le entrega valor a un repositorio no son los datos en sí, sino la forma en que éstos son procesados y que en consecuencia proveen valor[72].

Es necesario, dar a conocer tres conceptos que son de relevancia para poder construir una definición de delito informático, esto es *datos*, *información* e *informática.* La Real Academia Española define *información*, como la comunicación

[69] Es un término utilizado en el dominio de las herramientas CASE. El repositorio podría definirse como la base de datos fundamental para el diseño; no sólo guarda datos, sino también algoritmos de diseño y, en general, elementos software necesarios para el trabajo de programación. Diccionario informático [accesible en] <http://www.lawebdelprogramador.com>.

[70] CASE: (Computer Aided Software Engineering). Bajo el término de Ingeniería de Software Asistida por Ordenador se incluyen una serie de herramientas, lenguajes y técnicas de programación que permiten la generación de aplicaciones de manera semiautomática. Las herramientas CASE liberan al programador de parte de su trabajo y aumentan la calidad del programa a la vez que disminuyen sus posibles errores. Diccionario informático [accesible en] <http://www.lawebdelprogramador.com>.

[71] MUÑOZ TORRES, Ivonne, *Delitos informáticos…*op. cit. pág. 18.

[72] Directamente relacionado, y para ver, *knowledge* (Base de Conocimiento). En el mundo de la informática, consiste en una base de datos de temas relacionados con un sistema informático concreto, hardware o software, en la cual se encuentran los problemas más comunes y sus soluciones, metodologías para trabajar con el sistema y respuestas a las preguntas que más frecuentemente se hacen los usuarios. Diccionario informático, (como en nota 49).

o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada[73].

Del mismo modo, la Real Academia Española, define *informática* como el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores[74]. Y por otro lado, la Real Academia Española indica que *dato* Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho; información dispuesta de manera adecuada para su tratamiento por un ordenador[75].

Teniendo definidos entonces, estos tres conceptos podríamos definir el delito informático, *como aquel que tipifica cualquier acto del ser humano como ilícito, cuando el mismo tiene por fin perturbar o afectar datos, información o sistemas de información teniendo como consecuencia el daño directo o indirecto en ellos, así como también el mal uso de los mismos.*

Para concluir, es dable señalar que la dogmática penal actual se incluye un concepto de delito informático tanto el delito tradicional cometió a través de ordenador o Internet, como el propiamente tal, es decir el que ataca los datos o sistemas informáticos o las vías telemáticas de comunicación, usando preferentemente Internet, con el fin de bloquear sistemas, destruyendo programas, dañando dispositivos de almacenamiento, alterando datos, destruyendo datos o usándolos en forma ilícita. Siendo esto un concepto meramente instrumental, que

[73] Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa calpe, Madrid, 2005, pág. 1274.

[74] Diccionario De La Lengua Española…op. cit. pág. 1274.

[75] Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa Calpe, Madrid, 2005, pág. 728.

engloba entonces toda la actividad ilícita desarrollada a través de las nuevas tecnologías[76].

6. Ciberdelito o cibercrimen

Hoy en día la doctrina ha comenzado a prescindir del término delito informático, para sustituirlo por otro como por ejemplo ciberdelito o cibercriminalidad. Podemos definir *cibercrimen,* como aquella conducta relativa al acceso, apropiación intercambio y puesta a disposición de información en red telemática, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar al bien jurídico diversa naturaleza individual o supraindividual.

La anterior definición entregada por ROMEO CASABONA, tiene características generales, a saber la difusión de contenidos ilícitos; el acceso, alteración u obstrucción de sistemas y bases de datos ajenos, cualquiera que sea su estructura y contenido; los ataques a diversos objetos de la propiedad intelectual; delitos convencionales en los que la red constituye el factor más relevante para facilitar la comisión de reiteración instantánea sucesiva del hecho[77].

El diccionario de la Real Academia Española, no definió la palabra cibercrimen, pero si se refiere a la palabra *crimen*, y la define como acción indebida

[76] VELASCO NÚÑEZ, Eloy, *Delitos cometidos a través de internet, cuestiones procesales,* 1ª edición, Editorial La Ley, Madrid, 2010, pág. 41.

[77] ROMEO CASABONA, Carlos M, *De los delitos informáticos al cibercrimen,* El Cibercrimen, nuevos retos jurídicos-penales, nuevas respuestas Político-Criminales, Editorial Comares S. L., Granada, 2006, pág. 9.

o reprensible[78]. A su vez, la expresión *ciber*, el diccionario antes señalado no lo acepta como un prefijo, sin embargo al intentar encontrar dicho prefijo, lo define en relación con redes informáticas, ciberespacio[79], cibernauta[80]. Por consiguiente, el término *cibercrimen* o *ciberdelito*[81], se considera que abarca toda acción indebida o reprensible que ocurre en el ámbito de Internet, con independencia de sus implicancias legales y de si se trató, de un ataque potencial exitoso[82]. Igualm*ente cibercrimen*, puede ser definido como el conjunto actividades en la que se emplean ordenadores o redes como mecanismos blancos o lugares para la comisión de fines criminales.

Es necesario recalcar, que al hablar ya de *ciberdelito*, nos entrega alusión a quebrantamiento de una ley sancionada y vigente en un determinado territorio, por ello muchas organizaciones internacionales actuales, prefieren hablar de cibercrimen, puesto en múltiples países no cuentan con normas específicas en la materia y a pesar que existiesen, se encuentran demasiadas asimetrías en la

[78] Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa Calpe, Madrid, 2005, pág. 683.

[79] *Ámbito artificial creado por medios informáticos*. Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa Calpe, Madrid, 2005, pág. 546.

[80] *Persona que navega por el ciberespacio*. Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa Calpe, Madrid, 2005, pág. 546.

[81] PRANDINI, Patricia / MAGGIORE, Marcia, *Ciberdelito en América Latina y el Caribe*, En Proyecto Amparo 2° informe elaborado por iniciativa del Registro de Direcciones de Internet para Latinoamérica y el Caribe (LACNIC), (coordinador) MARTÍNEZ, Carlos, 2013, pág, 10.

[82] P*royecto amparo:* Fortaleciendo la Capacidad Regional en Seguridad Informática para la región de América Latina y el Caribe. El proyecto AMPARO es una iniciativa de LACNIC, el Registro de Direcciones de Internet para América Latina y el Caribe, que contó en su primera fase de desarrollo con el apoyo del Centro Internacional de Investigaciones para el Desarrollo (International Development Research Center – IDRC) de Canadá. Este proyecto se propone fortalecer la difusión, conocimiento y atención de la problemática de Seguridad Informática en los distintos países de América Latina y el Caribe fundamentalmente en el ámbito privado de las empresas y organizaciones sociales.

legislaciones existentes en cuanto al alcance tipificación de este tipo de delitos, por ello puede afirmarse que *cibercrimen* es simil*ar* al *ciberdelito* aunque este último se vincula más directamente como se dijo, con el quebrantamiento de las leyes y con su consecuencias jurídicas la pena, en cambio el primer concepto, es más amplio puede abarcar cualquier acción indebida o reprensible que ocurre en el ámbito de Internet[83].

Es necesario señalar, que la seguridad de la información tiene por fin evitar o minimizar la utilización de la tecnología con fines ilícitos, es decir, de manera contraria la moral o las leyes, y proteger la información en sí misma, con independencia de si ya sido tipificado o no en el país correspondiente. En todo el mundo, se han creado centros de respuesta para la seguridad informática, por ejemplo CSIRT[84], o el proyecto amparo.

[83] PRANDINI, Patricia / MAGGIORE, Marcia, *Ciberdelito en América Latina y el Caribe*, En Proyecto Amparo 2° informe elaborado por iniciativa del Registro de Direcciones de Internet para Latinoamérica y el Caribe (LACNIC), (coordinador) MARTÍNEZ, Carlos, 2013, pág, 11.

[84] Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT por su sigla en inglés) Estos grupos deben ser capaces de brindar información oportuna sobre cómo responder a los distintos tipos de incidentes, determinar su impacto, alcance y naturaleza, comprender las causas técnicas, investigar soluciones, realizar recomendaciones, coordinar y dar apoyo para la implementación de las estrategias de respuesta con las partes involucradas, difundir información sobre los tipos de incidentes más frecuentes y toda información relevante que permita estar preparado para dar respuesta a los mismos y mitigar sus efectos, coordinar y colaborar con otros actores, tales como proveedores de Internet (ISP), otros grupos de seguridad, etc. La existencia de estos grupos de tratamiento de incidentes permiten una más rápida y más eficiente dilucidación del origen de los problemas y con eso se evitan prejuicios aún mayores para la organización, usuarios o terceros que sean afectados.

B) El delito informático definido por distintos autores y organismos internacionales

1. **Delito informático definido por autores**

Uno de los primeros autores en referirse a este tipo de delito fue PARKER, el cual lo definió como *abusos informáticos,* y lo precisó como cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo pudo haber obtenido un beneficio. El autor anteriormente indicado no se limitó a describir las conductas relevantes para el ámbito penal sino que reconoce que se trata de un amplio abanico de comportamientos entre los que se incluyen, además de conductas de naturaleza penal, otras de relevancia civil y meros incidentes sin transcendencia jurídica[85].

A su vez TIEDEMANN, apunta a que todos los actos antijurídico según la ley penal vigente realizados con el empleo de un equipo automático de datos[86]. Asimismo TIEDEMANN, hace bastante tiempo se refería a la expresión criminalidad mediante computadoras, que aludía a todos los actos, antijurídico según la ley penal vigente o socialmente perjudiciales y por eso penalizarles en el futuro, realizados con el empleo de un equipo automático de procesamiento de datos[87].

[85] PARKER, *Crime by computer*, pág. 12 sigs. y 237 sigs. PARKER, D. B., Fighting Computer Crime, Charles Scribner's Sons, New York, 1983, Crime by Computer, Charles Scribem's Sons, New York, 1976.

[86] TIEDEMANN, Klaus, citado por MOLINA A, Carlos, *Introducción a la criminología*, Editorial, Biblioteca Jurídica, Medellín, 1988, pág. 307.

[87] TIEDEMANN, Klaus, *Poder económico y delito, Introducción al derecho penal económico y de la empresa,* Editorial Ariel. S.A., 1ª edición, Barcelona, 1985, pág. 122.

Los distintos enfoques doctrinales, se resumen en que el delito informático, más que un delito específico, debemos entenderlo como modalidades delictivas vinculadas, de algún modo a los ordenadores, tal cual como indica Romeo Casanova, puesto que el término delito informático de usarse en forma plural, toda vez que se utiliza para referirse a múltiples conductas ilícitas y no sólo va a una de carácter general

Volviendo a lo que indica *Parker*, que los términos son utilizados con frecuencia de forma indiscriminada, intercambiable y aún sin definición alguna, en consecuencia parece conveniente intentar aportar una definición que ayude a delimitar y precisar su contenido. El mismo autor hace alusión a la definición que ha sido entregada por el Departamento Justicia Norteamericano[88], sin embargo igualmente la crítica debido a que precisamente su excesiva amplitud, no aporta a comprender el contenido, del llamado delito informático. De esta manera, PARKER[89], define delito informático como cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor obtuvo o pudo haber obtenido intencionadamente un beneficio[90].

---

[88] *(computer crime*) Delito informático: cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su Comisión investigación o persecución. U.S. Department of Justice, Criminal Justice Resowve Manual on Computer Criminal Justice Information and Statistics Service, Washington, D. C., 1980.

[89] PARKER, citado por, ROMEO CASABONA, Carlos María. *Poder informático y seguridad jurídica. La función tutelar del Derecho penal ante las Nuevas Tecnologías de la información*, FUNDESCO, Colección impactos, Madrid, 1988, pág. 41, y sigs.

[90], Parker además entrega una tabla en que la que se definen los delitos informáticos de acuerdo a los propósitos que se persiguen: 1. Propósito de investigación de la seguridad: abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia (Parker, Nycum and Oura, 1973). 2. Propósito de investigación y acusación: delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática (Departamento de Justicia de Estados Unidos). 3. Propósito legal: delito informático es cualquier acto tal como está especificado en una ley sobre delito informático en la jurisdicción en que la

En forma general el concepto de delito informático puede comprender tanto conductas que se valen de medios informáticos y que lesionan intereses jurídicamente protegidos como en el caso de la intimidad, el patrimonio económico, la seguridad etcétera y por otro conductas que atacan directamente herramientas informáticas, como son los programas, o el mismo ordenador. Cuando la conducta lesiona distintos intereses jurídicos protegidos, la forma en que se comete de este delito es muy amplia y al momento de usar el ordenador como instrumento delictivo existe la posibilidad de usar la analogía, con el fin de ir adaptando la figura penal a las avances de la informática.

De acuerdo la anterior, se debe tener en cuenta lo que el legislador supuso o previo, como medio determinado, es decir casos calificados o donde no se emplea dicha conducta, sin embargo vale recordar lo anteriormente señalado en cuanto a la distinción entre delito o cibernético, telemático, computacional, etcétera, donde se denunciaron en forma genérica la distinciones entre ellos, puesto que los medios dentro de los cuales te cabida el uso de ordenador o cualquier medio para cometer el ilícito, no entrega al delito carácter informático, sin perjuicio que se hable en torno a la informática.

A su vez, TIEDEMANN, nos relata según las argumentaciones de KAISER[91], quien estima que la criminalidad informática es un fenómeno sometido constantemente cambios, a través del desarrollo técnico social en cuyo ámbito nuclear se encuentran manipulaciones a ordenadores, con el fin de conseguir una

---

norma se aplica. 4. Otros propósitos: abuso informático (sea cual sea su objetivo), es cualquier delito que no puede ser cometido sin computador. citado por, ROMEO CASABONA, Carlos María, *Poder informático y seguridad jurídica. La función tutelar del Derecho penal ante las Nuevas Tecnologías de la información*, FUNDESCO, Colección impactos, Madrid, 1988.

[91] KAISER, "Kriminologie. Eiii Lehrbuch", 3ra. ed., 1996, art. 74, n. raarg. 61. Citado por TIEDEMANN, Klaus, *Derecho penal y nuevas formas de criminalidad,* Editorial Idemsa, Lima, Perú, 2000.

ventaja patrimonial, a favor del autor o de un tercero. KAISER añade lo que tomó en cuenta legislador como base para introducir el artículo 263 a StGB, en 1986, puesto que el 90% de los casos de fraude informático, estaba constituido por el abuso de los cajeros automáticos de banco, o autores ajenos a la empresa.

BEQUAI[92], en 1978, realizó un análisis de estos delitos considerando que la definición de delito informático el acento debe ponerse en que los ordenadores pueden ser usados por el autor del delito, no sólo como instrumento para cometer el mismo, sino también como objeto delito, incluyendo entre los *compur crimes*, los delitos de sabotaje informático, robo de información digitalizada y programas, espionaje industrial, hurto de tiempo de uso del ordenador, robo de mercancía por manipulaciones de datos o fraudes financieros[93].

CAMACHO LOZA, indica como delito informático toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata la víctima, y en cuya misión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en actividades informáticas. Este autor, no considera que dicho concepto

[92] GUTIÉRREZ FRANCÉS, recuerda y explica, "no olvidemos, tampoco, la dimensión instrumental de la informática, que, al mismo tiempo que abre infinitas posibilidades de progreso y desarrollo a la humanidad, pone a disposición de la inteligencia del delincuente un enorme abanico de vías para alcanzar su propósito criminal, dando a luz perspectivas nuevas de la delincuencia tradicional". Asimismo cita a BEQUAI, *"Si con el ordenador hoy se puede hacer prácticamente todo, también con él pueden cometerse casi todos los delitos (ilícitos patrimoniales, que suelen merecer una atención privilegiada por su frecuencia y efectos, y otros de naturaleza distinta, como actos de terrorismo, sabotaje, daños, espionaje, falsedades, etc.).* BEQUAI. A, *1987 Technocrimes, pág. 1(The Computerization of Crime and Terrorism), Heath Lexington Books, Lexington.* GUTIÉRREZ FRANCÉS, María Luz, *Fraude informático y estafa*, 1ª Edición, Editorial Ministerio de Justicia, Secretaría técnica, Centro de publicaciones, Madrid, 1991, pág. 44.

[93] Autor citado, por HERNÁNDEZ DÍAZ, Leyre, *El delito informático*, En revista Eguzkilore, Número 23, San Sebastián, 2009, pág. 231. (BEQUAI *Computer Crime, White-Collar Crime*, pág. 3 y sigs. / *20th-Century Crisis*, pág. 105 sigs.

deba incluirse aquellos hechos en los que los dispositivos informáticos son objeto de un delito de los tipificados en el Código penal[94].

A su vez, ROMEO CASABONA, señala que cualquier conducta que no opere sobre la base de estas funciones, es decir el procesamiento y transmisión automatizados de datos y la confección y utilización de programas para tales fines, aunque puede resultar delictiva o merecedora de sanción penal, en su caso, no posee era ya esa especificidad, como sucede con la mayor parte de las agresiones sobre el *hardware*, y deberá ser, por tanto apartada del estudio de la delincuencia vinculada informática o tecnologías de la información[95]. Dicho autor advierte que "el Delito Informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución"[96]. Añade el mismo autor que entendiéndoles como todo acto intencional asociado de una manera u otra a los computadores; en los cuales la victima ha o habría podido sufrir una perdida; y cuyo autor ha o habría podido obtener un beneficio"[97].

Refiere DAVARA RODRÍGUEZ, indica que para estudiar el tema es necesario aceptar la expresión delito informático, definiéndola como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea

[94] CAMACHO LOSA, Luis, El delito informático, Editorial Madrid, 1ª edición, Madrid, 1987, pág. 25.

[95] ROMEO CASANOVA, Carlos, *Poder informático y seguridad jurídica, La función tutelar del derecho penal ante las nuevas tecnologías de información*, Editorial Fundesco, Madrid, 1988, pág. 43.

[96] CASABONA Romero, *Hacia un concepto de delito Informático*, Ponencia presentada al XI Congreso Internacional de Informática, Buenos Aires, Agosto, 2011.

[97] ROMERO CASABONA, Carlos, *Poder Informático…*op. cit., pág. 175.

llevada a cabo utilizando un elemento informático y/o el hemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software[98].

El profesor NAVA GARCÉS**,** señala que los delitos informáticos son actividades criminales que, en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, robo o hurto, fraude, falsificaciones, perjuicios, estafa, sabotaje, entre otros; sin embargo, debe destacarse que el uso de los ordenadores ha propiciado, a su vez, la necesidad de regulación por parte del derecho, para sancionar conductas como las señaladas. Los delitos informáticos tratan de encuadrar en delitos existentes y el asemejar una nueva conducta delictiva con anteriores, probablemente no sea la mejor manera de dar un buen comienzo a una legislación apropiada, sin antes haber tomado en cuenta todas las vertientes que las tecnologías implican[99].

Por su parte TÉLLEZ VALDÉS[100], señala que "no es labor fácil dar un concepto sobre delitos informáticos, puesto que su misma denominación alude a una situación muy especial, ya que para hablar de delitos en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión delitos informáticos esté consignada en los códigos penales. Tomando en cuenta lo anterior TÉLLEZ, define delito informático como actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumentos o fin,

[98] El autor hace énfasis en, está refiriéndose con dicha definición de la Comisión delito por medio informáticos y/o telemáticos, ya que la comisión de otros delitos en los que de alguna forma interviene un elemento informático, se encontrará sin duda dentro del Derecho penal en general y nada tiene que ver con el tema que estamos tratando. DAVARA RODRÍGUEZ, Miguel, *Manual de Derecho informático*, Editorial Thomson Aranzadi, 7ª Edición, Navarra, 2005, pág. 356.

[99] NAVA GARCÉS, Enrique, *Análisis de los delitos informáticos*, Editorial Ed Porrua, México, 2005, pág. 18.

[100] TÉLLEZ VALDÉS, Julio, *Derecho Informático*, 2ª edición, Editorial Graw Hill, México, 2001, pág. 105

(concepto atípico) o las conductas típicas, antijurídicas y culpables en que tiene a las computadoras como instrumento o fin (concepto típico)[101].

Refiere, BELTRAMONE junto a HERRERA BRAVO que un delito informático es "toda conducta que revista características delictivas, es decir, que sea típica, antijurídica y culpable, y atente contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del empleo de las tecnologías de la información, y el cual se distingue de los delitos computacionales o tradicionales informatizados"[102].

El profesor alemán ULRICH SIEBER, los define como "todas las lesiones dolosas e ilícitas del patrimonio relacionadas con datos procesados automáticamente"[103].

Por su parte HERRERA BRAVO[104], indica que el delito informático "es toda conducta que revista características delictivas, es decir, sea típica, antijurídica y

[101] TÉLLEZ VALDÉS, Julio, *Derecho Informático*, 3ª edición, Editorial Mc. Graw Hill, México, 2003, citado por, VELASCO SAN MARTÍN, Cristos, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*, Editorial Tirant Lo Blanch, Valencia, 2012, pág. 53.

[102] BELTRAMONE, Guillermo / HERRERA BRAVO, Rodolfo, *Nociones básicas sobre los Delitos Informáticos*, Ponencia preparada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile, Et all, 1998, pág. 6. Agregan los autores que de la definición, no todos los datos digitalizados merecen una protección penal (sí una protección civil o administrativa frente al mal uso que se les dé). Sólo los datos relevantes deben ser protegidos penalmente. Por ejemplo, en relación a los datos personales, sólo los datos sensibles deben protegerse creando delitos, es decir, aquellos datos que son muy personales y que permiten llegar a conformar un perfil del individuo que puede ser usado para discriminarlo, como su tendencia política, religiosa, sexual, historial médico, etc.

[103] HERRERA BRAVO, Rodolfo, *Reflexiones sobre la delincuencia vinculada con la tecnología digital, basadas en la experiencia chilena*, pág. 7. [accesible en] www.rodolfoher.pdf

[104] Asimismo Herrera Bravo indica respeto del tema: de la relación entre el delito e informática surgiendo tipo de ilícitos, los delitos computacionales y los delitos informáticos. Cuando los delincuentes de delitos tradicionales comienzan a utilizar como medio específico de

culpable, y atente contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del empleo de las tecnologías de la información, y el cual se distingue de los delitos computacionales o tradicionales informatizados"[105].

ABOSO advierte que el delito informático "es cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos"[106].

BAÓN, define la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software. Este autor añade la exigencia, que además las conductas incluibles en tales expresiones reúnan los requisitos que delimitan el concepto de delito[107].

---

comisión a la tecnología de la información, se produce una informatización de los tipos tradicionales, naciendo el delito computacional, que en realidad se trataría sólo de ilícitos convencionales que ya están regulados en el Código penal. Sin embargo también se crean conductas nuevas, no contempladas en los ordenamientos penales por su especial naturaleza, lo que hace necesario crear los llamados delitos informáticos. Citado por VELASCO SAN MARTÍN, Cristos, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*, Editorial Tirant Lo Blanch, Valenci a, 2012, pág. 53.

[105] BELTRAMONE Guillermo / HERRERA BRAVO, Rodolfo, ZABALE Ezequiel, *Nociones básicas sobre los Delitos Informáticos*, Ponencia preparada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile, agosto de 1998, pág 6.

[106] ABOSO, Gustavo / ZAPATA María, *Cibercriminalidad y Derecho penal*, 1ª edición, Editorial B de F, Buenos Aires Argentina, 2006, pág. 183.

[107] BAÓN RAMÍREZ, R, *Visión general de la informática en el nuevo Código Penal*, En Cuadernos de derecho judicial, 11, Barcelona, 1996, pág. 88.

Para GARCÍA, el delito informático es una "acción dolosa que provoca un perjuicio a personas o entidades y en la que se hacen intervenir dispositivos o programas informáticos"[108]. A su vez, la lexicógrafa MOLINER señala el delito informático "implica actividades criminales, que con la ayuda de la informática o de técnicas anexas, que llegan a configurarse como robos, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, entre otros"[109].

Se entiende Delito como "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas"[110] "Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma"[111].

CALLEGARI manifiesta que "delito informático es aquel que se da con la ayuda de la informática o de técnicas anexas"[112].

Refiere, CÁMPOLI KESSLER, que los delitos informáticos "son aquellos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo, por medio de la utilización

[108] GARCÍA BARCELÓ, Miguel, *Ponencia presentada al: Congreso sobre*, *Derecho Informático*, Universidad de Zaragoza, España, en junio de 2013.

[109] CASTRO OSPINA, Sandra, Ponencia presentada dentro de las XXIII Jornadas Internacionales de Derecho Penal, Colombia, *Delitos Informáticos*, 15 de Julio 2002, [disponible en] http://www.delitosinformaticos.com/delitos/colombia.shtml.

[110] MOLINER, María. (1996) Diccionario de María Moliner Edición Digital. Copyright© 1996 Novel Inc.; Copyright 1996 © María Moliner.

[111] CARRIÓN, Hugo, *Presupuestos para la Punibilidad del Hacking*, 2001. [accesible en] www.delitosinformáticos.com/tesis.htm.

[112] CALLEGARI, Lidia, *Delitos Informáticos y Legislación en Revista de la Facultad De Derecho y ciencias Políticas de la Universidad Pontificia Bolivariana*, Medellín, Colombia, Número 70, 1985, pág. 115.

indebida de medios informáticos"; considera que pueden ser definidos también, como delitos electrónicos o informáticos electrónicos, porque son una especie del género de delitos informáticos, en los que el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos, violando la intimidad de sus propietarios[113].

FERNÁNDEZ CALVO, define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española"[114].

GUERRERO MATEUS "concreta que estas maniobras delincuenciales virtuales como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando el elemento informático o telemático contra los derechos y libertades de los ciudadanos conforme a la constitución"[115].

VIEGA RODRÍGUEZ estima que son "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos."[116]

---

[113] CÁMPOLI KESSLER, Gabriel, *Principios de Derecho penal, Informático,* Editorial Ángel, México, 2004, pág. 29.

[114] FERNÁNDEZ CALVO, Rafael, *El Tratamiento del Llamado Delito Informático, En el proyecto de Ley Orgánico del Código Penal,* (Comisión de Libertades e Informática), En Informática y Derecho, 2015, pág. 1150.

[115] GUERRERO MATEUS, M, *La Ciberdelincuencia: La Ley Patriótica y sus efectos globales en las regulaciones nacionales y en particular en el caso colombiano*, En Revista de Derecho privado, Volumen 16, N° 29, Colombia, 2012.

[116] VIEGA RODRÍGUEZ, María José, *Un Nuevo Desafío Jurídico: Delitos Informáticos,* Editorial Mc Graw Hill, México, 2013, pág. 26.

Para María Luz LIMA, el delito electrónico "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"[117]. También hace alusión a que el delito informático de cualquier conducta criminal que en su realización hace uso de tecnología electrónica ya sea como método medio fin, por lo tanto, se entiende como delito informático las conductas típicas, antijurídica y culpable en que se tienen a los ordenadores como instrumento fin[118].

En palabras de PALAZZI, se define como toda (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas, sin que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena[119].

TIEDEMANN, considera que con la expresión "criminalidad mediante computadoras", se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos"[120].

---

[117] LIMA MALVIDO, María de la Luz, *Delitos electrónicos en criminalia*, México, Academia Mexicana de Ciencias Penales, Editorial Porrúa, Número 1-6. Año I., Enero-Junio 2004, pág. 100.

[118] LIMA MALVIDO, María de la Luz, *El delito electrónico*, Editorial Ariel, México, 1999 pág. 67.

[119] PALAZZI, Pablo Andrés, *Delitos Informáticos*, Editorial Ad-Hoc, Buenos Aires, Argentina, 2000, pág. 37.

[120] TIEDEMANN, Klaus, *La criminalidad económica como objeto de investigación*, En Cuadernos de Política Criminal, Número 19, Barcelona, 1983, pág. 171.

SUAREZ SÁNCHEZ señala, que "en conclusión, el delito informático está vinculado no solo a la realización y una conducta delictiva a través de miembros o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información per se cómo bien jurídico tutelado, diferente de los intereses jurídicos tradicionales[121].

Según CURY, delito informático se entenderá como una acción u omisión típicamente antijurídica y culpable[122].

HUERTA y LÍBANO, para quienes delito informático "son todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro[123].

Loa autores chilenos HERRERA y NÚÑEZ, señalan que toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable, y que atente contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del uso natural de las tecnologías de la información, y el cual se distingue de los delitos computacionales o tradicionales informatizados. Los autores antes

[121] SUAREZ SÁNCHEZ, Alberto, *La estafa informática*, Editorial Grupo Ibáñez, Bogotá. 2009.

[122] CURY URZÚA, Enrique, *Derecho Penal, parte general*, Ediciones Universidad Católica de Chile, 9ª edición, Santiago de Chile 2009, pág. 243.

[123] HUERTA MIRADA, Marcelo / LÍBANO MANSSUR Claudio, *Delitos Informáticos*, 2ª edición complementada y actualizada, Editorial Jurídica Cono Sur Ltda, Santiago de Chile, pág. 105 y sigs.

mencionados mencionan en su definición el objeto del delito distinto del bien jurídico protegido, el soporte lógico de un sistema de procesamiento de información[124].

Vale señalar, lo que indica la autora estadounidense MAJID YAR[125], estima que la ausencia de una definición específica sobre el fenómeno del *cibercrimen*, o *ciberdelito,* tiene su fundamento en que la delincuencia informática se refiere no tanto a un único tipo distintivo de actividad delictiva, sino más bien a una amplia gama de actividades ilegales ilícitas que comparten en común el único medio electrónico, a saber el *ciberespacio,* en el que tienen lugar. Añade dicha autora, que el término debe interpretarse como un rango de actividades ilícitas, es decir contrarias a la ley o la moral, cuyo denominador común es el rol central de las tecnologías de información y las comunicaciones y las redes para su comisión.

Por su parte el autor BALMACEDA HOYOS, rechaza la utilización de la de la definición *delito informático* que se utiliza por la doctrina para referirse a las conductas desarrolladas por medios informáticos, por cuanto indica que no se puede definir lo que comprende cabalmente la informática y porque el tipo penal en sí no existe a su juicio, prefiriendo elegir más bien un concepto funcional y de criminología como el de los que hablan de *criminalidad informática* y agrega que por las innumerables formas de comisión no podrían expresarse claramente en un tipo penal definido[126].

Para concluir, el término más usado hoy en día, el delito cibernético, puesto que las definiciones de *delito cibernético* dependen en gran medida del propósito

[124] HERRERA BRAVO, Rodolfo / NÚÑEZ ROMERO, Alejandra, *Derecho informático*, Ediciones Jurídicas la Ley, Santiago, 1999, pág. 219.

[125] Yar, Majid: Cybercrime and society. London, Sage Publications, 2006, pág. 5.

[126] BALMACEDA HOYOS, Gustavo, *El delito de Estafa Informática*. Ediciones Jurídicas de Santiago, Chile, pág. 60 y sigs.

para el que se use el término, decir un número limitado de actos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos representa el núcleo del delito cibernético. Los actos informáticos realizados por daño o beneficio personal o financiero, que incluyen delitos relacionados con la identidad y actos relacionados con contenidos informáticos no se prestan fácilmente para los esfuerzos de acuñar definiciones legales del término compuesto[127]. Se requieren ciertas definiciones para el núcleo de los actos delictivos cibernéticos[128].

2. Delito informático según organizaciones internacionales[129]

[127] El enfoque de cada definición, debe tomar en cuenta dos factores distintivos, puesto que las hipótesis delictivas que admite ser encuadrada dentro de los tipos tradicionales, ya que en ellas los medios informáticos sólo han sido una específica herramienta de comisión, mientras que los segundos requieren una configuración distinta en consideración a las particularidades que envuelven. Siempre debemos tener en consideración que el delito informático atenta contra soporte lógico informático, esto es software o programas de datos e información, puesto que el objeto material del delito se trata de impulsos electromagnéticos, de bienes intangibles o inmateriales no apropiarles o aprehensible físicamente, son cosas corporales muebles susceptibles de apoderamiento y que pueden ser objeto de apoderamiento, y perjudica la víctima. JIJENA LEIVA, Renato, *Delitos Informáticos, Internet y Derecho*, En delito, pena y proceso: Libro en homenaje a la memoria del profesor SOLARÍ PERALTA, Pontificia Universidad Católica de Valparaíso Facultad de Derecho, (coordinador) RODRÍGUEZ COLLAO, Luis, Editorial Jurídica de Chile, 2008, pág. 151.

[128] El estudio reafirma que, *la definición de delito cibernético no es tan relevante para otros fines, como el definir el alcance de los poderes investigativos especializados y la cooperación internacional, que es mejor que se enfoquen en la evidencia electrónica de cualquier delito y no en un constructo amplio y artificial para el delito cibernético*. UNODC (United Nations on Drugs and Crime), Estudio exhaustivo sobre le delito cibernético Oficina De Las Naciones Unidas Contra La Droga y El Delito, Naciones Unidas, Nueva York, 2013, pág. 13.

[129] En la última década se han visto avances considerables en la promulgación de instrumentos internacionales y regionales dirigidos a contrarrestar el delito cibernético. Estos incluyen instrumentos vinculantes y no vinculantes. Se pueden identificar cinco grupos, compuestos por instrumentos elaborados, o inspirados por: a) el Consejo de Europa o la Unión Europea; b) la Comunidad de Estados Independientes o la Organización de Cooperación de Shanghái; c) organizaciones intergubernamentales africanas; d) la Liga de los Estados Árabes; e) las Naciones Unidas. Existe un grado considerable de influencia mutua entre todos los instrumentos, incluyendo,

Cuando hablamos de delito informático, son varios organismos los que poseen una definición, de esta manera Estados Unidos de Norteamérica, el departamento justicia (*Departament of Justice*) ha definido al delito informático o *computer crime* como "cualquier acto ilegal que requiera el conocimiento de tecnología informática para su perpetración, investigación o prosecución"[130]. En una presentación sobre fraude informático la INTERPOL, 1979, destacó que "la naturaleza del delito informático es internacional, debido al estable crecimiento de las comunicaciones por teléfono, satélite, etc., entre los distintos países"[131].

Adicionalmente, la Organización de Cooperación y Desarrollo Económico OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos[132]. Para poder

---

en particular, conceptos y enfoques desarrollados en el marco del Convenio sobre Ciberdelincuencia del Consejo de Europa.

[130] Departamento de Justicia de USA, sección dedicada al Cybercrime y a la Propiedad Intelectual, [accesible en] http://www.usdoj.gov/criminal/cybercrime/index.html.

[131] Tercer Simposio sobre Fraude Internacional, París, 11-13 de diciembre de 1979.

[132] La OCDE expone: a) En esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados. b) La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos de la información como el objeto a proteger. c) No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, más poderosa delinquir. d) No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen. E) La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento. Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas. f) La protección de los sistemas informáticos puede abordarse desde distintas perspectivas: civil, comercial o administrativa. Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y lograr una protección global desde los distintos sectores para

entender los delitos informáticos es necesario tener presente los conocimientos generales de la Internet, como un conjunto de servidores conectados entre sí mediante un sistema maestro de computadoras dentro de una red alrededor de todo el mundo.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas. En aras de proporcionar claridad conceptual sobre los delitos informáticos, es pertinente comentar una breve reseña de la pluralidad de definiciones que conforman el mapa semántico de la expresión Delito Informático a partir de las diversas maneras en que la doctrina informática lo describe. La Organización de Cooperación y Desarrollo Económico OCDE[133], publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica donde se reseñan las normas legislativas vigentes y se define Delito Informático como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos"[134].

Por otro lado la ITU[135], define *ciberdelito* señalando que "un delito informático (computer-related crime) es aquél cuyo objeto o medio de realizarlo es un sistema informático, está relacionado con las tecnologías digitales y se integra en

---

alcanzar con eficiencia la defensa de los sistemas informáticos. OCDE. Organización de Cooperación y Desarrollo Económico, [accesible en] http://www.oecd.org/centro.com

[133] Por su parte la OCDE en 1983 hablaba de *infracción informática*, refiriéndose a "todo comportamiento ilegal, inmoral o no autorizado que afecta a la transmisión o al procesamiento automático de datos"

[134] Organización de Cooperación y Desarrollo Económico OCDE. (1993). Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en Mayo de 1993.

[135] La UIT es el organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación.

los propios de la delincuencia de cuello blanco. El ciberdelito (cybercrime) es una forma del delito informático que recurre a las tecnologías de Internet para su comisión, refiriéndose por tanto a todos los delitos cometidos en el ciberespacio".

La Commonwealth, define el "delito relativo a los sistemas de cómputo" como un "acto criminal en el que el objetivo es un sistema informático"[136].

Ahora bien, los instrumentos internacionales o regionales muchas veces no definen el delito cibernético siendo un término correcto utilizar hoy en día, de esta manera ni el Convenio sobre Ciberdelincuencia del Consejo de Europa, ni la Convención de la Liga de los Estados Árabes[137], ni el proyecto de Convención de la Unión Africana, por ejemplo, contienen una definición del delito cibernético para los fines del instrumento. Sin embargo, se puede señalar que el Acuerdo De La Comunidad Estados Independientes[138], refiere que el delito informático es un "acto delictivo cuyo blanco es informático", ya su vez la Organización De Cooperación De Shanghái[139], indica que *delitos de información*, se refiere al "uso de recursos de información y al impacto sobre ellos en la esfera informática para fines ilegales".

Como se ha dicho al hablar de delito cibernético y delito informático, nos estaríamos refiriendo a fenómenos distintos. Por ello es posible constatar, la existencia de diversos delitos relacionados con elementos informáticos, tales como la estafa por Internet, o el contenido sexual entre adultos y menores de edad vía

[136] (*Commonwealth of Nations*), comunidad de naciones vinculada al Reino Unido.

[137] Liga de los Estados Árabes, Ley Modelo Árabe para el Combate de los Delitos relacionados con los Sistemas de Tecnología de la Información, 2004.

[138] Acuerdo de la Comunidad de Estados Independientes, sobre Cooperación para Combatir Delitos Informáticos, Art. 1, 2001.

[139] Acuerdo de la Organización de Cooperación de Shanghái, en el Campo de la Seguridad Informática Internacional, 2010.

Internet, o los datos de un banco en particular, correspondiendo ellos a los que la ONU, llama delitos cibernéticos. En cuanto la Unión Europea, reconoce los términos delincuencia informática y cibernética, teniendo mismo significado puesto que se refieren a la explotación de la red información y comunicación, sin ninguna dificultad hagiográfica, ya su vez a la circulación de datos intangibles y volátiles, tal como indica en la Decisión Marco de 2005 del Consejo de la Unión Europea[140]. La ONU en la Unión Europea, no hacen una distinción si el elemento informático justifica el tipo pese al delito en que se encuentra el objeto o fin en sí mismo el delito, o si consta en el mero medio para la realización de un fin ilícito, por ejemplo en el caso del intromisión en la red interna de un banco para obtener antecedentes comerciales de un tercero, o una estafa vía Internet, para dichas entidades delito cibernético o informático sería lo mismo[141]. Vale señalar que la definición de delito cibernético, propuesta por la ONU envuelve distintas conductas relacionadas con un sistema o red computacional, ya sea que la relación exista a nivel de medio o que la conducta tenga como fin afectar un sistema informático, proponiendo la ONU la noción de delitos cibernéticos en dos dimensiones distintas, a saber la primera definida como delito cibernético en sentido estricto o delito informático; la segunda la define como delito cibernético en sentido lato o delito relacionado con ordenadores[142].

[140] El Consejo de la Unión Europea es un organismo de la Unión Europea, Decisión Marco 2005/222/JAI del consejo de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información». Diario Oficial de la Unión Europea.

[141] LARA, Juan /MARTÍNEZ, Manuel / VIOLLER, Pablo, Hacia una regulación de los delitos informáticos basada en evidencia, En revista chilena de derecho tecnología, Volumen 3, Numero 1, 2014, pág. 104.

[142] Todo comportamiento ilícito realizado por medio de un sistema o red informático, o en relación a ellos; incluidos los delitos como la posesión, el ofrecimiento o la distribución ilegales de información por medio de un sistema o una red informática. ONU, Delitos Relacionados Con Redes Informáticas, Documento Antecedente Para El Curso Práctico Sobre Delitos Relacionados Con Las

Los instrumentos internacionales y regionales, nos llevan a delimitar ciertos enfoques principales, a saber terminología que se basa en datos o sistemas de ordenadores o computarizados y terminología basada en sistemas o datos informáticos, pero a pesar que existen definiciones distintas para los términos mencionados, se puede mencionar que los términos en gran medida se han usado en forma intercambiable. Sin embargo se puede mencionar en cuanto las disposiciones legales, cuando se refieren los textos internacionales, como ordenador; sistema computarizado; o sistema informático, el factor común es que el dispositivo debe ser capaz de procesar datos o información computarizada, ya su vez algunos exigen que debe ser automático o de alta velocidad o con un programa. Algunos entienden que la definición a los dispositivos que almacenan o transmiten y reciben datos o información computarizada las tienden a sí misma y otros incluyen dentro de la definición los datos informáticos que son procesados por el sistema.

Vale señalar que cuando el término sistema computarizado sistema informático excluya datos almacenados en el sistema o en otros dispositivos de almacenamiento, éstos a menudo son manejados por separado en las disposiciones sustantivas legales del instrumento, como por ejemplo, el Convenio sobre Ciberdelincuencia del Consejo de Europa y la Ley Modelo de la Comunidad de Estados recurre a los términos *sistema computarizado* y *datos informáticos*. A su vez el proyecto de Convención de la Unión Africana usa *sistema computarizado* y *datos informáticos*, y también la Decisión de la Unión Europea, relativa a los ataques contra los sistemas de información recurre a *sistema de* información y *datos informáticos*.

Redes Informáticas, En 10º Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente, Vienna, 2000.

Por último, cuando algunos instrumentos definen computadora como sistema computarizado, este último normalmente fluye primero, lo mismo sucede con redes computarizadas y sistemas computarizados. Y en cuanto al concepto central de procesamiento de datos informáticos o información, se estima que las disposiciones normalmente apliquen a dispositivos como servidores y ordenadores centrales, ordenadores personales de escritorio, ordenadores portátiles, teléfonos inteligentes, tabletas y ordenadores de a bordo del transporte maquinaria así como los dispositivos multimedia como las impresoras, reproductores, máquinas de juego etcétera[143]. A su vez los *datos informáticos y la información computarizada*, son descritos como una representación de hechos, informaciones o conceptos que pueden ser leídos, procesados almacenados por un ordenador.

El no haber una definición aceptada, parece un pequeño problema, ya que en la mayoría de los casos son definiciones similares, que incluirían los mismos tipos de delito. Pero sigue habiendo una gran discusión sobre que es ciberdelito y lo que no. Esto es un gran problema en el ámbito jurídico, que obliga prácticamente a desarrollar un listado de delitos que estarían definidos como delito en cada documento o ley formulada, ya que el hecho de no haber consenso puede generar muchos problemas con las leyes como veremos en el punto

[143] Una nota de guía para el Comité del Convenio sobre Ciberdelincuencia del Consejo de Europa también llega a la conclusión de que la definición del término *sistema informático* en el artículo 1 del Convenio sobre Ciberdelincuencia del Consejo de Europa cubre formas de tecnología en desarrollo que van más allá de las computadoras centrales o de escritorio tradicionales, como los teléfonos móviles modernos, los smartphones, los PDA, las tabletas o dispositivos similares. UNODC (United Nations on Drugs and Crime), Estudio exhautivo sobre le delito cibernético Oficina De Las Naciones Unidas Contra La Droga y El Delito, Naciones Unidas, Nueva York, 2013, pág. 16.

IV. Características y elementos del delito informático

A pesar, que se han entregado varios intentos de conceptualización del delito informático, vale señalar que estos nacen de la criminalidad evolutiva, la cual viene en forma concomitante con las nuevas tecnologías informáticas y telemáticas, por ello este delito se comete con el empleo de ordenadores o equipos electromagnéticos que tramiten datos o información. A pesar de las definiciones analizadas cuando TIEDEMANN, analiza el comportamiento dentro de su definición en forma general, el autor de alguna manera incluye todos los hechos ilícitos cometidos a través de un equipo informático.

A) Elemento del delito informático

De acuerdo lo anterior, antes de analizar las características propiamente tales de este tipo de ilícito, ya pesar de la discusión acerca de su naturaleza, existen elementos comunes a todos ellos.

Primero que todo existe una *conducta fraudulenta*, que se refiere al uso indebido fraudulento de elementos informáticos a través de la introducción o manipulación de datos falsos. En segundo lugar, existe un *instrumento*, tomando en consideración que debemos estar en presencia de componentes físicos o también lógicos del sistema informático. En tercer lugar debemos hablar de la *finalidad*, la cual tiene que ver con la obtención de un beneficio ilícito, ya sea en forma directa o indirecta y no siempre va ser necesariamente patrimonial. Y por último debe existir un *resultado*, que se traduce en un perjuicio, igualmente que lo anterior no

necesariamente patrimonial, pudiendo ser tanto de un tercero o de una colectividad[144].

B) Principales características del delito informático

A partir de las diferentes fuentes jurídicas pueden identificarse determinadas características de los delitos informáticos.

1. Permanencia del hecho

Significa que los delitos cibernéticos o delitos informáticos pueden repetirse continuamente del tiempo. ROVIRA DEL CANTO, se refiere ellos señalando, "que la incidencia de la posible repetición de una actuación ilícita en el ámbito informático, favorece su nueva Comisión, incluso en múltiples ocasiones, derivando la práctica a que en un alto porcentaje los supuestos conocidos y enjuiciado ilícitos informáticos la conducta de los autores nos ha limitado a una única acción delictual, sino a una reiteración continua la misma"[145].

A su vez, ALASTUEY BOBÓN, denomina como efecto continuado, propio de esta delincuencia, y que por la jurisprudencia se aprecia en un alto porcentaje de

[144] MORABITO, MARIO, *La regulación de los Delitos informáticos en el Código Penal argentino,* Editorial Thomson Reuters, La ley, [accesible en] <www.dab.com.ar>.

[145] ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Editorial Comares, Granada, 2002, pág. 78.

ocasiones la figura del delito continuado por la sanción de tales comportamientos[146]. En la actualidad la herramienta para cometer dicho lícitos encuentra disposición todo el mundo, se notó delito de comisión instantánea y de efectos permanentes.

2. Dificultad para su investigación y prueba

Nuevamente ROVIRA DEL CANTO, no señala que estos he venido dando la doctrina en el sentido de un análisis como vínculo causa-efecto, como base de una consecuencia, también de índole criminológica, puesto que se caracteriza por el anonimato del perjuicio producido, la facilidad para encubrir el hecho y la disminución del riesgo de ser descubierto el autor gracias a la posibilidad de borrar huellas[147]. Por ejemplo, un delincuente al accionar bajo la Internet profunda u ocultar, su IP se hace variable, siendo difícil su persecución, lo mismo ocurre en el caso de un próximo puesto que funciona como una barrera entre delincuente víctima imposibilitando la manera de determinar la dirección IP. En segundo lugar la distancia física, en razón a que los delincuentes nunca están en el "lugar del crimen" físicamente, por lo que su localización es más compleja y el riesgo que asumen es menor.

[146] ASTUEY DOBON, Mª Carmen, *Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial*, Informática y Derecho (director) CARRASCOSA LÓPEZ, Valentín, Área De Derecho Penal, Facultad De Derecho De La Universidad Zaragoza, Editorial Aranzadi, España, 1994, pág. 484.

[147] ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Editorial Comares, Granada, 2002, pág. 82.

3. Delitos con un carácter altamente técnico

Para cometer dichos ilícitos el sujeto activo debe tener algunos conocimientos especiales en sistemas informáticos, para poder llevar acabo el hecho. A pesar que hoy en día todas las herramientas tecnológicas están a disposición en la red, existen variados delitos informáticos, que para poder cometer lo se requiere de conocimientos técnicos avanzados, y por consiguiente también se necesita una policía técnica especializada para poder perseguirlos o descubrirlos. Su complejidad derivada de la profesionalización y redes organizadas de ciberdelincuente; en numerosos casos las actividades fraudulentas son llevadas a cabo por mafias y redes de delincuentes organizadas y especializadas, frecuentemente ubicadas en otros países.

4. Delitos con un carácter transfronterizo

Esta característica es casi de la esencia del delito puesto que con la arremetida de Internet las fronteras para este tipo de delitos han desaparecido, como indica ROVIRA DEL CANTO, el alejamiento entre el lugar donde se encuentra el autor de la acción, o donde ésta se realiza, y la del lugar donde va a producir sus efectos o consecuencias, aparece la superación de las barreras nacionales. La transnacionalidad de los delitos informáticos trascienden las fronteras de los Estados, lo que hace recomendable regulaciones también transnacionales de este tipo de actividades criminales. La transnacionalidad es un tema preocupante ya que un delincuente japonés puede cometer una estafa en Estados Unidos estando físicamente en Francia, a través de una red de ordenadores, controlados

remotamente localizados en Rusia. Así la complejidad procesal resultante de la coexistencia de diferentes tipos delictivos y la aplicabilidad de diversas legislaciones puede dificultar la persecución del delito. En base a las soluciones tradicionales, se suele abogar por la persecución del delito por parte de las autoridades del país en el que la víctima sufre sus consecuencias. Esta situación tiene una cierta utilidad práctica, que ha conducido a un relativo consenso en torno a su adopción.

5. Son delitos masivos, colectivos o difundidos

Atendiendo a las particularidades propias de algunos delitos, hay autores que han querido caracterizar a los delitos informáticos como delitos masivos, colectivos o difundidos, por cuanto su comisión afecta a un número indeterminado de personas, el que habitualmente puede ser muy alto.

6. Son delitos de mera actividad

Estos delitos pueden revestir el carácter de "delito formal o de mera actividad, que se perfecciona por la sola acción u omisión del sujeto activo (como ejemplo cabe señalar el caso del acceso indebido), como el de delito material, cuyo perfeccionamiento el legislador lo ha condicionado a la obtención del resultado ilícito de parte del agente (cabe señalar el caso del sabotaje informático.

7. Alto volumen de cifra oscura

ROVIRA sobre el particular nos señala que "con la mejora y avances en las técnicas de investigación, lo cierto es que en base a los estudios empíricos más recientes efectuados a nivel internacional, se reafirman las tres clásicas apreciaciones de que el número de los delitos informáticos comprobables no es excesivamente alto, ello no obstante el número de los casos que verdaderamente tienen lugar no es ni mucho menos escaso, y ello debido a que la cifra oscura en el ámbito de la criminalidad informática es efectivamente excepcionalmente alta[148].

8. Son pluriofensivos

No atenta en contra de uno sino de varios bienes jurídicos protegidos, sean ellos de caracteres propiamente informáticos o tradicionales, y se suma a ello, la ubicuidad, ya que es posible cometer delitos de forma simultánea en lugares muy distantes.

V. Clasificación del delito informático

[148] ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Editorial Comares, Granada, 2002, pág. 87.

Para clasificar el delito informático en forma general la doctrina tiene cuenta tres criterios fundamentales: El subjetivo, el Objetivo y el Funcional.

A) Criterio subjetivo

Se centra en lo distintivo de los delincuentes informáticos, pues observa a los sujetos y a sus características; clasificándolos si es delito de cuello blanco, o si es un delito común, donde la persona no tiene una posición destacada en la sociedad; así mismo de acuerdo a si el criminal informático posee conocimientos técnicos en sistemas lógicos de información o desconoce por completo técnicas y lenguajes de información.

B) Criterio Objetivo

Este criterio clasifica los delitos informáticos acorde con el objeto material contra el cual recae o se dirige el comportamiento criminal informático y los agrupa de la siguiente manera: Los fraudes Informáticos o Manipulaciones no autorizadas de datos: Son tenidos como la "incorrecta utilización del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o están ya contenidos en el computador en cualquiera de las fases de su procesamiento o tratamiento informático, siempre que sea con ánimo de lucro y en

perjuicio de tercero"[149]. Entendidos como aquellas actividades ilícitas que se cometen a través de la manipulación del sistema contra los programas de procesamiento de datos.

C) Criterio Funcional

Desde este criterio los delitos informáticos son aquellas conductas que tienen por objeto el funcionamiento de los sistemas informáticos. Esta categoría mira el proceso informático o de procesamiento de datos, y a partir de este se propone la clasificación de los delitos, a saber delitos contra la fase de entrada del sistema o sustracción de datos, que consiste en tomar algunos de los datos procesados por la computadora sustrayéndolos, a través del medio magnético, óptico o magnético-óptico, para luego ser leídos, manipulados o simplemente mantenidos en otra computadora; Atentados contra la fase de salida del sistema, el cual se efectúa fijando un objetivo al funcionamiento del sistema informático, creando instrucciones falsas o fictas las cuales la computadora recibe y asume como ciertas, ejecutando la instrucción normalmente, el ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos; Atentados contra los programas del sistema, el cual es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática; Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas al programa computacional. Con

[149] VERA QUILODRÁN, Alejandro, *Delito e informática, La informática como fuente de delito*, Ediciones Jurídicas La Ley, Santiago de Chile, 2014, pág. 109.

esto se busca desorientar las funciones del programa para buscar un beneficio o aprovechamiento propio.

CAPÍTULO II

Consideraciones sobre informática.

Cuestiones relativas a internet, cibercrimen y su falta de regulación

I. Aspectos genéricos sobre tecnología de la información y el uso del ciberespacio

Tomando consideración una de las características principales del derecho, a saber que el derecho no permanece inmóvil, si no que se va desarrollando según como se desarrolla la sociedad, el Derecho penal y sus normas van en continuo avance quedando sujetas a la modificaciones, debiendo ser actualizadas constantemente[150]. El uso diario de los ordenadores del acceso Internet ha producido cambios importantes, en todo el ámbito del ser humano tanto la producción, organización del trabajo y prestaciones servicios generando nuevo orden social caracterizado, por la importancia de la información[151], naciendo el derecho

[150] Una de las primeras preocupaciones gubernamentales sobre el uso de la informática en el nivel social, se le atribuye al presidente francés Valéry GISCARD D´ESTAING y al inspector general de Finanzas en 1976, Simón NORA, en razón a que la informática representaba un factor de transformación de la organización social y económica que el Estado y debía tratar de dominar para poner al servicio del desarrollo que señala: *"En tiempos pasados, toda revolución tecnológica provocaba una intensa reorganización de la economía y la sociedad (...) la "revolución informática" tendrá consecuencias más amplias. No es la única innovación técnica de los últimos años, pero sí constituye el factor común que permite y acelera todas las demás. Sobre todo, en la medida que altere el tratamiento y la conservación de la información, modificará el sistema nervioso de las organizaciones y de la sociedad entera".* NORA, Simón / Alain, MINC, *La informatización de la sociedad*, Fondo de Cultura Económica, México, 1982, pág. 17.

[151] El término *información*, que según la definición de la Real Academia de la Lengua Española significa, *enterar, dar noticia de algo* y que en términos legos hubiera significado tan sólo una simple acumulación de datos, se ha ampliado, transformándose *en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico*.

informático, debiendo encargarse del fenómeno tecnológico y el surgimiento de un ordenamiento especial que ha venido a socavar los esquemas jurídicos tradicionales, por ello necesario analizar en forma breve algunos conceptos básicos relacionados con la tecnología de la información.

A) Planteamientos

1. Sociedad de la información[152]

Brevemente podemos decir que al lograr la automatización de los servicios respecto de un bien inmaterial e ilimitado el sistema económico vuelve a

GUTIÉRREZ FRANCÉS, María luz, *Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa*, En MAZUELOS COELLO, Julio (coord.) Derecho Penal Económico y de la Empresa, Editorial San Marcos, Lima, 2014, pág. 383.

[152] La lotería información se origina en un famoso artículo de CLAUDE SHANNON, de 1948, The Mathematical Theory, of Communication, el cual habla sobre la base de particulares necesidades tecnológicas relacionadas con la física, dicho artículo fue seguido por muchos autores y replicaban muchos trabajos posteriores que tenían relación con el haría de la radio, televisión, economía y telefonía etcétera, resumiéndose dicha teoría de la información, en que una situación de comunicación queda definida por una fuente, un receptor y un canal. Por ello para algunos el término información, refiere a un concepto totalmente formal, que se define exclusivamente sobre la base de una distribución de probabilidad previamente definida, por ello desde una perspectiva matemática, informaciones una medida del modo en que se modifica nuestro estado de conocimiento. Tomando la información desde este punto de vista, es decir sobre la teoría de información, en la cual el tema se posiciona de un modo puramente formal, no hace alusión alguna a la transmisión o recepción de señales. Así las cosas hablando de un modo informacional de la observación científica, se argumenta a favor del enfoque que incorpore la relevancia del conocimiento previo en todo proceso observación científica subrayando la dependencia respecto de tal conocimiento y no sólo teórico sino también específico acerca de la distintas situaciones consideradas no mermando con ello carácter objetivo de la observación. *Zapata*, María, / ABOSO, Gustavo, *Cibercriminalidad y Derecho penal, La información y los sistemas informáticos como nuevo paradigma del Derecho penal*, Editorial, B de F, Buenos Aires Argentina, 2006, pág. 24.

reorganizarse, el cual trae consecuencias, sufriendo el modelo social transformaciones de gran magnitud, como es del caso que nace la sociedad de la Información[153]. Cuando se trata de definir lo que es sociedad de la información, son recurrentes las opiniones que afirman que se trata de una sociedad en formación en que las nociones de información, comunicación y nuevas tecnologías se integran, alejándose de entregar conceptualizar en forma directa, sólo dando afirmaciones sobre características más indiscutidas, pero el asunto se refiere a un concepto complejo. Es del caso que resulta útil la definición que entrega el Libro Verde sobre la Sociedad de la Información en Portugal de 1997, el cual señala que se refiere a una forma de desarrollo económico y social en el que la adquisición, almacenamiento, procesamiento, evaluación, transmisión, distribución diseminación de la información con vistas a la creación de conocimiento de la satisfacción de las necesidades de las personas de las organizaciones, juega un papel central en la actividad económica, en la creación de riqueza de la definición de la calidad de vida y prácticas culturales de los ciudadanos[154].

Anteriormente, se hablaba de la sociedad del conocimiento entregándoles el trato de términos sinónimos, puesto que la información no equivale a conocimiento, existiendo una relación entre ambos de medio-fin, es decir la información es un instrumento para el conocimiento, pero no el conocimiento en sí mismo, en la medida en que el conocimiento requiere de una elaboración una mediación

[153] El Derecho Informático, está enfocado únicamente a una protección de los datos informáticos o la información concentrada en medios magnéticos o digitales. Esta información "tiene un valor patrimonial y es susceptible de apropiación; haciéndose una distinción entre *Derecho sobre la Información* y *Derecho a la Información*, entendiéndose como derecho sobre la información la referente a datos. CORREA, Carlos, *Derecho informático*, Editorial Desalma, Buenos Aires, Argentina, 1999. pág. 288.

[154] El Libro Verde elaborado por la Comisión de la Sociedad de la Información del Ministerio de Ciencias de Portugal y aprobado por el Consejo de Ministros de ciencias de Portugal, Brasil, abril de 1997.

intelectual con arreglo criterio metodológico y epistemológico aplicado sobre la información de que se dispone. Podemos decir entonces que la información es la condición que debe existir para que nazca el conocimiento, por ende la información en el contexto del estudio, es un conjunto de impulsos electrónicos con capacidad para producir texto imágenes en un ordenador, sin mayores implicaciones epistemológica al no transmitir ningún conocimiento auténtico.

La sociedad de la información, se dicho que es la sucesora de lazo siendo trial, que viene caracterizada a partir de los años 80, por las nuevas tecnologías, la informática, la robótica inteligencia artificial, las telecomunicaciones, Internet etcétera todo lo cual está basado en la digitalización del información favoreciendo con ello la interdependencia y el acceso, almacenamiento y transmisión de la información. Con esta nueva revolución llamada sociedad de la información ha posicionado al ser humano en un mundo totalmente distinto donde han cambiado los conceptos de espacio y tiempo, hablándose ahora de espacios digitales, de atemporalidad, y relación virtual entre los sujetos[155].

2. Electrónica

Resulta importante iniciar el tema, explicando en primer lugar, que es la electrónica, a fin de poder entender la diferencia entre un delito informático y los delitos electrónicos.

[155] RODRÍGUEZ VILLASEÑOR, Isabel / GÓMEZ GARCÍA, Juan, *Investigación y documentación jurídicas*, 2ª edición, Editorial Dykinson, Madrid, 2013, pág. 53 y sigs.

La electrónica, *es la parte de la ciencia que estudia los fenómenos que intervienen electrones en estado libre*[156]. Por otro lado como técnica *es el estudio y aplicación del comportamiento de los electrones en diversos medios, como el vacío, los gases y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos*[157]. De manera sencilla, dentro de un aparato electrónico, el flujo de estos electrones genera corriente eléctrica y ésta a su vez usada en dispositivos que cambian la energía eléctrica en calor, luz o movimiento, a lo que se conoce como eléctrica, pero usada en dispositivos provistos de inteligencia artificial genera una radio, una televisión y un ordenador.

3. La Cibernética

La palabra Cibernética proviene del griego kibernetes, y significa piloto o el arte de pilotear un navío[158]. Platón la utilizó en su obra la República con el significado de arte de dirigir a los hombres o arte de gobernar.

El nacimiento de la cibernética se estableció en el año 1942, en la época de un congreso sobre la inhibición cerebral celebrado en Nueva York, del cual surgió la idea de la fecundidad de un intercambio de conocimiento entre fisiólogos y técnicos en mecanismos de control. Cinco años más tarde, uno de los principales fundadores

[156] Diccionario De La Lengua Española, Editorial Real Academia Española. Vigésima segunda Tomo, 3, Madrid, 2015, pág. 461.

[157] Diccionario De La Lengua Española, Editorial Real Academia Española, Vigésima segunda edición, Tomo 4, Madrid, 2015, pág. 590.

[158] MATEOS MUÑOZ, Agustín, *Compendio De Etimologías Greco-Latinas Del Español.* Editorial Esfinge, Cuadragésima sexta edición, México, 2007, pág. 299.

de esta ciencia, Norbert WIENER[159], propuso el nombre de cibernética, derivado del griego, lo cual traducido puede significar piloto, timonel o regulador, como lo plasmó en su obra cibernética o el control y comunicación en animales y máquinas. Se trata del estudio del control y comunicación en los sistemas complejos es decir, organismos vivos, máquinas y organizaciones. Es la rama de las matemáticas que se encarga de los problemas de control, recursividad e información. Estudia los flujos de información que rodean un sistema, y la forma en que esta información es usada por el sistema como un valor que le permite controlarse a sí mismo y ocurre tanto para sistemas animados como inanimados.

La cibernética es una ciencia interdisciplinaria, ligada a la física, al estudio del cerebro, los computadores y, relacionada directamente con los lenguajes formales de la ciencia, proporcionando herramientas con las que describir de manera objetiva el comportamiento de todos estos sistemas y también llamadas dimensiones o atributos, representadas de forma binaria con variables que toman dos valores, en función de la existencia o no del sistema. La representación binaria puede ser generalizada a una propiedad con múltiples valores discretos o continuos.

Vale señalar que no se debe confundir cibernética con equipo puesto que este último está diseñado a los principios por los cuales el equipo de cómputo opera, es decir el equipo realiza tareas a través de los programas. Toda actividad cibernética, debe llevarse a cabo con la participación integradora de tres elementos a saber tarea, hombre y máquina. La cibernética permite la interrelación de las diversas actividades humanas de manera ordenada así como la gestión del trabajo multidisciplinario, por ello se dice que sería la ciencia de la comunicación y control relacionando todo campo de estudio.

[159] Fue un matemático estadounidense, conocido como el fundador de la cibernética. Acuñó el término en su libro Cibernética o el control y comunicación en animales y máquinas, publicado en 1948.

Además se puede indicar que esta ciencia proporciona un estudio comparativo de la operación entre cerebro humano y el ordenador electrónico, puesto que no hay una diferencia tan radical entre entregar una orden a una máquina o a una persona, puesto que la máquina individualmente hablando que receptores sensoriales que captan información a través de la operación individual, cruzando información entre hombre y máquina. Por otro lado, existe una manifestación de la cibernética, cuando facilita el análisis sistematizado del contenido normativo del sistema jurídico dado, porque a través de la tecnología se podrá utilizar como medio para organizar las reglas de dicho sistema[160]. Por ello en cuanto a la teoría de los sistemas se trata, permite la cibernética el estudio cuantitativo de los hechos y las reglas de conducta de las personas, siendo el análisis de la conducta legal como técnica de control social[161].

Vale señalar que la Cibernética es la ciencia que trata de explicar y dar solución a eventos de control y comunicación ya sean fenómenos acontecidos en la naturaleza, sociedad o humanos. En cambio la Informática busca desarrollar máquinas dotadas de *inteligencia artificial*, capaces de simular actividades y capacidades humanas como la robótica, la búsqueda de solución de problemas y la toma de decisiones por sí mismas, conocido como *heurística o método heurístico*.

En definitiva, es importante resaltar que el sentido moderno del vocablo cibernética radica en el énfasis especial que pone sobre el estudio de las comunicaciones, mensajes y, la forma cómo se encuentran regulados internamente todos los sistemas de comunicación, ya sean biológicos, sociales o, sino sobre las

[160] ARROYO BELTRÁN, Miguel, *Cibernética*, [accesible en] <http://razssosa.blogspot.cl>.

[161] LOPES DA SILVA, Rita, *Direito penal, e sistema informático,* Editorial Revista dos Tribunais, Ciencia Derecho penal contemporánea número 4, (Coordinador) PRADO REGIS, Luis, Sao Paulo, 2003, pág, 19.

máquinas que imitan procesos de regulación u ordenación, cálculo, comparación lógica, búsqueda de objetivos, etc., como en el caso de los ordenadores, autómatas[162].

4. Informática

Un acelerado proceso de cambio, a una verdadera revolución que ha sido capaz de conquistar tres infinitos: lo infinitamente pequeño, *el átomo;* lo infinitamente grande, *el cosmos*; y lo infinitamente complejo, *la informática*. Por ello, se habla de sociedad informática o sociedad cibernética[163].

Si bien es cierto, la tecnología informática, ha traído grandes beneficios, sin embargo, su desarrollo ofrece también un aspecto negativo, que ha generado nuevas conductas delictivas, que se manifiestan en formas que no era posible imaginar en el siglo pasado, Los sistemas de computadoras ofrecen oportunidades nuevas y muy complejas de infringir la ley y han creado la posibilidad de cometer delitos tradicionales en formas distintas[164].

La informática es una rama de la ingeniería que estudia el tratamiento de la información mediante el uso de máquinas automáticas y proviene del francés

[162] SALAZAR CANO, Edgar, *Cibernética y Derecho Procesal Civil*, Ediciones Técnico-Jurídicas, Lima, 1979.

[163] GARCÍA-PABLOS MOLINA, Antonio, *Informática y Derecho penal*, en Implicancias socio-jurídicas de las tecnologías de la información, Editorial Citema, Madrid, 1984, pág. 39.

[164] BUITRAGO RUIZ, Ángela, *El Delito Informático,* Revista Derecho Penal y Criminología Vol. 18, número 59, 1996, pág. 96.

informatique que a su vez por la conjunción de las palabras información y *automatique*, para dar idea de la automatización de la información que se logra con los sistemas computacionales, acuñado por el ingeniero *Philippe Dreyfrus* en 1962, siendo el procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales[165].

MAGLIONA MARKOVICTH nos dice que la informática, se entiende como *aquella ciencia que estudia y tiene como objeto el tratamiento automatizado o electrónico de la información*[166]. Por otro lado el término *información*, según la definición de la Real Academia de la Lengua Española significa, *enterar, dar noticia de algo* y que en términos legos hubiera significado tan sólo una simple acumulación de datos, se ha ampliado, transformándose *en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico*[167], por ello la informática estudia el tratamiento automático de la información, utilizando dispositivos electrónicos y sistemas computacionales; siendo claro que todos los aparatos informáticos son electrónicos, y como parte esencial el flujo de corriente eléctrica para transformarlo en otro tipo de energía de ambos, siendo el procesamiento de información, el que da nacimiento a la informática. Existen otras conceptos más técnicos como para el Diccionario de informática y telecomunicaciones, que es tenida como *una rama del saber humano que se ocupa de todo lo relacionado con las ordenadores, su comportamiento, su diseño y*

[165] Diccionario de informática y telecomunicaciones, Inglés-Español, Editorial Ariel S.A., Barcelona, España 2001, pág. 131.

[166] MAGLIONA MARKOVICTH, Claudio, *Delincuencia y fraude informático*, Editorial Jurídica de Chile, Santiago de Chile, 2014, pág. 19.

[167] GUTIÉRREZ FRANCÉS, María Luz, *Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa*, En MAZUELOS COELLO, Julio, *Derecho Penal Económico y de la Empresa*, Editorial San Marcos, Lima, 2014, pág. 383.

desarrollo de todo tipo de programas de dichas maquinas[168]; desde los sistemas operativos hasta los más modesto programas de aplicación operación y uso de ordenadores[169].

Sumándose a lo anterior también se puede agregar lo que indica la enciclopedia de la seguridad informática, la cual refiere que es la interpretación y procesamiento lógico de los impulsos eléctricos de manera ordenada[170].

5. Bases en las cuales se emplaza la informática y las telecomunicaciones

Es necesario destacar en forma general características de la informática y las telecomunicaciones, que son los pilares sobre los cuales descansa lo anteriormente señalado, a saber la forma en que se representa los mensajes que, el conducto por los cuales dicho mensaje se tramiten; los medios de comunicación y sus contenidos, es decir digitalización, las redes informáticas y la convergencia.

5.1. Digitalización

[168] En cuanto a la informática jurídica, dicha disciplina que enlaza una metodología tecnológica con su objeto jurídico, tendiente a socializar el conocimiento del Derecho, para hacerlo más común a todos los ciudadanos, mediante una racionalización lógica y tecnológica. CAICEDO, Fernando, / RIVERA LLANO Abelardo / PÉREZ LUÑO, Antonio, *Curso de informática jurídica*, Editorial Tecnos, Bogotá, 1998, pág. 22.

[169] Diccionario De Informática y Telecomunicaciones, inglés-español. Editorial Ariel S.A. Barcelona, España 2001, pág. 131.

[170] GÓMEZ VIEITES, Á, *Enciclopedia de la seguridad informática*, Editorial Alfa-Omega Ra-Ma, México, 2007.

Esto se refiere al paso del mundo analógico al digital, puesto que con ello se pudo separar el contenido del mensaje de su soporte, cambiando entonces la obligación de la materialidad y la conservación de lo que se escribía pudiendo entonces ahora saltar las barreras geográficas y difundir información simultánea a millones destinatarios. Además de ello se logró con la información digital almacenar gran cantidad de información respaldando su vez copias que antes eran imposibles, copias tanto de audio de imagen o de cualquier dato que pudiera ser necesario[171].

5.2. Nuevas redes informáticas

Primeramente en los inicio de la informática existían ordenadores fijos que permitió el reemplazo de la mano de obra, para muchísimos cálculos repetitivos que

[171] HERRERA BRAVO, nos entrega un ejemplo que demuestra la importancia de dicho cambio. "Un reloj analógico marca las horas, los minutos y los segundos con una constante variación en la posición de sus manijas, representando el tiempo de forma continua. Con la magnitud analógica es posible ir fraccionando los segundos en unidades cada vez más pequeñas, en forma infinita, con lo cual se obtiene un grado de precisión muy alto, pero también muchas variables que son difíciles de manejar. Un reloj digital, en cambio, muestra el paso entre cada segundo de modo discreto, es decir, sin continuidad, saltando de número en número, sin admitir valores intermedios entre cada segundo. Así, desde el segundo 58 se pasa al 59 sin mostrar las centésimas, milésimas u otras fracciones más pequeñas que existen entremedio. Por lo tanto, es más impreciso, pero mucho más simple para trabajar con esos datos. Esa simpleza de la magnitud digital se buscó para la representación informática de los datos. Por eso, para codificar instrucciones a las máquinas, convencionalmente se optó por la baja cantidad de variables que ofrece el sistema de numeración binario, prefiriéndolo por sobre el sistema decimal que utilizamos. La justificación parece bastante clara, es mucho más fácil diseñar circuitos y más eficiente su uso, si los valores o estados posibles se reducen a sólo dos: 0 ó 1, sí o no, verdadero o falso, encendido o apagado. HERRERA BRAVO, Rodolfo, *Ciberespacio, sociedad y derecho*, En revista chilena derecho informático, U. De Chile, número 3, Santiago de Chile, 2003, pág. 5.

se conectaban a ordenadores centrales. Posteriormente se crearon los ordenadores autónomos los cuales podían también procesar diferentes datos mejorando con ello la productividad. Por último se creó Internet y otras redes informáticas públicas y privadas naciendo con ello el usuario conectado a la red, aumentando las posibilidades servicio, y la calidad de la información.

Lo anteriormente señalado corresponden a tres grandes paradigmas que experimentaba la tecnología en información, y que ha aumentado de una u otra manera la forma en que las personas se comunican puesto que para enviar cualquier tipo de información o mensaje se requiere de alguna día o canal para que este pueda circular[172].

5.3. Convergencia[173]

[172] BARROS, Óscar, *Tecnologías de la información y su uso en gestión*, Editorial McGraw Hill, Santiago, 1998, pág. 1-6, citado por HERRERA BRAVO, Rodolfo, Ciberespacio, sociedad…op. Cit. 2003, pág. 6.

[173] La Unión Europea en el Libro Verde sobre la Convergencia de los Sectores de Telecomunicaciones, Medios de Comunicación y Tecnologías de la Información y sobre sus Consecuencias para la Reglamentación, la define y señala Tradicionalmente, cada medio de comunicación ha venido constituyendo un sector independiente. Existían servicios, muy diferentes, de radiodifusión, telefonía vocal e informática en línea. Estos servicios funcionaban en redes diferentes y hacían uso de plataformas distintas: televisores, teléfonos y ordenadores. Cada uno de ellos estaba regulado por su legislación propia y por reguladores diferentes, normalmente de nivel nacional. Sin embargo, la tecnología digital actual permite transportar una capacidad sustancialmente más elevada de servicios tradicionales y nuevos por las mismas redes y utilizar dispositivos integrados de consumo para aplicaciones tales como la telefonía, la televisión o la informática personal. Entonces la define como *la capacidad de diferentes plataformas de red de transportar tipos de servicios esencialmente similares*. Comisión Europea, *Libro Verde sobre la Convergencia de los Sectores de Telecomunicaciones, Medios de Comunicación y Tecnologías de la Información y sobre sus Consecuencias para la Reglamentación*, Bruselas, diciembre de 1997. [accesible en] <http://www.europa.eu.int>.

Se refiere al hecho que ya no sólo el usuario está conectado de forma exclusiva a la red informática mediante un solo ordenador personal, sino que a una multiplicidad de dispositivos. Se suma a ello, la posibilidad de conectarse a redes inteligentes remisión de datos, tanto de voz o imagen. La convergencia podemos decir que se trata de una característica que presenta la actual desarrollo de la infraestructura de red y de los dispositivos terminales, que les permite, B.C. a su naturaleza diversa, transmitir y recibir, en esencia, la misma información, todo ello girando en torno a la digitalización de lo contenido que se tramiten y conduciendo ineludiblemente a una transformación de la actividad económica que desarrolla en forma separada las empresas de telecomunicaciones, de informática y de contenidos audiovisuales[174].

La sociedad de la información se extiende, incluyendo progresivamente vastos segmentos sociales y ampliando el espectro de su funcionalidad a acciones y actividades que tienden a tener significativas consecuencias jurídicas. Toda la tecnología disponible hace incrementar la tendencia la convergencia de las TICs., Proceso en el que la radio, la televisión, la telefonía fija y móvil e internet tienden a fusionarse en una sola red digital[175], ámbito en el que el derecho tiene que producir progresos equiparables a dicho avance.

Todo esto se presenta por la inexistencia de límites territoriales para la comunicación, donde muchas veces el usuario desconoce la localización física de su

[174] LESSIG, Lawrence, *El Código y otras leyes del ciberespacio*, Editorial Grupo Santillana, Madrid, 2001, pág 23 y sigs.

[175] OLIVERA, Noemí, *El sistema jurídico de la sociedad de la información procesos y tendencias*, En la sociedad de la información en Iberoamérica. (coordinadora) ARELLANO TOLEDO, Wilma, Editorial INFOTEC, 1ª edición, México, 2012, pág, 57.

interlocutor con todas las consecuencias jurídicas que ello trae, como son la ley aplicable y la judicial competente. De esta relación muchas veces el internauta puede resultar involucrado en términos jurídicos, que muchas veces le desconocida, o más aun estando involucrado en algún delito informático[176] [177].

[176] Los pioneros proclamaron el *fin del derecho*, llamado sucumbir frente a la tecnología; en palabras de la LESSIG, Lawrence, "el código [de programa] en la ley". Si bien el código de programa puede imponer ciertas restricciones a que lo utiliza, lo cierto es que, a diferencia de aquellas que involucran el acceso a contenidos disponibles en la red, mucha de la actividad jurídicas mediadas por las TICs., no son afectadas por el software que las hace posibles, de modo que no puede sostenerse válidamente que, para aquéllas, el código de programación la ley. OLIVERA, Noemí, *El sistema jurídico de la sociedad…*op. cit. pág. 59.

[177] Vale indicar lo indicado por HERRERA BRAVO, al entregar un catálogo de los cambios más significativos la tecnología de información: "1) el cambio de lo analógico a lo digital, que ya expliqué al considerarlo como uno de los tres pilares; 2) el paso de la tecnología tradicional de semiconductores a la de microprocesadores, atendido que con ello se logró un procesamiento de alto rendimiento para organizaciones de alto desempeño; 3) el reemplazo del ordenador de tipo anfitrión por la de cliente/servidor, íntimamente relacionada con el paradigma del usuario conectado en red, aunque sea más preciso vincularla con el paso desde el paradigma del procesamiento de datos al de información; 4) el cambio de escenario desde la banda estrecha a la autopista de información, ya que gracias a un mayor ancho de banda es posible la transmisión de contenidos diversos que faciliten la interactividad; 5) la transformación de dispositivos de acceso no inteligente, como la televisión, el teléfono o el terminal computacional, por el dispositivo de información representado por el ordenador personal, y ahora por otros que son una expresión de la convergencia tecnológica; 6) el paso desde los datos, texto, voz e imagen separados a la multimedia, de modo de permitir comunicaciones completas; 7) el reemplazo de los sistemas propietarios por los sistemas abiertos, porque permite la interoperabilidad sin tener que utilizar un mismo tipo de sistema operativo, de aplicaciones o de equipos; 8) el cambio de las redes no inteligentes a las que sí lo son por utilizar hipermedia y agentes o *knowbots* que navegan buscando la información que el usuario les ha solicitado; 9) la sustitución de la computación de tipo artesanal por la computación orientada a los objetos, es decir, pasar del desarrollo de programas de software grandes y complejos, a conjuntos de software (objetos) que se desarrollan en formas estándares y con comportamientos e interfaces estándares; y 10) la variación de la interfaz gráfica de usuario a la interfaz multimedia de usuario y a nuevos ambientes de cooperación como dimensiones o calabozos multiusuario y la realidad virtual. HERRERA BRAVO, Rodolfo, *Ciberespacio, sociedad y derecho…*op. cit. pág 6.

6. Derecho informático e informática jurídica

La relación entre derecho informática tiene dos líneas de investigación, primero los aspectos normativos del uso de la informática, desarrollado bajo el derecho del informática, y la aplicación del informática en el tratamiento de la información jurídica, conocida como informática jurídica. Por ello para que exista desarrollo de la informática jurídica e necesario que se tengan en consideración elementos de origen como son la aplicación de la lógica del derecho o raciocinio jurídico; análisis del discurso jurídico; aplicación de la teoría los sistemas; aplicación de la teoría de información entre otros, siendo estos elementos la base fundamental para para la informática jurídica.

Para el desarrollo de la de la misma informática jurídica se tiene como principal función la ordenación que lleva su tratamiento y el análisis del discurso jurídico el cual se anexan estudios de lenguaje jurídico ya la creación de instrumentos que permitan el acceso a la información jurídica, puesto que el discurso jurídico está basado sistema normativo, que parte de proposiciones lógicas en cuanto al ser y al deber ser, y de la combinación en una cierta estructura surge el ordenamiento jurídico, que constituye el mismo objeto de la ciencia el derecho[178].

Así las cosas, la informática jurídica, es una ciencia que se desprende del Derecho, para el estudio no sólo de las normas jurídicas que dictaminan y regulan el ambiente informático, sino que también abarca en ese estudio a todo el material

[178] RÍOS, ESTAVILLO, Juan, *Informática jurídica,* [accesible en], <www.revistas.juridicas

doctrinario y jurisprudencial que trate esta materia, para lograr un mejor control, aplicación y vigencia del ámbito informático.

Con el paso del tiempo y la evolución de las sociedades fue necesario que se inventara técnica mediante las cuales, las tareas rutinarias pudieran ser sustituidas o aminorarlas en su tiempo de realización, con la utilización de herramientas, dando origen entonces a la *automática*, ciencia que trata de la sustitución del operador humano por un operador artificial en la ejecución de una tarea física o mental previamente programada[179].

El derecho informático, no corresponde simplemente a la interrelación entre el derecho informática, puesto que la relación entre ambos es compleja y de constante movilidad, puesto que más que combinarse entre ellos deben integrarse, naciendo de dicha comunicación, otros campo de estudios como son los contratos electrónicos, el derecho de Internet, y por supuesto los delitos informáticos.

El derecho ajeno a los cambios de la vida social, y con los nuevos sistemas de comunicación y el trazado de redes han cambiado la configuración territorial y política de los Estados, puesto que la clásica noción de espacio con las tecnologías de la comunicación ha cambiado, entrando en crisis la dimensión normativizada hora en cuanto al derecho se trata. Existe en día una autorregulación por parte los sujetos, que se basa en supuestos de ilegalidad relacionados con las TICs, toda vez que los estados nacionales han perdido control normativo en esta nueva sociedad informacional[180].

---

[179] PRIETO ESPINOSA, Alberto, *Introducción a la informática*, 3ª edición, Editorial Mc Graw Hill, España, 2002, pág. 647.

[180]RODRÍGUEZ VILLASEÑOR, Isabel / GÓMEZ GARCÍA, Juan, *Investigación y documentación jurídicas*…op. cit. pág. 57 y sigs.

La principal influencia del derecho en la conformación y el desarrollo de la sociedad información viene dada por el llamado Derecho de las TICs, siendo esta nueva escena jurídica el más importante modo de incidencia de la normativa jurídica en los procesos láseres sociales propias del nuevo modelo social, ya que aquí es donde se manifiesta de forma casi exclusiva su auténtica capacidad de su potencialidad reguladora del nuevo marco socio jurídico.

De acuerdo lo anterior, la *informática jurídica*, es el ámbito de las TIC donde se manifiestan de manera más clara o las repercusiones derivadas de la aplicación de esta nueva tecnologías al derecho, como son lo que respecta la seguridad jurídica, y su nueva forma de aplicación. Esta rama del derecho, estudia el tratamiento automatizado de las fuentes del conocimiento jurídico, las fuentes de producción jurídica y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho[181]. Dentro de esta lógica, resulta evidente que es la rama del Derecho que fue creada para el abordaje de temas tecnológicos, se ha denominado informática Jurídica. Entendida como la técnica interdisciplinaria que tiene como objeto el estudio y aplicación de la informática general en la recuperación y aprovechamiento de la información jurídica, así como la elaboración de los instrumentos de análisis y tratamiento de esta información. También se ha dicho que es la aplicación de los sistemas computacionales en todas las ramas y enfoques de derecho. Para el autor, CÁCERES NIETO, consiste en la utilización de

[181] No se desconoce sin embargo que su desarrollo y evolución puedan conllevar a que las máquina de cómputo procese informaciones y establezca inferencias lógicas, cuyo fin generaría la suplantación plena del razonamiento jurídico del juez o del abogado, aunado al hecho que no es infalible, por lo que el abogado o jurista, deben asumir su responsabilidad por decisiones judiciales erróneas, debido a la inferencia de análisis lógico-matemático realizado por un ordenador. PÉREZ LUÑO, Antonio, *Ensayos de Informática Jurídica*, Editorial Biblioteca de Ética, Filosofía del Derecho y Política, México, 1996, pág. 41.

conceptos, categorías, métodos y técnicas propias de la informática en el ámbito de lo jurídico[182].

Se suele confundir al Derecho de la informática con la informática jurídica, que no es sino aplicar los sistemas informáticos a la resolución de problemas específicos de los profesionales del Derecho, como puede ser la búsqueda de información documental o la tramitación de asuntos, por ejemplo. La informática jurídica es la tecnología que se ocupa del problema jurídico, sea a través de la creación de bases de datos jurídicos, de programas para la gestión propia de los profesionales del Derecho, o incluso, a través de sistemas informáticos que apoyan la toma de decisiones jurídicas. No es derecho informático, no es norma jurídica, no es derecho[183].

B) Aspectos más relevantes relativos a Internet

Sin desconocer que en lo que comporta a la cibernética e informática, han sido numerosos los avances en beneficio de la sociedad en todos los aspectos;

[182] CÁCERES, Nieto, Enrique, *Lógica jurídica e información jurídica*, Revista de la facultad de Derecho Universidad Complutense, informática y derecho, monográfico 12, Madrid, pág. 33.

[183] Caben diversas versiones, expresión a su vez de la posible aplicaciones de la informática y derecho así se podrá hablar de: *informática jurídica de gestión,* la cual constituye una aplicación referente al uso de la informática la actividad de la excepcionalidad de cotidiana de la industria jurídicas, como son la miseria pública, registros, tribunal; *informática jurídica documental,* la cual permite el procesamiento, tratamiento recuperación de la documentación jurídica, ya sea legislativa, jurisprudencial, doctrinal previamente almacenada en soporte informático. Y es aquí donde se incardinar de manera central toda la problemática relativa a la documentación jurídica en el contexto de la sociedad información; *informática jurídica decisional,* su propósito es el uso de los medios informáticos para la obtención de esencia jurídica válidas y justas. Rodríguez Villaseñor, Isabel / Gómez García, Juan, *Investigaciones y documentación jurídicas*…op. cit. pág. 60.

facilitándonos a través de un ordenador multiplicidad de actividades de uso cotidiano tales como el pago de los servicios bancarios, la solicitud de préstamos a instituciones financieras, el pago de boletos para un espectáculo, la consulta de bibliotecas enteras en cualquier parte del mundo; el almacenar y guardar información confidencial, la celebración de contratos informáticos, el uso de diversos medios de comunicación como la telefonía inalámbrica y celular, o como procesador de palabras; en todas y cada una de estas actividades meramente enunciativas, es claro que el ordenador se ha convertido en una necesidad que implica la sistematización de información ya sea confidencial, clasificada, de uso público o de recopilación extra curricular.

La base de datos con fines económicos y administrativos han creado una relación de dependencia con las empresas, haciéndolas vulnerables a posibles atentados, que generan daños y pérdidas económicas. De manera que tal almacenamiento, requiere de una especial seguridad; la primera es la seguridad física concerniente a la estructura que sustenta la base de datos, como lo son soportes magnéticos *diskettes*, ópticos *CDRoom* y las mismos ordenadores; un segundo problema de seguridad, surge cuando se efectúan transferencias de datos transfronterizos; que exigen una constante comunicación, lo que comporta beneficios económicos que sólo genera el mundo digital, pero a su vez conlleva problemas sociales y culturales debido a sabotaje en la información.

Las bases de datos, son usadas con fines administrativos, de control, académicos e incluso económicos; esta digitalización de base de datos, tiene 3 problemas fundamentales básicos por resolver, en primer lugar el derecho de autor del material almacenado en los bancos de datos, la autorización sobre el uso de sus obras y otorgar la facultad de administrar la base datos; en segundo lugar el derecho originado a los productores de la base de datos por la sistematización y elaboración; por último los derechos y obligaciones derivados entre la relación del creador,

distribuidor y usuario, este último al ser consultado y ser adquirido. De manera que esta transferencia y uso de almacenamiento de datos ha generado nuevos problemas en los que el Derecho tiene que enfocarse como el uso ilícito de datos, intercepción de datos, revelación de información confidencial, control y alteración de documentos fuente, extravío de información, tarifas y régimen fiscal, atentados contra las soberanía de los Estados, regulación de contratos que rodean a la información, propiedad intelectual de la información difundida, seguridad jurídica de las empresas y en muchos casos de los usuarios. Ello haciendo mención sólo al uso, desuso y abuso de la base de datos, como quiera que hoy en día se calcula que existen, más de 2 billones de usuarios de internet en todo el planeta, siendo un medio de comunicación social masivo, mediante el cual los seres humanos se comunican, trabajan, estudian, encuentran entretenimiento y efectúan diversas actividades; actividad a la cual grandes y chicos tienen acceso.

La nueva forma de comunicación masiva, permite innumerables avances y acorta impensables distancias, por lo cual, su uso, hoy por hoy es de primera necesidad en las economías mundiales, las cuales fungen también como presas fáciles de los adiestrados cibernautas que ante los incautos consumidores, realizan las más improbables maneras de delinquir de manera rápida y segura, dada la precariedad de las instituciones gubernamentales y de la justicia en general, de enfrentar con eficacia esta peculiar manera de delinquir[184].

Internet se ha convertido en un amplio mercado negro, al que puede acceder cualquier comprador o vendedor de armas, ofreciendo confidencialidad y movilidad

[184] El problema cambia sus características o sus formas, sin embargo la esencia prevalece, la unidad delictiva se conserva y es donde se debe de ahondar. Es necesario revisar los factores y las circunstancias que le dan vida a una conducta injusta, luego, a partir de sus caracteres se puede clasificar la misma, distinguiéndola de sus figuras o tipos penales afines. La tecnología ha dado esta tarea urgente, pues cada vez más se depende de este desarrollo tecnológico. AMUCHATEGUI REQUENA, Griselda, *Derecho Penal*, Tercera Edición, Oxford, México, 2005, pág. 61.

desde cualquier parte del mundo bajo la apariencia de compras lícitas llevadas a cabo mediante el anonimato de la Internet.

A medida de que el uso indebido de computadoras fue creciendo a partir de la expansión de redes, los Estados se vieron en la necesidad de modernizar su legislación de acuerdo con las emergentes modalidades criminales, lo que obligó a que los gobiernos incorporaran en su normativa los delitos informáticos, incluyendo nuevas figuras que otorgaran a la información un bien para proteger. En otros países, sin embargo, aplicaron los tipos penales convencionales para la protección, como por ejemplo los delitos contra la propiedad cuando el bien afectado eran las computadoras personales o delitos contra la intimidad, para el caso de la interceptación del correo electrónico como correspondencia personal.

1. Origen[185] y desarrollo

Como en muchas otras situaciones, no se puede señalar a una sola persona como el inventor o el padre de Internet, sino que fue el trabajo de muchos durante muchos años lo que desembocó en el nacimiento de Internet, la red de redes, la madre de todas las redes, la red de comunicaciones que disfrutamos todos los días y que, como veremos a continuación nació a partir de una red de ordenadores llamada ARPANET[186].

[185] Atribución y derivado de Actívate, Google España", [accesible en] http://google.es/acti.

[186] ROJAS AMANDI, Víctor, *El uso Internet en el derecho*, 1ª Edición Editorial, Oxford, México, 2001, pág. 2.

Aunque se ha repetido hasta la saciedad que internet tiene su origen en un proyecto militar estadounidense para crear una red de ordenadores que uniera los centros de investigación dedicados a labores de defensa en la década de los 60 en los Estados Unidos y que pudiera seguir funcionando a pesar de que alguno de sus nodos fuera destruido por un hipotético ataque nuclear, los creadores de ARPANET, la red precursora de Internet, no tenían nada parecido en mente y llevan años intentando terminar con esta percepción.

Internet surgió con el fin de poner a disposición de IPTO, la oficina para la tecnología de procesado de la información, precisamente recursos informáticos, toda vez que se trataba de darle otro uso a las grandes máquinas calculadoras, puesto que todo lo investigadores y los laboratorios de informática trabajaban en forma independiente con ordenadores propios, con ello se duplicaban los esfuerzos.

Robert TAYLOR[187], en 1966, fue nombrado director del IPTO, tuvo la idea de conectar todos los ordenadores entre sí, construyendo enlaces electrónicos entre diferentes máquinas, para que la persona que fuere analizando investigaciones en distintas lugares, pudieran compartir los recursos obtenidos, con ello la ARPA[188], podría unificar esfuerzos solamente en un par de lugares instalando ordenadores potentes enlazados. Lo que se necesitaba era implementar una red pequeña con cuatro nodos, para aumentar la posteriormente, sin embargo se producía un inconveniente el cual era que se debían comprar ordenadores pero existían inconveniente con las leyes existentes y también las necesidades técnicas a la hora de obtenerlos, por oposición del departamento de defensa del que a su vez dependía

[187] C. R. LICKLIDER en un artículo llamado Man-Computer Symbiosis

[188] Agencia para Proyectos de Investigación Avanzados, agencia de la que dependía la IPTO de Roberts TAYLOR; hoy en día se llama DARPA, por sus siglas en inglés, Agencia de Proyectos de Investigación Avanzados de Defensa.

ARPA, y además que debían ser ordenadores de un mismo fabricante para poder estandarizar el trabajo de los mismos, es decir había que solucionar el problema de la *terminal*[189], puesto que se debían utilizar procedimientos distintos para acceder a cada tipo ordenador.

Con la creación de la *World Wide Web*[190][191] en 1990[192], como el servicio más popular de la red y la liberalización de la red, en 1995, por parte de la administración

[189] Es un aparato, situado en la periferia de la unidad central y a distancia, que permite la salida de datos que se solicitan al sistema global. Hay también terminales activos que, mediante un teclado u otro dispositivo, pueden entrar datos al sistema. Además, cierto tipo de terminales pueden ejecutar algunas operaciones de tipos generales o especializados. Llamado erróneamente módem (Dispositivo externo que se encarga de la interfaz entre la línea ISDN (Integrated Services Digital Network, Sistema para transmisión telefónica digital, con línea y adaptadores especiales para ISDN es posible conectarse a internet y cualquier equipo digital compatible con ISDN). No es un realmente un módem porque no modula ni demodula señales. Permite, por ejemplo, conectar la computadora (una terminal) a una red ISDN. [accesible en:] http://www.lawebdelprogramador.com-http://www.alegsa.com.ar.

[190] Sistema de hipertexto que funciona sobre Internet. La información se visualiza mediante la aplicación llamada *navegador web,* que se utiliza para extraer elementos de información comúnmente nominados documentos o páginas web de los servidores web o portales y mostrarlos en la pantalla el usuario. El usuario puede entonces seguir hiperenlaces que la página o a otros documentos e incluso enviar información al servidor para interactuar directamente con él. A la acción de seguir esta clase se le suele llamar navegar por la web. Comúnmente se confunde la web con Internet que la red física mundial sobre la que circula la información. [Accesible en] <http:/www.3.org/Berners-Lee.html>.

[191] BERNERS-LEE, Tim, Británico, Licenciado en la Universidad de Oxford, trabajó en el CERN en los ochenta, comenzó a diseñar un programa, *Enquire,* que permitiera almacenar y recuperar información mediante asociaciones no deterministas. Partiendo de ese programa, en octubre de 1990 emprendió la elaboración del HTML6, que permite combinar texto, imágenes y establecer enlaces a otros documentos, además crea el primer servidor World Wide Web y el primer programa cliente WorldWideWeb. TRIGO ARANDA, Vicente, *Historia y evolución de internet*, En Autores científicos-técnicos y académicos, Madrid, pág. 3, [accesible en], <http://www.acta.es>.

[192] En 1994, las primeras restricciones a la actividad comercial en Internet se relajaron. Esto, junto con la creciente popularidad de la web, ocasionó una explosión en el uso personal y comercial de Internet durante la década de 1990. Los PSI comerciales conectaron a los usuarios con Internet y a una gama en constante expansión de herramientas y servicios de información. A mediados de la década de 1990 se vio el ascenso de las primeras compañías de gran tamaño auténticamente basadas en Internet, principalmente motores de búsqueda, que ayudaron a darle sentido al gran acervo de información que ahora estaba disponible. Yahoo!, fundada en 1994, fue

norteamericana, se amplió definitivamente el espectro de usuarios a escala global más allá de los ámbitos gubernamentales y académicos. Con la aparición de la Web y su posterior expansión mundial, nuevas aplicaciones fueron surgiendo sobre la base de los avances en la informática interactiva surgida desde mediados de los 90 en Silicón Valley, Estados Unidos.

La flexibilización digital trasforma internet en una tecnología *maleable* en cuanto a su estructura y configuración, lo que representa la clave del éxito de esta tecnología. Para CASTELLS, el carácter abierto de la arquitectura de internet constituyó su principal fuerza, y su desarrollo autoevolutivo permitió que los usuarios se convirtieran en productores de tecnología y en configuradores de la red[193].

A partir de su expansión global, Internet fue exportada a diferentes sociedades y culturas que le asignaron usos diversos de acuerdo con sus costumbres y valores. Si bien es una red global con presencia de gobiernos, empresas, comunidades y usuarios particulares, los usos de Internet son básicamente individuales y se encuentran en constante evolución.

Al convertirse la Internet en un sistema abierto, éste realiza dos funciones importantes la primera como medio de comunicación y la segunda como medio de información. Como medio de comunicación, la red entre computadores permite la comunicación entre sí y entre los usuarios realizada mediante cable telefónico o conexión por línea de alta velocidad o banda ancha DSL, debido a esto cualquier

---

uno de los primeros líderes, seguida de Google en 1998. UNODC (United Nations on Drugs and Crime), Estudio exhautivo sobre le delito cibernético Oficina De Las Naciones Unidas Contra La Droga y El Delito, Naciones Unidas, Nueva York, 2013, pág. 320.

[193] CASTELLS, M, *La galaxia, reflexiones sobre Internet, empresa y sociedad*, Editorial Areté, Barcelona, 2001, pág. 42.

ordenador puede conectarse a internet sólo debe contar con el respectivo *modem*[194], y un servidor de un proveedor de internet el cual debe tener acceso a la espina dorsal del mismo internet, (*backbone*)[195].

En cuanto a su diseño, es un medio de comunicación *descentralizado*, ya que no posee una unidad central que concentre el tráfico de información, sino una serie de nodos distribuidos geográficamente que operan para el intercambio de mensajes. Las redes que componen Internet poseen su propia configuración y se clasifican en diferentes tipos de acuerdo con el área geográfica o topología.

Existen redes de área local *lam*[196] y redes de red amplia *wan*[197], como así también redes de área metropolitana, redes de área global y redes de área personal, entre otras. Las unidades mínimas de información digital son los bits, contracción de Binary Digit o Digito Binario en inglés, el elemento básico de los ordenadores e internet. A diferencia de las tecnologías analógicas, las comunicaciones digitales son más flexibles en tanto que, como señala NEGROPONTE, del Instituto de Tecnología de Massachusetts, *un bit no tiene color, ni tamaño, ni peso y puede desplazarse a la*

[194] MOdulador-DEModulador: Periférico de entrada/salida, que puede ser interno o externo a un ordenador, y sirve para a conectar una línea telefónica con el ordenador. Se utiliza para acceder a internet u otras redes, realizar llamadas, etc. Los datos transferidos desde una línea de teléfono llegan de forma analógica. El módem se encarga de *demodular*, para convertir esos datos en digitales. Los módems también deben hacer el proceso inverso, *modular* los datos digitales hacia analógicos, para poder ser transferidos por la línea telefónica.

[195] Mecanismo de conectividad primario en un sistema distribuido. Todos los sistemas que tengan conexión al backbone (columna vertebral) pueden interconectarse entre sí, aunque también puedan hacerlo directamente o mediante redes alternativas.

[196] (*Local Área Network*). Red de área local. El término *lan* define la conexión física y lógica de ordenadores en un entorno generalmente de oficina. Su objetivo es compartir recursos (como acceder a una misma impresora o base de datos) y permite el intercambio de ficheros entre los ordenadores que componen la red.

[197] (*Wide área Network*) Red de Área Extensa.

velocidad de la luz. Es el elemento atómico más pequeño en la cadena de *Adn* de la información, que describe el estado de algo, es decir encendido o apagado, verdadero o falso, arriba o abajo, adentro o afuera, blanco o negro[198].

La web ha permitido una descentralización repentina y extrema de la información y de los datos. Algunas compañías e individuos han adoptado el uso de los *weblogs*[199], que se utilizan en gran parte como diarios actualizables. Algunas organizaciones comerciales animan, a su personal para incorporar en sus áreas de especialización en sus sitios, con la esperanza que impresionen a los visitantes con conocimiento experto e información libre.

Por otro lado, la *WWW*[200], es un conjunto de protocolos que permite de forma sencilla, la consulta remota de archivos de hipertexto. La *web* fue un desarrollo posterior y utiliza internet como medio de transmisión. La funcionalidad elemental de la *web* se basa en tres estándares básicos: (URL), *Localizador Uniforme de Recursos*, que especifica cómo a cada página de información se asocia a una dirección única y en dónde encontrarla. (HTTP), *Protocolo de Transferencia de Hipertexto* que especifica cómo el navegador y el servidor intercambian información en forma de peticiones y respuestas. (HTML), *Lenguaje de Marcación de Hipertexto*

[198] BEDROPONTE, Nicholas, *Ser Digital*, Editorial Atlántida, Buenas Aires, Argentina, 1995, pág. 21.

[199] Blog o bitácora. Es un sitio web personal donde se escriben periódicamente, como un diario on-line, sobre distintos temas que le interesan al propietario. Cada escrito está ordenado cronológicamente y en general posee enlaces a otras páginas para ampliar el tema que se habla.

[200] Siglas para World Wide Web: (www) Telaraña mundial, desarrollada junto con el HTML, la URL y el HTTP (elementos indispensables de la www), en 1990 por Robert CAILLIAU y Tim BERNERS-LEE, en el CERN en Suiza. Permite incorporar multimedia e hipertextos en internet, dando origen a la Web como la conocemos. En cuanto a CERN, corresponde a la sigla provisional utilizada en 1952, que responde al nombre en francés Conseil Européen pour la Recherche Nucléaire, es decir, Consejo Europeo para la Investigación Nuclear), hoy *Organización Europea para la Investigación Nuclear*. [accesible en:] <www.csic.es>.

un método para codificar la información de los documentos y sus enlaces y puede referirse a una *web* como una página, sitio o conjunto de sitios que proveen información por los medios descritos, o a la *web*, que es la enorme e interconectada red disponible prácticamente en todos los sitios de la internet. Para el acceso a Internet se cuenta con aproximadamente 5000 redes en todo el mundo y, más de 100 protocolos distintos basados en TCP/IP, que se configura como el protocolo de la red. Los servicios disponibles en la red mundial de PC, han avanzado gracias a las nuevas tecnologías de transmisión de alta velocidad, como DSL y wireles, se ha logrado unir a las personas con videoconferencia, ver imágenes por satélite; observar el mundo por webcams, hacer llamadas telefónicas gratuitas, o disfrutar de un juego multijugador en 3D, un libro *PDF*, o álbumes y películas para descargar[201].

2. Concepto de internet [202]

Entre los generales se concibe internet[203], como el sistema de acceso a información más completa del mundo, sistema de comunicación más veloz y con mayor capacidad de creación que se conozca estas son sus funciones principales per

[201] FERNÁNDEZ, R. *Origen y Evolución Histórica del internet*, 1997, [accesible en] http://www.solociencia.com.

[202] Atribución y extracto de Actívate, Google España", [accesible en] http://google.es/acti.

[203] Internet es una *combinación* de redes que se comunican entre sí. La palabra *Internet*, en sí implica la abreviatura de *inter-networking*, que puede traducirse, como la conexión entre que están compuestas de ordenadores individuales, desde los domésticos hasta supercomputadoras, que hablan entre sí, a través de una infraestructura mundial de cables físicos y enlaces inalámbricos. UNODC (United Nations on Drugs and Crime), Estudio exhautivo sobre le delito cibernético Oficina De Las Naciones Unidas Contra La Droga y El Delito, Naciones Unidas, Nueva York, 2013, pág. 314.

internet tiene también otras innumerables funciones. Igualmente se puede decir que su medio intercambio de bienes que permite el uso de comercio electrónico a cualquier usuario ampliándolo así desde las redes de comercio electrónico cerradas razón por la cual lo masificado generando innumerables fuentes de trabajo, permite la realización de las escenas bancarias, y otra innumerables fiscal y tributaria. Además permite el desenvolvimiento del joven electrónico[204].

Por otro lado, podemos decir que Internet es un sistema global descentralizado de redes de cómputo interconectadas entre sí con base en los estándares o protocolo conocido como protocolos de transmisión de control (TCP) y el protocolo Internet (IP), que se utilizan para transmitir e intercambiar paquetes de datos[205]. Además se puede agregar que internet representa un conjunto de redes independientes que se encuentran conectadas entre sí. Sus principales características son: la interactividad, la libre elección de contenidos y la ausencia de una autoridad de control[206].

Vale señalar, que internet como se dijo anteriormente es conocida como la red de redes o simplemente una red que es un conjunto descentralizado de redes de comunicaciones interconectadas. Por ello internet permite que redes de diferentes tipos, lo que se llaman redes físicas heterogéneas, puede conectarse entre sí, permitiendo que un usuario pueda conectarse a Internet, a través de una red

[204] Gobierno electrónico: uso de tecnologías de información por parte de la administración estatal para mejorar los servicios y las informaciones que se ofrecen a los ciudadanos, aumenta la eficiencia y eficacia la gestión pública, incrementar la transparencia sector representa la participación ciudadana. PINOCHET CANTWELL, Francisco, *Los principios especiales del derecho internet*, Editorial el jurista, Santiago de Chile, 2015, pág 28.

[205] VELASCO SAN MARTÍN, Cristos, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*, Editorial Tirant Lo Blanch, Valencia, 2012, pág. 33.

[206] HANCE, Oliver, *Leyes y negocios en la Internet, origen de la internet,* Editorial McGraw-Hill, México, 1996, pág. 12.

cualquiera de comunicación, como sería por ejemplo una red de telefonía por cable o una red de telefonía celular, o satelital. Siendo todo posible porque es de suma importancia para Internet y su funcionamiento, que no es la forma de conexión física lo principal, sino que lo más importante que la red permita una comunicación mediante el protocolo TCP/IP, es decir en este caso un protocolo como el antes indicado, es el lenguaje que empleando sistemas, dos ordenadores para comunicarse entre sí, dando un ejemplo de fácil entendimiento para que exista comunicación entre dos personas es necesario que hablan el mismo idioma, lo mismo ocurre dos sistemas para que puedan entenderse, es de además a veces, al igual como ocurre con la comunicación entre individuos es necesario un traductor, para que dichos sistemas puedan darse entender.

Por otro lado, podemos asimilar Internet a una carretera que tiene múltiples autopistas o interconexiones, y por ellas circulan los datos que se transmiten, por ello los datos que se transmiten emplear distintos idiomas (diferentes protocolos), entonces de acuerdo ello la World White web, la web, es solamente un sistema más con su protocolo, el cual es el protocolo HTTP, que hace a su vez el uso de Internet para la transmisión de los datos, y en este caso las páginas web. Se puede agregar que además del protocolo antes indicado también circulan por Internet otros como son el protocolo FTP, el cual se emplea para la trasmisión de ficheros o el protocolo SMTO y POP, que se usan para la recepción de correos electrónicos y el protocolo Telnet, el cual se emplea para conexiones remotas entre ordenadores. La web es el sistema ya explicado más utilizado por millones de usuarios por ello existe la confusión que Internet y la web sólo mismo[207].

[207] Atribución Google España: [accesible en] http://google.es/acti.

3. Ciberespacio[208]

El término adoptado tras la publicación de una obra de ciencia-ficción de 1080 82 del autor William GIBSON, denominada *Burning Chrome,* y popularizada a través de otra de sus obras del año 1984 titulada *Nouromancer,* durante los años 90, el término se comenzó a usar como sinónimo de internet, y posteriormente para referirse a World White web, especialmente en los círculos académicos donde se originó el protocolo IP. *Velasco San Martín*, hace referencia a John Perry Barlow, autor y fundador de la organización Electrónic, Frontier Foundation, el cual indica que aplicar el concepto de ciber espacio, erróneo puesto que el mismo es independiente y se encuentra fuera de los límites geográficos de la sobrina estatal,, y por ende fuera de control y la regulación gubernamental.

Hoy en día dicho concepto se utiliza para referirse a los contenidos actividades que acontecen en internet también se utiliza para referirse a distintas cosas o entidades que puedan estar inmersas en el mundo de las comunicaciones la tecnología, donde la ubicación física no es perceptible por los sentidos sin embargo se indica que se encuentra en dicho espacio, sabemos que está ahí pero no se puede percibir, utilizándose conceptos actualmente es como por ejemplo que la información se encuentra en la *nube*, refiriéndose entonces al ciberespacio[209].

---

[208] VELASCO SAN MARTÍN, Cristos, *La jurisdicción y competencia sobre delitos cometidos…* op. cit. pág. 36 y sigs.

[209] Una de las características de este ciberespacio es que está formado por información contenida en medios electrónicos de almacenamiento y que estos medios de almacenamiento son de orden físico, por lo que en última instancia esa información esa ubicada en cierto lugar físico territorial, pero puede ser accedida desde cualquier parte del mundo. ZABALE, Ezequiel, *La competencia en materia de acciones civiles o penales derivadas del uso de la red Internet*, Argentina, 2002, pág. 121. Citado por CASSOU RUIZ, Jorge, *Delitos informáticos en México*, En revista del Instituto de la judicatura Federal, Número 28, México, 2008, pág. 2.

En necesario hacer referencia que Estados Unidos de Norte América ha tratado de una u otra manera de regular este espacio virtual, puesto que como se indicaba anteriormente en forma teórica no existen límites jurista anales y tampoco regulación de los países y por ende del derecho, pero en el ciberespacio hoy en día se está utilizando por el cibercrimen para cometer todo tipo de actos ilícitos que a pesar de ser cometidos en este espacio que no está regulado y no es percibido, tiene consecuencias en el mundo real, por ello a continuación se dará un breve resumen de lo que ocurre en *Internet oscura, o internet oculta.*

4. La faceta oscura de Internet, algunas cuestiones relativas a criminalidad informática; internet profunda y monedas electrónicas

La dificultad que se presenta en el ordenamiento jurídico del mundo globalizado se manifiesta fundamentalmente porque la mayoría de las legislaciones penales fueron redactadas con el espíritu de proteger los bienes y las propiedades materiales de las personas. En efecto, la nueva figura jurídica delictiva, es en la actualidad una preocupación propia de la criminología moderna, por la dificultad para reprimir las conductas delictivas cometidas mediante Internet, dada la falta de uniformidad legislativa, y el obstáculo temporo-espacial que se presenta al momento procesal de analizar el hecho delictivo con la conducta ilícita tipificada[210].

[210] La regulación y gobierno de Internet, radica en varios entes gubernamentales: El principal ente normativo es el Grupo de Trabajo de Ingeniería de Internet (IETF). Compuesto por voluntarios de todo el mundo, el IETF desarrolla y adopta nuevas normas para las tecnologías de Internet, y coordina con otros entes normativos. El producto más conocido del IETF son sus peticiones de comentarios (RFC, por sus siglas en inglés). Estas describen abiertamente los nuevos protocolos de Internet, de modo que cualquiera pueda construir tecnologías compatibles. La Corporación para la asignación de nombres y números en Internet (ICANN) administra las direcciones IP y los nombres de dominios. ICANN es en sí una corporación privada sin fines de

En la medida en que los datos e información transmitidos a través de las redes informáticas poseen un valor económico o personal, se constituyen en un bien jurídico susceptible de ser protegido a través de la legislación; de esta manera, la información en forma de "bits", independientemente de la forma que adopte en un ordenador, ya sea texto, imagen o sonido; es incorporada al derecho como un bien al igual que la materia y la energía.

Frente al rápido e inminente avance de la criminalidad informática, no sólo es necesario criminalizar estas nuevas conductas sino también estudiarlas de manera detallada para buscar mecanismos de prevención. Es la misma Asociación Mundial de Derecho Penal la que reconoció en el XV Congreso Internacional de Derecho Penal realizado que: La comunidad académica y científica, conjuntamente con los gobiernos deben comprometerse a realizar más investigaciones sobre el delito de la tecnología informática (…) La teoría y política jurídica debe prestar especial atención al estudio y desarrollo de la ley informática, tomando en consideración las características específicas de la información, al compararla con los objetos tangibles, e investigar los probables cambios que afectan los principios generales y paradigmas. En un mundo globalizado, cada vez más dependiente de la tecnología informática y la Internet, son en su mayoría muchos los Estados que se encuentran

---

lucro registrada en Norteamérica. La Unión Internacional de Telecomunicaciones (ITU) establece normas para las comunicaciones telegráficas y telefónicas, así como para el espectro radiofónico. Las Normativas internacionales sobre telecomunicaciones (ITR) complementan la Convención Internacional sobre Telecomunicaciones, con miras a establecer principios generales que estén relacionados con el suministro y operación de distintos aspectos de las comunicaciones mundiales, incluyendo los flujos de tráfico y la calidad del servicio. Las ITR fueron redactadas antes del surgimiento de Internet como plataforma dominante de las comunicaciones internacional, y por lo tanto no hacen referencia específica a Internet en sí. ZIEWITZ, M / BROWN, I, 2013. A prehistory of Internet governance. En Brown, I.Research Handbook on Governance of the Internet, Cheltenham, Edward Elgar. Citados en UNODC (United Nations on Drugs and Crime), Estudio exhautivo sobre le delito cibernético Oficina De Las Naciones Unidas Contra La Droga y El Delito, Naciones Unidas, Nueva York, 2013, pág. 319.

en extrema vulnerabilidad a este tipo de ataques, los cuales pueden llegar a generar pérdidas económicas y lo más lamentable, pérdidas humanas a gran escala. Es así, que el desafío, para poder perseguir estos delitos, es por hoy de una magnitud de grandes proporciones tanto, a nivel empresarial, gubernamental y por supuesto a nivel particular, llevando a las distintas legislaciones mundiales, a tener que progresar de manera intensa e inmediata, para poder enfrentar esta nueva forma de delinquir, toda vez que los delitos que se cometen por medio de la red de redes, son de difícil punición, debido a distintos factores. De esta manera, se pueden apreciar a simple vista, distintas problemáticas principalmente porque su consumación es transfronteriza; una ausencia de tipificación del delito; la diversidad de calificación jurídica de una conducta de un país en relación a otro, o; la imposibilidad de mantener actualizadas la tipificación y sanción de la conductas que van surgiendo. Dicho lo anterior, he decidido analizar el delito cometido por Internet o por medio electrónico.

Uno de los mayores problemas jurídicos con la aparición de Internet y de los delitos informáticos, es el replanteamiento de la concepción del delito, si entendemos que un delito tiene lugar cuando concurren cuatro elementos: una ley, un infractor, un objetivo un lugar; ya que este tipo penal se comete en un espacio virtual; por lo que las hipótesis de lugar son variadas, dado el espacio físico de ocurrencia del delito; lo que también comporta una barrera en miras de la búsqueda de mecanismos para su prevención y lucha. Todos los ordenamientos, jurídicos se van construyendo a medida que la sociedad va evolucionando, cambiando, por lo mismo al nacer el cibercrimen, con su componente transfronterizo, debe la justicia y los operadores jurídicos dar una respuesta, tanto al ciudadano como a los países, de cómo poder atacar, prevenir y por último sancionar el delito informático.

Los distintos poderes judiciales y otros operadores del sistema de justicia de todos los países se están enfrentando cada día, a esta nueva delincuencia tanto

organizada, como realizada por individuos que operan de manera solitaria, y que intentan a través de la red de redes, defraudar para obtener ganancias ilícitas. Ello comporta el que se haga necesario establecer una sistematización, clarificación y solución de los intrincados problemas jurídico-penales que se plantean en la materia de Delito Informático, así como en sede de imputación objetiva de responsabilidad al ciberdelincuente, en, es decir será trabajado de acuerdo a la jurisdicción y la legislación aplicable al ciberdelito en Chile y su relación con la legislación internacional vigente que afecta al mismo.

Es necesario realizar un análisis completo de la conducta típica, teniendo siempre en consideración que la invención de nuevas tecnologías, hace que los medios de cometimiento, en este caso de los delitos informáticos avance junto con estas, es por eso que la legislación para lograr un grado de eficacia y efectividad requiere de tipificación plena de aquellos delitos, y que a la vez requieren de respuestas concretas y precisas, hasta el punto que puedan ser perseguidos desde cualquier parte de la orbe, para lo cual se requiere que los hechos estén efectivamente tipificados como delitos.

Merece especial atención la denominación de “delitos informáticos”, frente a la cual no existe uniformidad alguna, lo que hace más difícil una adecuada tipificación, ya que podemos encontrar delitos cometidos por medios informáticos, o bien, los ilícitos cometidos de manera directa en contra de lo que implica todo el mundo cibernético. Luego ante tal eventualidad, un delito cometido con un medio cibernético es un delito independiente o una atenuación del tipo penal, como quiera que el mismo se precisa de una actividad especializada cuya utilización es opcional por el delincuente como el delito de pornografía infantil, entre otros. Lo anterior comporta claramente la necesidad de un análisis jurídico-penal de manera actualizada de la materia debido a la magnitud de las consecuencias que tienen o pueden llegar tener las conductas delictivas a nivel mundial, razonando sobre la idea

de la rápida evolución de la misma y de la insuficiencia que tiene tanto la judicatura, como el operador jurídico de poder diferenciar la figura penal del Delito Informático de otras relacionadas con el mismo, comenzando por la acción hasta su punibilidad.

4.1. Monedas electrónicas[211] [212]

El Pilar fundamental, de toda la nueva sociedad de la información, es precisamente *Internet*, siendo éste es un espacio común al que todos pueden acceder y se lo denomina *ciberespacio*, sirviendo este espacio común, para poder realizar todo tipo de transacciones, comunicaciones en definitiva usarlo para fines lícitos o totalmente positivos que traigan un beneficio para la humanidad, pero en todo lo que crea el hombre las personas encuentran la forma de poder utilizarlo en beneficio propio y de una manera ilegítima. Vale recordar que en un comienzo internet tenía un fin militar, creado en Estados Unidos de Norteamérica, pensado y diseñado para la Guerra Fría, toda vez que se necesitaba mantener un enlace ante cualquier evento de gran magnitud de tipo nuclear, a pesar que fue creada por un civil.

[211] La nebulosa moneda digital que se negocia en el ciberespacio y es minada por ordenadores que descifran códigos, emergió este año como una mejor apuesta que las monedas, índices bursátiles y contratos de materias primas importantes. La moneda electrónica que se negocia y es regulada como el petróleo y el oro, se disparó 79% desde el inicio de 2016 a US$778, su más alto nivel desde comienzos de 2014, muestran datos compilados por Bloomberg. Eso es cuatro veces el avance registrado por el rublo de Rusia y el real de Brasil. Después de su creación en 2008, los entusiastas elogiaron al bitcoin como el nuevo grande en los mercados de divisas, una obvia evolución monetaria en un mundo crecientemente digital. Pero para 2014, su valor se había derrumbado 58% conforme los Gobiernos limitaban su uso y una bolsa importante perdió fondos de titulares de cuentas.

[212] SALLIS M, Exequiel, Cibercrimen, *Desafío de la investigación,* Área de cibercrimen, Policía Metropolitana, REMJA, Buenos Aires, Argentina, 2016. Material extraído, de la reunión de ministros de justicia u otros ministros, procuradores fiscales generales de la América. Grupo de trabajo en delito cibernético. Organización de los Estados Americanos.

El *Bitcoin*, esta criptomoneda fue creada y puesta a funcionar por Satoshi NAKAMOTO en el 3 de enero de 2009. Su arquitectura está basada en las redes P2P, por lo que funciona de manera totalmente descentralizada. Satoshi implemento los mecanismos de seguridad basándose en una plataforma criptografica de código abierto, que hace impracticable la posibilidad de reversar una transacción validada, brindado así protección contra el fraude. La plataforma se apoyó en 4 pilares importantes de la criptografía, a saber *confidencialidad;* Integridad*; No repudio; Autenticación.* En resumen, es una moneda digital que funciona de forma descentralizada, sin contratos, ni intermediarios.

El 22 de mayo de 2010 ocurrió la primera transacción de un ítem físico 10.000 Bitcoins por una pizza (25 USD). La generación de bitcoins es controlada, predecible y limitada (Máximo 21.000.000 de Bitcoins), y se calcula que esta cifra se alcanzara en el año 2033. Los bitcoins se generan libremente mediante hardware y software que realizan la actividad llamada *minería* y la minería requiere de una inversión, por lo que los mineros reciben un bono por bloque, que hoy es igual a 25 bitcoins distribuidos en toda la red. Cada 4 años el valor del bono decrece.

Los bitcoins se almacenan en una billetera digital, representada por una dirección compuestas por 34 caracteres, alfanuméricos. Los bitcoins se pueden adquirir de alguna de las siguientes tanto; por adquisición por medio de la minería; adquisición por intercambio de dinero en efectivo; Adquisición del mercado formal. De esta manera para los fines de que se concrete una transacción se requiere la dirección de la billetera digital origen, también la cantidad de bitcoins objeto de la transacción, la dirección de la billetera digital destino y las claves privadas.

Ahora bien, las direcciones origen y destino se generan de forma automática al momento de crear y configurar una billetera digital. Por cada billetera y dirección se genera una clave privada, la cual opera como firma digital respecto de la posesión

de un usuario sobre la criptomoneda, alanceándose, la clave privada se almacena en diferentes locaciones fijas dependiendo el tipo de billetera que el usuario tenga, de esta forma la información de las transacciones es totalmente transparente, publica y permite que cualquier persona pueda visualizar el camino de las mismas, manteniendo como beneficio un cierto anonimato que resguarda al usuario. La historia completa de las transacciones se almacena en lo que se conoce como *Blockchain* o cadena de bloques, esta información es de acceso público y se replica en cada nodo de la red P2P.

El bitcoin tiene razones para ser atractiva, a saber; *Controles de capital*, es decir las restricciones globales a las monedas soberanas juegan un importante papel en la mayor demanda de bitcoins; *La perspectiva de una reducción de las remesas*, puesto que las políticas aislacionistas de algunos gobiernos, destinadas a restringir las remesas, también empujan a la gente a recurrir a bitcoins; *La desaceleración de la oferta*, toda vez que la explosión de la oferta de bitcoins está cediendo porque los llamados mineros obtienen menos monedas electrónicas a cambio de permitir que la red use su poder informático; *Mayor aceptación*, cada vez más consumidores están usando bitcoins y más compañías los aceptan como medio de pago; *Medidas más estrictas contra la corrupción y el terrorismo,* ya que algunos países han prohibido sus billetes de más alta denominación para que resultara más difícil pagar sobornos y comprar contrabando con efectivo. Eso aumentó la demanda de las personas que quieren recibir y enviar efectivo sin toda esa supervisión.

4.2. Deep web o internet profundo

En la historia de la humanidad, siempre han existido fenómenos, que están rodeados de misterio y ocultismo, hoy en día es con el desarrollo de la informática, existe un fenómeno relacionado con Internet, el cual se tiene poco conocimiento, una cara poco visible de la red de redes[213].

a) Naturaleza y origen

En principio podemos decir que todo el contenido dentro de internet que no forma parte los sitios web que pueden referenciar o encontrar diferentes buscadores, aquello que se encuentra oculto más allá de la zona habitual y pública de navegación conocidas de Internet superficial o Surface web. En este Internet invisible, se pueden encontrar todos los sitios descartados por los propios buscadores, o páginas webs sobre las cuales los dueños no permiten la indexación o referencia, para los motores de búsqueda.

Internet profunda, está compuesta por todos los datos del banco, el código administrativo de gobierno, empresas y universidades, podemos decir entonces que sería como mirar debajo del capó de internet, el usuario común y corriente sólo de la punta del iceberg. Al comenzar a ser conocido esta parte invisible Internet los usuarios comenzaron a visitarlo puesto que querían privacidad. Para poder acceder a esta zona en necesario contar con un software llamado TOR, el cual fue desarrollado

[213] *Ya no es la era industrial, vivimos en una era fundamentalmente tecnológica, los fascistas tienen los recursos, pero nosotros tenemos imaginación, estamos fabricando las herramientas para recuperar nuestras soberanía respecto al sistema, rompemos el dominio de las herramientas de poder que se usan contra nosotros. Venimos aquí y quitamos la oscuridad con blancura pura. Es un falso relato, porque hay corrupción en esos castillos. La verdadera base de poder está con nosotros. Somos la oscuridad.* Referencia, indicada por un experto informático, un hacker de sombrero oscuro, perteneciente a la agrupación anónimos.

por las Fuerzas Armadas de Estados Unidos de Norteamérica, el cual hoy en día se encuentra financiado públicamente y este código público o abierto, dicho programa se usa alrededor del mundo, tanto por los gobiernos como por todas las agencias relacionadas información como por ejemplo periodistas.

b) Funcionamiento

Se trata de un servicio online que funciona con un software específico, con el cual se puede conectar a una red de comunicaciones de baja latencia que brinda anonimato a los usuarios, surgiendo en el año 2003, el cual se basaba en el proyecto OR, del laboratorio de investigación naval de los Estados Unidos, sin embargo ello en el año 2004, se traspasó a manos de la EFF, (en la fundación frontera electrónica, en inglés Electronic Frontier Foundation, EFF), y hoy en día dicho proyecto está en manos de una entidad sin fines de lucro dedicada a la investigación, denominada *TOR Project*. Este código abierto, que permanece en constante evolución es utilizado diariamente por ciento de miles de usuarios alrededor del mundo, y se dice que se asemeja a una cebolla, por su similitud con las capas de la misma.

Al tratarse de un medio o espacio que se encuentra separado del resto de internet y debidamente encriptado y oculto, supone la vía perfecta para realizar cualquier tipo de actividad ilícita o prohibida sin que pueda ser monitorizada o rastreada de una manera fiable, ni la propia actividad ni tampoco la posible transacción al utilizarse como método de pago con la moneda virtual. En dicho espacio se realizan todo tipo de actuaciones ilícitas, a saber, ciber-espionaje, piratería informática o revelación de secretos o tráfico de drogas, compra-venta de armas, pornografía infantil, tanto la creación, intercambio, distribución, y venta.

CAPÍTULO III

Fraudes, a través de sistemas informáticos: planteamiento del problema

I. Planteamientos

Los avances tecnológicos y la utilización de estos han puesto a disposición de la sociedad mundial una gran cantidad de información, en las distintas áreas del conocimiento, permitiendo hoy en día procesar gran cantidad de información que llega a todos gobiernos, instituciones y a las personas en general. Como se ha venido señalando el empleo de estos medios tecnológicos han facilitado de alguna u otra manera que los sujetos dedicados a cometer ilícitos en contra el patrimonio puedan acceder a distintas formas de vulneración de información, como son la clonación de tarjetas bancarias, vulneración de alteración de los sistemas de cómputos así como la forma de transferencias electrónicas, mediante la manipulación de los programas pertinentes, por lo mismo en todo el mundo se ha tenido que replantear la forma en que se persiguen y se juzgan este tipo de delitos, debiendo la legislaciones adecuarse a los avances tecnológicos informáticos.

Se suma ello, con la trascendencia de las TICs, puesto que se ha pasado de la economía análoga a otra digital en cuanto a la macroeconomía se refiere, ya su vez también en la microeconomía, con todos los cambios que en día han surgido en la manera de cómo comercializar todo tipo de productos naciendo multiplicidad de sitios que ofertan al usuario, con la posibilidad de obtener cualquier bien o servicio a través de la red con pago inmediato sin utilizar dinero en efectivo, recibiendo el bien

o servicio directamente en su hogar, de esta manera tenemos por ejemplo *e-Bay*[214], o los sistemas de pago, como son transferencia bancaria, o el mismo *PayPal*[215]. En todo el mundo, se trata de reemplazar la moneda metálica, por las transacciones en línea llegando incluso a lugares que nos acepta el dinero en efectivo, sólo pago virtual o a través de tarjetas, siendo reemplazado por este nuevo dinero virtual[216].

La estafa es uno de los delitos más clásicos cometidos contra el patrimonio, cuyo principal componente corresponde a un elemento intencional, ánimo de lucro de una conducta que se basa en tres elementos básicos, engaño, error y disposición patrimonial. De acuerdo ello se sanciona a la persona que provoca de alguna manera una disposición patrimonial ajena por medio de un engaño, el cual tiene que ser

[214] E-Bay es el mayor centro de compra y venta en internet, lugar en el que se reúnen compradores y vendedores para intercambiar prácticamente de todo. Funciona en el entendido que un vendedor pone un artículo a la venta, casi de cualquier tipo, (antigüedades, coches, libros). El vendedor opta por aceptar sólo un anuncio de subasta u ofrecer la opción de precio fijo. La empresa pone a disposición de las partes la plataforma en la que se celebrarán las diferentes subastas o compras y dicha empresa como prestador de servicios de la sociedad de la información, debe cumplir los deberes que le impone la LSSICE, puesto que la empresa cobra por los anuncios en su sitio web, por su situación de mero punto de encuentro entre comprador y vendedor y cobra un porcentaje por producto vendido. SÁNCHEZ CALERO, F, *Instituciones de Derecho mercantil*, Vol. II, 23ª Edición, Madrid, 2000. Pág. 181, citado por PANIZA FULLANA, Antonia, *E-Consumidores, Aspectos Problemáticos en la normativa española*, En revista Chilena de derecho informático, 8/-2006. pág. 22.

[215] PayPal, empresa del sector del comercio electrónico, cuyo sistema permite a sus usuarios realizar pagos y transferencias, a través de internet sin compartir la información financiera con el destinatario, con el único requerimiento de que estos dispongan de correo electrónico. Es un sistema rápido y seguro para enviar y recibir dinero. Paypal procesa transacciones para particulares, compradores y vendedores online, sitios de subastas y otros usos comerciales. La mayor parte de su clientela proviene del sitio indicado en la nota al pie anterior, eBay, compañía que compró PayPal en 2002.

[216] El año 2012, en Italia el Consejo de ministros votó afirmativamente en el sentido de limitar el uso dinero efectivo en transacciones de mate €1000, posteriormente limitó los pagos en metálico a €50. Del mismo modo en España a finales del año 2016 se propuso reducir de 2500 a €1000 la cantidad máxima que se puede abonar en efectivo. Ambos países lo han hecho con el fin de acabar o por lo menos limitar de manera sensible el fraude en el pago de impuesto sobre el valor añadido.

suficiente y tener la aptitud para generar el error, que lleva al acto disposición patrimonial. Como se ha venido tratando, en la sociedad de la información el cibercrimen, se expresa en múltiples formas con distintas y nuevas modalidades de comisión de los tradicionales delitos, tornando hoy en día mucho más compleja la persecución quedando en impunidad, puesto que la legislaciones muchas veces no tienen las herramientas necesarias para hacer frente a estas formas actuales de llevar a cabo estos delitos a través de los sistemas o redes informáticas de transmisión de intercambio de datos por internet.

La legislaciones muchas veces, se muestran lentas ante los cambios, que van sucediendo en esta nueva era informática, se suma ello que los delitos trasciende las fronteras con todo el problema que ello trae, puesto que muchas personas, también discuten acerca de la libertad que se debe tener para navegar por Internet, discusión que va en directa relación con la expansión del Derecho Penal[217]. Ahora bien, el fraude informático o estafa por medios informáticos es una de las tipologías del cibercrimen, en el que se da la defraudación por medios informáticos, es decir la utilización del sistema informático, como medio para transferir patrimonio Fausto a favor del sujeto activo, denominándolo de distintas formas, como son estafa telemática, estafa por computación, fraude informático, estafa informática. Hoy en día las legislaciones se han visto la necesidad, de tener que crear o adecuar sus sistemas a la realidad mundial. Ahora bien el derecho penal, este sistema normativo que también es un sistema de control de la sociedad que tiene por objeto mantener la convivencia social debe, por lo mismo ir adecuándose a los tiempos. "Inevitablemente este instrumento de control social no podía permanecer ajeno a los problemas de convivencia e interacción que se venía sujetando como consecuencia

[217] ÁLVAREZ VIZCAYA, Maite, *Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red, en Internet y Derecho penal*, Cuadernos de Derecho Judicial, (2001), 260 y 261.

de la creciente masiva utilización de los modernos sistemas informáticos en ámbitos sociales que tradicionalmente habían gozado de su tutela; siendo la creación del delito de estafa informática, precisamente, una muestra evidente de la preocupación del legislador penal por el mantenimiento de las normas básicas de convivencia en este nuevo campo de interacción social"[218]. En sentido se entiende que el delito de estafa informática tiene como fin una norma de control social tendiente a establecer y garantizar reglas básicas de convivencia, en el campo de las relaciones sociales patrimoniales que se desarrolla mediante la utilización de sistemas informáticos[219]. Así las cosas, la prevención general positiva se instituía en el fundamento básico no sólo de la pena como sanción característica de este instrumento jurídico, sino del conjunto del sistema penal como tal[220].

Toda la informatización que se realiza a través de internet y a su vez las transacciones financieras, como todo tipo de pagos relacionado con bancos, instituciones financieras u otros, han dado paso a la creación de nuevos tipos delictivos que tienen directa relación con delitos de carácter económico. A su vez la rápida trasmisión de datos, facilita la realización y comisión de estos delitos, bastando para ellos una terminal, conocimientos básicos, y un instrumento para transferencias adecuado, al tipo de delito que se trata de realizar.

---

[218] GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos, análisis del artículo 248.2 del Código Penal Español,* Editorial Iirant lo Blanch, Valencia, 2005, pág. 183.

[219] Sobre esto, nos dice, GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos, análisis del artículo 248.2 del Código Penal Español*, Editorial Tirant lo Blanch, Valencia, 2005, pág. 183. La visión del derecho penal, que podríamos denominar funcionalista, entiende que las normas penales serían meros instrumentos destinados establecer los parámetros por lo que debe discurrir la vida social, creyendo sus penas, por principal función la de restablecer su propia vigencia como normas sociales, cuando esta se hubiese visto de esa autorizada por las conductas efectuadas por alguno de sus destinatarios.

[220] JAKOBS, Günther, *Derecho penal parte general, fundamentos y teoría de la imputación*, 2ª edición corregida, Editorial Marcial Pons, Madrid, 1997. pág. 14.

De esta manera, las normas penales actuales han incluido nuevos tipos de *fraudes o estafas informáticas,* toda vez que se han puesto en el caso, que estos fraudes o estafas se realicen, tanto con la fabricación de programas que tiene por fin medios delictivos o con la manipulación informática de ciertos datos para cometer los delitos.

El *phishing* o también la estafa mediante la manipulación informática se regula el Código Penal Español en su artículo 248.2 letra a), el cual señala como reos de estafa a quienes "con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante, consigan la trasferencia no consentida de cualquier activo patrimonial en perjuicio de terceros".

Este tipo de estafa nace a la vida delictiva mediante la *manipulación informática,* estando en ese escenario cuando la introducción, alteración, borrado o supresión indebida de datos informáticos, como serian por ejemplo, todos los datos de identidad de una persona, la interferencia al margen de la ley para que un programa informático funcione correctamente, produciendo por ende, un resultado dañino, el cual se traduce en que el delincuente informático, transfiere de una manera efectiva y real, y en perjuicio de tercero patrimonio, el cual puede ser evaluable económicamente, es decir un activo del sujeto pasivo. Todo esto se produce cuando se alteran los programas, utilizando como son *bombas lógicas*, *caballos de troya* u otras técnicas que provocan la realización de transferencias involuntarias para el sujeto pasivo, pero que muchas veces son automáticas.

Por otro lado existe el apartado b) del artículo 248.2 donde se sanciona la elaboración, difusión e incluso la mera tenencia de estas aplicaciones, o programas que permiten la realización de estafas, aun cuando se tenga y no se utilices, solamente se requieren que sean para dicho fin, en este caso el legislador pretende sancionarlos como *actos preparatorio,* puesto que sirven para cometer un delito,

propiamente tales, no son estafas. Éstas manifestaciones lesivas, que son por lejos las que se realizan, frecuencia en la red tienen directa relación con la producción de alguna manera fraudulenta de perjuicios patrimoniales a terceros, toda vez que el gran potencial que tiene internet, como elemento o con un instrumento para el intercambio con el comercial ha llevado, ciertamente, e inevitablemente aquí también en este mismo canal que pueden realizarse distintas transacciones de orden comercial, que tienen fines lícitos y que ayudan al comercio nacional como internacional o mundial también pueden colmarse, de sujetos que pretenden tener algún lucro ilícito, por esta razón la estafa con el componente informático, tiene múltiples manifestaciones, que no tienen límite en cuanto a la forma de realización puesto que día a día se van creando nuevas e ingeniosas formas o maneras de llegar o hacer estas estafas que tienen fines ilícitos. De manera tal, que alguna de estas manifestaciones de tipo fraudulento o defraudaciones patrimoniales, se condicen con la estafa básica o el modelo tradicional, y que ha tenido también de alguna forma un incentivo al mayor desarrollo, puesto que las legislaciones de alguna u otra forma no han querido o no han podido adaptarse a los constantes cambios, sumando ello la percepción errónea de los usuarios de Internet, que no tienen una visión suficientemente desarrollada respecto del riesgo, circunstancia que hace, que la persona que desarrolla este tipo de actos ilícitos en la red sea un incentivo para seguir defraudando.

Todo esto gira en torno a relaciones patrimoniales, que van en directa relación con las finanzas, tomando siempre como base o supuesto, relaciones interpersonales, puesto que sólo ellas pueden generar el engaño y el error, toda vez que estos dos conceptos son manifestaciones de la voluntad y se perciben a través de los sentidos, del intelecto. Tradicionalmente la estafa mirada de un punto de vista intelectual, impedía que las disposiciones fraudulentas de algún tipo de patrimonio fueran observadas como estafa, puesto que al ser consideradas y proyectadas en el

error sobre un ordenador o en el engaño de un sistema informático, nos impedía reconocerla como este tipo de delito.

Haciendo hincapié en que las conductas más frecuentes en la red se manifiesta con la realización fraudulenta de perjuicios patrimoniales a terceros lo que comúnmente llamamos estafa, se ha incrementado con el gran potencial de internet para poder obtener un lucro con fines ilícitos, como se indicó, dando paso a que el fraude tradicionalmente conocido como estafa, se haya multiplicado exponencialmente con muchas formas de cometerlo, por lo mismo algunas pueden o no coincidir con el concepto jurídico de estafa antiguamente conocido, y otras que escapan a las denominaciones tradicionales.

La delincuencia en términos generales, y la delincuencia económica en particular, que no se encuentran sometidas a parámetros procesales ni a dictados dogmáticos, supone para el legislador un esfuerzo de revisión y, en su caso, actualización de los tipos penales tradicionales o clásicos. Ello para intentar impedir que determinadas conductas criminales, ágiles, cambiantes y más próximas al fenómeno de las nuevas tecnologías, queden fuera de cualquier marco legal y que, por ende, faltas de previsión típica, puedan resultar impunes.

Bajo esta premisa, se pretende abordar la evolución y materialización que el fenómeno de los medios informáticos ha comportado sobre el tipo penal de estafa, dando lugar a la denominada *estafa informática* y en concreto, abordar la problemática referida al *phishing y otras modalidades*. Lo anterior, debe consecuentemente conectarse con la problemática que en su momento, legislador supranacional previo, las conductas criminales que resultaban atípicas por la celeridad y cambio de las nuevas tecnologías especialmente las transacciones de tipo comercial dando pie para abordar el tema. De esta manera el Consejo de Europa, a

través de la decisión marco[221], se dirige a los estados miembros estableciendo directrices para incrementar cautelas e implementar los ordenamientos para la previsión de este tipo de conductas[222]. Por otro lado, el Consejo de Europa, de noviembre de 2001, en su artículo octavo prevé el concepto de *estafa informática*.

Estos dos instrumentos jurídicos internacionales, generó que los autores entrecrucen sus opiniones, haciendo que la brecha respecto de las conductas criminales se torne más amplia, puesto que por un lado se tomaba como base los tipos penales clásicos, y por otro se trataba como otro el tipo penal de estafa ya existente en el ordenamiento jurídico español.

El legislador español tomó una postura modificatoria del Código Penal Español, tanto los años 2000 y 2010, entregando autonomía como tipo sustantivo en el artículo 248 número dos actual[223]. De esta manera, como primera aproximación se vislumbra una diferencia con el delito de estafa tradicional, puesto que la primera disposición patrimonial propia del delito lo realiza el propio sujeto activo y no la víctima, y ello porque la propia forma comisiva de los delitos incorporados por el citado artículo 248.2, del Código Penal Español trabaja sobre la idea o supuesto que no puede estarse a los mismos elementos exigidos por el engaño y error propios de

[221] Actos adoptados en aplicación del título VI del Tratado de la Unión Europea, Decisión Marco del Consejo de 28 de mayo de 2001, Sobre La Lucha Contra El Fraude y La Falsificación de Medios de Pago Distintos del Efectivo. (2001/413/JAI).

[222] Por ejemplo: la realización o provocación de transferencias o valores monetarios sin consentimiento, la introducción, supresión, alteración o borrado de datos informáticos, entre otros.

[223] CPE, artículo 248, El precepto reza como sigue: 2. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

la modalidad de estafa básica, esto por la relación interpersonal; Así la conducta se lleva a cabo por el empleo de manipulación informática o artificio semejante, perpetrando de esta manera la disposición patrimonial del sujeto activo, el cual obtiene una transferencia no consentida por la víctima. Para poder ingresar de alguna manera al tema de esta estafa especial, debemos saber algo, acerca de la evolución y orígenes del delito en comento, tal cual se hará el epígrafe siguiente.

II. Comentarios acerca de la voz fraude informático y estafa informática

Al comenzar a tratarse el fenómeno de la delincuencia informática la doctrina comenzó a hacerse cargo de los delitos que afectaban el patrimonio mediante la informática, de esta manera la doctrina fue denominándolas de distintas formas de acuerdo al delito que se tratare y la forma como se entendían los conceptos técnicos referentes a la materia, así las cosas algunos de ellos se han referido a la estafa mediante manipulación informática; estafa informática, estafas mediante manipulaciones informáticas; estafa por medio informáticos; estafa por computación; defraudación por computación; o manipulaciones informáticas defraudatorias patrimoniales.[224].

[224] Distintos autores, han analizado el tema desde sus ópticas, con el denominador de común que todo el delito que se comete es, a través de internet, de esta manera, se refiere a la estafa: estafa mediante manipulación informática (VALLE MUÑIZ); estafa informática (GUTIÉRREZ FRANCÉS); estafas mediante manipulaciones informáticas (SERRANO GÓMEZ); estafa por medio informáticos (VIVES ANTÓN-GONZÁLEZ CUSSAC); estafa por computación (CHOCLÁN MONTALVO); defraudación por computación (MATA Y MARTÍN) o manipulaciones informáticas defraudatorias patrimoniales (ROVIRA DEL CANTO).

Cuando hablamos de engaño con fines lucrativos, nos referimos al fraude. Ya en el código de *Hammurabí*[225] [226], se contemplaba varias formas de fraude, como son la entrega en préstamo de granos y plata en distinta medida de lo que se había acordado, siendo castigado con la pérdida total de lo que se había prestado, y la apropiación de granos o forrajes cedidos a la siembra cría, se castigaba con la pérdida de la mano, asimismo cuando se alteraban las marcas o la disposición del ganado cedido para pastar, se castigaba con multa de 10 veces el valor de lo prestado[227]. En el derecho romano, la acción originalmente concedida para perseguir los fraudes era de naturaleza privada y auxiliar procedimiento civil, aunque mediante la práctica de los tribunales se extendió como auxiliar procedimiento acusatorio, revistiendo entonces carácter penal.

El *stellionatus,* nombre genérico para estafa, fue precedido la criminalización por la ulceración testamentos y de monedas, y por la corrupción de funcionarios y, aún antes, desde la ley de las XII tablas, por el falso testimonio, el cohecho de

[225] LARA PEINADO, Federico, *Código de Hammurabí, estudio preliminar, traducción y comentarios,* 2ª Edición, Editorial Tecnos, Madrid, 1986.

[226] MARCHILI, Luis Alberto, *Como legislar con sabiduría y elocuencia, el arte de legislar reconstruido a partir de la tradición retórica,* Editorial Dunken, Buenos Aires, Argentina, 2009.

[227] El código de leyes, (1750 a.c.), unifica los diferentes códigos existentes en las ciudades del imperio babilónico. Pretende establecer leyes aplicables en todos los casos, e impedir así que cada uno *tomara la justicia por su mano*, pues sin ley escrita que los jueces hubieran de aplicar obligatoriamente, era fácil que cada uno actuase como más le conviniera. De esta manera rezaban las hipótesis referidas: artículo 194 Si el prestamista ha prestado con interés trigo o plata, y si cuando ha prestado a interés, ha entregado plata en una cantidad menor o el trigo con una medida inferior, o si cuando ha percibido (lo que le era debido), ha percibido el dinero (en cantidad superior), el trigo (con una medida superior) este prestamista perderá todo lo que ha prestado; artículo 253, Caso que un hombre haya contratado a otro hombre para que guarde un campo, y le confía cereal, le encarga el cuidado de las reses y el deber de cultivar el terreno, si ese hombre sustrae simiente o forraje y lo hallan en su poder, que le corten la mano; artículo 265, si un pastor, a quien le fueron confiadas reses u ovejas para que las apacentara, comete fraude y cambia las marcas del ganado y lo vende, y se lo prueban, lo que hubiese robado, reses u ovejas, lo restituirá 10 veces a su dueño. Pontificia Universidad Católica de Valparaíso. [Disponible en], < wwwhttp://educarchile.cl>, [en línea], <www.feebooks.com>.

jurados y la compra de votos. Todos estos delitos implican alguna forma de engaño mediante inducción error, si bien el interés tutelado no constituye, salvo los casos fraude, el patrimonio individual[228].

Las estafas hoy en día, se conciben como conductas fraudulentas en las cuales se induce al error para obtener un provecho causan un perjuicio a un tercero puesto que suponen una apropiación indebida de algún bien o de algún derecho patrimonial, a raíz de una representación falsa de la realidad, que generada por el delincuente. Siempre se ha hablado en los conceptos de fraude que existe una apropiación o una ganancia indebida que tiene como consecuencia que ignora un derecho socialmente reconocido. Ahora bien, teniendo en cuenta estas referencias al fraude, es dable señalar que en cuanto al fraude informático, se puede sostener que tiene aspectos distintos y nuevos a los conceptos señalados.

El desarrollo de la tecnología de la información ha traído una forma distinta de cometer fraude, añadiéndose formas nuevas para la comisión del delito, siendo este aspecto el *medio de comisión,* la característica relevante que le diferencia de los otros. Por lo mismo esto fraude se desarrollan tanto por particulares puesto que las redes y en día está institucionalizada la forma de hacer un pago, o cómo se desarrolla el sistema bancario total puesto que hoy todo se desarrolla en forma instantánea y a través de la red. Podemos decir entonces, el fraude electrónico o a través de medios informáticos, es toda conducta dirigida a la obtención de un provecho económico indebido, mediante la apropiación, la falsificación, la interferencia y la reproducción de códigos, instrucciones o programas, tanto sobre instrumento portables como sobre programas incorporados a sistemas de procesamiento de datos, que permiten el acceso a dinero en efectivo o a bienes y

[228] GABALDÓN GERARDO, Luis, *Fraude electrónico y cultura corporativa,* Editorial Universidad Federal de Bahía, pág. 195, Caderno CRH [en linea] 2006, (Mayo-Agosto)] Disponible en:<http://www.redalyc.org/articulo.oa>.

servicios con cargo diferido a cuentas bancarias[229]. Cuando hablamos de fraude, hablamos en forma genérica de la apropiación o búsqueda de un interés propio, aprovechándose el patrimonio de otro, sin embargo en otras legislaciones como la alemana se habla de estafa informática, basándose en el tipo básico de estafa, puesto que se agrega el componente informático, y que a través de se realiza la defraudación, requiriendo para que el delito se encuentre consumado la producción del daño patrimonial.

Entonces, el fraude informático o estafa por medios informáticos es una de las formas que adopta el cibercrimen, toda vez que existe una defraudación por medios informáticos, usando los sistemas en este caso de trasferencia de datos, como medio para trasladar o enviar los activos patrimoniales a un tercero a favor del sujeto activo existiendo un desplazamiento de manera virtual, que no se puede apreciar, haciendo que se vaya modificando la manera de operar, la forma de los diferentes delitos tal cual indica la autora ÁLVAREZ VIZCAYA[230].

Por su parte CORCOY Y JOSHI, señalas que las estafas por computador son las manipulaciones del proceso de elaboración electrónica de cualquier clase, y en cualquier momento de este, con la intención de obtener un beneficio económico, causando un tercero un perjuicio patrimonial[231]. A su vez para Casanova, el fraude informático es la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen, o ya

[229] Concepto del autor y complementado con la definición entregada por GABALDÓN GERARDO, Luis, *Fraude*…op. cit. pág., 196.

[230] ÁLVAREZ VIZCAYA, Maite, *Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red, en Internet y en derecho penal,* Cuadernos de Derecho Judicial, 2001.

[231] CORCOY BIDASOLO, Mirentxu / JOSHI JUBERT, Ujala, *Delitos contra el patrimonio cometidos por medios informáticos*, Revista jurídica Catalunya, vol. 87 N° 3, 1988, pág. 687.

contenidos en el computador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y perjuicio de un tercero[232].

Con frecuencia, se utiliza la palabra *fraude*[233] [234], así como también fraudulento, defraudar o defraudaciones, para referirse a una situación donde existe un engaño, siendo entonces engaño, sinónimo de fraude[235], sin embargo es forma general se puede adelantar que, se percibe que fraude no es cualquier engaño, el mismo tiene que revertir ciertas características, distintivas como son que el mismo se realiza, con la intención de cometer algún mal dirigido con el fin de provocar un perjuicio, de esta manera no se estaría cometiendo fraude cuando, por ejemplo, un padre asegura que su hijo ha terminado los estudios de la escuela judicial, siendo que la verdad, ha postulado en reiteradas ocasiones y no es aceptado. Pero cuando en el currículum, se agrega que se poseen certificado de egreso de la escuela judicial, para obtener un cargo dentro de la judicatura, estaríamos en presencia de un fraude[236].

---

[232] Citado, en el informe de Delitos Informáticos, Chile y legislación extranjera, biblioteca del Congreso Nacional de Chile, el cual, hace referencia a la cita de MAGLIONA MARCOVICTH, Claudio / LÓPEZ MEDEL, Macarena, *Delincuencia y Fraude Informático*, Editorial Jurídica, 1999, pág. 184.

[233] BULLEMMORE, GALLARDO, Vivían, *Curso Derecho Penal, parte especial, Tomo IV*, 2 edición, Editorial LexisNexis, Santiago, 2007, pág. 71. Nos indica, "el medio o modo de obrar engañoso o abusivo de confianza de que se vale una persona por obtener un resultado típico".

[234] ETCHEBERRY ORTHUSTEGUY, Alfredo, *Derecho Penal Parte Especial. Tercera Edición. Editorial Jurídica de Chile*, 1999, pág. 377. "En términos generales, puede caracterizarse el fraude como causar perjuicio en el patrimonio ajeno mediante engaño o incumplimiento voluntario de obligaciones jurídicas.

[235]QUINTANA RIPOLLÉS, A, *Tratando de la parte especial del derecho penal*, Tomo II, Revista de Derecho Privado, Madrid, 1977, pág 556.

[236] En Chile cuando estamos frente al fraude en general, y dentro de la clasificación de los delitos en relación al bien jurídico principal protegido, se encuentran los delitos contra la propiedad, siendo un concepto de propiedad distinto al utilizado por el derecho civil el cual se refiere propiamente el artículo 582 del código civil, señalando que el dominio, que se llama también

Vale indicar que el tema de la estafa informática va necesariamente unido al tema de la manipulación, cuando es indebida de datos buscándose una alteración de los datos contenidos en algún sistema, independientemente de las fases de tratamiento, con o sin ánimo de lucro. Tomando en cuenta esto, la mayoría de la doctrina al tratar de manipulación y fraude informático lo estudian como sinónimos, al referirse a la manipulación con carácter ilícito para obtener un beneficio patrimonial, tomando en consideración que los índices de delincuencia informática, son en el caso de las manipulaciones al ordenador los más altos, observando que los delitos informáticos en general protegen bienes jurídicos de una naturaleza múltiple. A mayor abundamiento, casi todos los delitos informáticos se realizan a través de alguna manipulación, salvo el espionaje que por su naturaleza, se capta a distancia. Señala GUTIÉRREZ FRANCÉS, que la voz fraude, con frecuencia en el lenguaje común suele identificarse como sinónimo de un engaño, aunque fraude no es cualquier engaño, por ello cuando se habla de fraude se está aludiendo a una forma de actuar,

---

propiedad, es el derecho real en una cosa corporal, para gozar y disponer de ella arbitrariamente; no siendo contra la ley o contra derecho ajeno. La propiedad separada del goce de la cosa se llama mera o nuda la propiedad. Por otro lado en el Derecho penal el concepto de propiedad cambia extendiéndose a otros puntos, de esta manera el autor Alfredo ETCHEVERRY, plantea "se extiende igualmente a la propiedad, entendida como el vínculo que une al sujeto con todos los derechos de que es titular y que sean económicamente apreciables, esto es, tanto a los derechos reales como no son el dominio, como el usufructo, como los derechos personales o créditos. De esta manera los delitos contra la propiedad se clasifican en delitos de destrucción y de apropiación siendo los primeros en los cuales implica la lesión incluso la desaparición de cosas sobre las cuales se posea propiedad, como son los de daños incendio. Por su parte los delitos de apropiación, que son aquellos en los que existe un desplazamiento patrimonial, determinados bienes saliendo de un patrimonio determinado para ingresar a otro. De esta manera en esta última clasificación existe otra que nace de los mismos, es decir delitos que para perpetrar dicha apropiación se valen de medios materiales como son el hurto y robo, y aquellos que se valen de medios inmateriales, obteniendo el desplazamiento del patrimonio mediante un elemento de carácter intelectual, orientado a engañar a la víctima, radicando la acción en la mente y no en la materialidad de una acción corporal, siendo *el fraude*, el principal delito dentro de ésta sub-clasificación.

que caracteriza un determinado comportamiento, que implica la presencia de un montaje o artimaña que desencadena determinada modalidad acción[237].

Por lo tanto, cuando hablamos de fraude nos encontraríamos que el engaño sería su faceta más importante, pero el mismo engaño no termina con el fraude, puesto que este último solamente supone medios para su comisión, el engaño o el abuso de confianza, sino que también supone el uso de otro artificio con el fin de crear ciertas confabulaciones, con el fin de perjudicar el patrimonio de la víctima. En definitiva, el carácter informático del fraude, puede radicar en el aprovechamiento, utilización o abuso de las que las características funcionales los sistemas informáticos como incremento para realizar una conducta engañosa, tomando en consideración que dicho carácter funcional de la informática que tiene directa relación con los instrumentos mediante los cuales se apoyan para realizar la defraudación[238].

Los autores estiman que se puede hablar tanto de *fraude* como de *defraudaciones,* puesto que ambas figuras conllevan una conducta o una forma de operar, que implica una artimaña o puesta en escena, visto de un punto de vista objetivo. Desde un punto de vista subjetivo, existe un ánimo de perjuicio hacia la víctima con un beneficio para el criminal cibernético.

La forma de trabajo que conlleva la naturaleza de este tipo de delito, que se realiza o se comete por medio de sistemas informáticos, viene en beneficiar a este

[237] GUTIÉRREZ FRANCÉS, María luz, *Fraude informático y estafa*, 1ª Edición, Editorial Ministerio de Justicia, Madrid, 1991, pág. 97 y sigs.

[238] La propia manipulación informática, ayuda distinguir el fraude informático de los otros hecho delictivo, que no obstante ser realizado por medios informáticos, no constituyen defraudaciones, como serían los atentados contra la intimidad cometidos por medio de manipulación informática. La finalidad perseguida por el sujeto activo, en la que condiciona el tipo de delito que se produce. MAGLIONA MARKCOVICH, Claudio / LÓPEZ MENDEL, Macarena, *Delincuencia y Fraude Informático*, Editorial Jurídica de Chile, 1999, pág. 188 y sigs.

tipo de delincuencia, puesto que al hablar de *fraude informático,* estamos hablando de una categoría criminológica, que tiene una multiplicidad de comportamientos con intereses económicos que no son muy claros, más bien difusos.

Es dable hacer presente, que cuando hablamos de *estafa informática*, al suponemos siempre que se alude exclusivamente a defraudaciones de carácter patrimonial realizada por medios informáticos, siendo al parecer un concepto más restringido que el de *fraude informático*[239]. Mayoritariamente se sostiene que el patrimonio comprendido dentro de la misma, cuando estamos en presencia del delito de estafa tradicional es el mismo bien jurídico penal protegido de la estafa informática[240].

De esta manera el delito de *fraude informático* tiene una relación de *género a especie,* con la *estafa informática*, puesto que conlleva múltiples conductas lesivas a múltiples intereses económicos que van más allá, de un patrimonio individual, teniendo en consideración, que la estafa no se está, protegiendo el bien jurídico que tiene relación con la información contenida en dichos sistemas, puesto que en el derecho europeo continental en general se concibe, que la estafa informática debe estudiarse vinculada al delito de estafa tradicional[241]. Tomando en consideración, que el termino defraudación se tiene como causa de un perjuicio económico causado, a través de engaños se puede indicar que la voz fraude informático, sería igual a defraudaciones y en cuanto a la estafa informática serian realizadas mediante computador y no sólo las defraudaciones patrimoniales por medios informáticos, sino todo tipo de defraudación llevada a efecto por medios similares contra intereses

[239] Así indica BALMACEDA HOYOS, Gustavo, *El delito de estafa informática*, Editorial Jurídicas de Santiago, 2009, pág 114 y 115.

[240] Cfr. BALMACEDA HOYOS, Gustavo, *El delito*.....Op. cit. pág. 115 y sigs., 129 y sigs.

[241] Cfr. BALMACEDA HOYOS, Gustavo, *El delito*...Op. cit. pág. 115 y sigs.

económicos. Podemos decir entonces que, el objeto redunda en el ámbito de defraudaciones patrimoniales informáticas, es decir estafa informática o estafa producida por medio de manipulaciones informáticas, por ende *estafa informática.*

Una vez delimitados los vocablos antes analizados, nos preguntamos ¿qué es el delito de estafa informática?, en el sentido de establecer cuál es la naturaleza jurídica, siendo importante para poder comprender las distintas consecuencias que trae la determinación de la misma, por esta razón es que se ahondará en este tema a continuación.

III. La red como fuente de fraudes

Antes de realizar un *análisis técnico jurídico*, en forma previa se debe explicar las distintas figuras ampliamente conocidas por todos, pero muchas veces sólo de nombre y a su vez intentar separar, cuál de ellas tienen un carácter delictivo y cuáles no, para posteriormente poder hacer la conexión con las normas penales que regulan la materia en estudio, es decir si ellas se encuadran dentro de la hipótesis de la estafa informática que regula el Código Penal Español de 1995.

Internet, se encuentra al alcance de todos, permitiendo rebasar las fronteras entre los países, teniendo la información a disposición inmediata, sin embargo los usuarios reciben en forma masiva constantes comunicaciones no deseadas trasmitidas a través de distintos medios informáticos, no sólo correos electrónicos sino también mensajes a través de vía telefónica.

La red es el medio utilizado para defraudar en esta materia, por ello se pueden vislumbrar algunas formas para producirlo, existiendo variadas modalidades, según sea la forma o método utilizado para cometer dicho fraude informático. A

continuación se hará una breve descripción de las principales fórmulas de fraudes utilizados a través de internet. Es dable hacer presente, que se describirán en forma general, con sus principales características tomando en consideración el capítulo en que nos encontramos, no adecuándolas aun, a la estafa informática que regula el Código Penal Español, cosa que se hará, al momento de estudiar la estafa informática propiamente tal.

Las conductas delictivas que tienen relación con los fraudes en internet, nacen a su vez con los comienzos comerciales que la red entregó a muchas empresas, que tuvo como consecuencia la mejora en las ventas y con crecimientos en todo orden, que si la internet no hubiera sido posible lograr, creando con ello un mercado que no sólo abarca el país en el cual la empresa tenga su asiento o domicilio comercial sino que, los posibles usuarios o destinatario de los servicios se extendió a todo el mundo, siendo los potenciales consumidores sin límites. Sin embargo ello, esta oportunidad de poder tener potenciales consumidores en todas partes trajo también consigo desventajas las cuales han sido utilizadas y son utilizadas por los delincuentes informáticos.

De modo general se puede mencionar los fraudes cometidos en *compraventas y subastas por internet*, donde en muchos casos se recibe un producto de menor calidad o con condiciones que las tratativas preliminares no existían o requisitos que no fueron expresados al momento de la transacción. A su vez existen, *engaños de parte de las mismas empresas proveedoras* de servicios, donde se vende o se ofrece una velocidad a un precio determinado, sin embargo la misma empresa proveedora de alguna u otra manera entrega una descarga de Internet distinta, con ello obligando al usuario a pagar un precio más alto para mejorar la calidad del servicio de Internet entregado, no pudiendo el usuario saber que la misma empresa es la que limita la velocidad. Asimismo se puede mencionar fraudes, que tienen por fin que el usuario acceda a una *empresa fantasma que solamente existe en Internet* ofreciendo

oportunidades de negocios aparentemente, sólo con ganancias. Del mismo modo, se puede mencionar las *páginas falsas*, que tienen que ver con el rápido avance del mismo Internet, donde cualquier persona con simples conocimientos de informática básica pueden crear páginas, donde las personas pueden depositar o digitar sus números de cuentas bancarias, número de tarjeta de crédito o cualquier otro dato que sirva, para el fraude.

Por último, la gran cantidad de páginas virtuales que existen como son los *casinos virtuales*, donde se invita al usuario a participar, dándole un tiempo de confianza para que él mismo pueda apostar usando sus números de tarjetas de créditos, ganando bajos montos con el fin que el apostar montos más altos pierdan tanto el valor apostado, como a su vez el monto que figura como el crédito en dicha tarjeta. Desde hace años en múltiples conferencias mundiales se viene tratando distintos problemas relacionados con la nueva sociedad de la información, sentándose principios básicos para que las personas puedan usar la herramienta de internet, teniendo en consideración que también debe ser regulada, fijando objetivos y lineamientos por los distintos países, de esta existe la UIT[242] [243].

[242] Unión Internacional de Telecomunicaciones, *Cumbre Mundial sobre la Sociedad de la Información*. Ginebra 2003-Túnez 2005. Declaración de principios: N° 36. Si bien se reconocen los principios de acceso universal y sin discriminación a las TIC para todas las naciones, apoyamos las actividades de las Naciones Unidas encaminadas a impedir que se utilicen estas tecnologías con fines incompatibles con el mantenimiento de la estabilidad y seguridad internacionales, y que podrían menoscabar la integridad de las infraestructuras nacionales, en detrimento de su seguridad. Es necesario evitar que las tecnologías y los recursos de la información se utilicen para fines criminales o terroristas, respetando siempre los derechos humanos. N° 37. El envío masivo de mensajes electrónicos no solicitados *spam* es un problema considerable y creciente para los usuarios, las redes e Internet en general. Conviene abordar los problemas de la ciberseguridad y "spam" en los planos nacional e internacional, según proceda.

[243] La UIT es el organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación – TIC. Este organismo fue fundado en Paris en 1865 con el nombre de Unión Telegráfica Internacional. En 1934 adoptó su nombre actual, y en 1947 se convirtió en organismo especializado de las Naciones Unidas. Como organización basada en la asociación público-privada desde su creación, y cuenta en la actualidad con 193 países miembros y más de 700

A) Antecedentes del spam[244] (correo no solicitado)

Primero que todo se hace necesario, conceptualizar el termino *spam*[245] [246], el cual no existe una definición ni un consenso internacional a cerca de su

entidades del sector privado e instituciones académicas. La UIT tiene su sede en Ginebra (Suiza), y cuenta con 12 Oficinas regionales y de zona en todo el mundo. <http://www.itu.int/es>.

[244] Al respecto consultar legislación aplicable, para combatir el spam, los programas espías, y los programas maliciosos. Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico LSSI, (artículo 21 y 22); Ley 32/2003 de 4 noviembre General de Telecomunicaciones LGT(artículo 2 y 22); Ley Orgánica 15/1999 de Protección de datos de carácter personal; Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas); El Código Penal Español, (artículo 197).

[245] El spam o correo basura es una utilización abusiva del correo electrónico (e-mail) que resulta en abuso de recursos de quienes lo reciben (privados) y lo transmiten (toda la sociedad) en beneficio de quien lo envía (el spammer). Es el uso de recursos ajenos para fines propios. [accesible en] <http://www.cauce.org.ar>.

[246] Al respecto señala la OCDE: Los países miembros de la OCDE se unen para combatir al spam: El Consejo de la OCDE aprueba Directrices para la cooperación transfronteriza en el combate al spam. Gobiernos e industria deben esforzarse más para combatir al spam: De conformidad con un conjunto nuevo de Recomendaciones por parte de la Organización para la Cooperación y Desarrollo Económico (OCDE), del cual México forma parte, los gobiernos y la industria deben mejorar sus esfuerzos de coordinación a fin de combatir el creciente problema global del llamado "spam". Es vital que los países actúen rápidamente. Los correos electrónicos no solicitados -Spam- son cada vez más peligrosos y costosos tanto para el sector privado como para los consumidores. Interrumpe redes, disminuye la productividad, transmite virus informáticos y es usado cada vez más por delincuentes que roban contraseñas para acceder a información confidencial y a las cuentas bancarias. Toda vez que no existe una solución única para combatir el problema del spam, los gobiernos y el sector privado deben actuar en varios frentes. La OCDE conmina a los gobiernos a establecer políticas nacionales claras anti-spam y a otorgar más poder y recursos a las autoridades encargadas de vigilar el cumplimiento de la ley. La coordinación y la cooperación entre los sectores público y privado son críticas para lograr resultados en la erradicación del spam, resaltó el documento de la OCDE. Dicha Recomendación insta a los países a asegurarse que sus respectivas leyes permitan a las autoridades responsables de vigilar el cumplimiento de la ley compartir información con otros países y hacerlo más rápido y eficazmente. Los países también deberán establecer un sólo punto de contacto nacional a fin de facilitar la cooperación internacional. Educar

significado[247], sin embargo, se puede indicar que cuando se habla de *spam se refiere a todos los mensajes no solicitados y que son enviados en forma masiva y a su vez recepcionados en múltiples direcciones de correos electrónicos, teniendo como característica que no existe alguna solicitud previa del destinatario y además tampoco existe consentimiento alguno por parte del mismo*[248][249]. Estadísticamente,

---

a las personas sobre los riesgos del spam y cómo lidiar con este problema también es importante. Los gobiernos, en colaboración con la industria, deben emprender campañas nacionales educativas para incrementar la toma de conciencia entre los usuarios. Por ejemplo, lecciones sobre el spam y la seguridad en Internet deberían incluirse en los cursos sobre computación brindados en las escuelas y en aquellos cursos destinados a grupos de población vulnerables, como los adultos mayores. *(Recomendación en materia de cooperación transfronteriza para la efectiva aplicación de las leyes de combate al spam de abril der 2016.*

[247] Vale indicar también que SPAM es una palabra inglesa que hace referencia a una conserva cárnica: el *spiced ham*, literalmente *jamón con especias*. Dicho producto al no necesitar refrigeración, fue muy utilizada en todo el mundo, sobre todo en el ejército, que ayudó mucho en su difusión. Debido a esto, y a su baja calidad, se ha utilizado este término para hacer referencia a todos los mensajes basura que se reciben tanto en los grupos de noticias como en los buzones particulares. También conocido como UBE o UCE. [accesible en] http://www.lawebdelprogramador.com.

[248] La Corte Suprema de Justicia, de Estados Unidos de Norteamérica, en cuanto a la pornografía se refiere y en relación al *spam* ha dicho "no puedo definirla, pero la reconozco cuando la veo". Icauce.ar. [En línea], <http://www.cauce.org.ar>.

[249] VELASCO SAN MARTÍN, Cristos, *Las nuevas tecnologías de la información y comunicación*, Revista de investigación jurídica, Nova Iuris, Año I, núm. 1, México, 2005. Dicho autor nos dice en relación al spam: El correo comercial no solicitado o chatarra, mejor conocido como Spam es otro de los grandes problemas que afectan a los consumidores que navegan en Internet puesto que su utilización y difusión por parte de las empresas e individuos representa un problema significativo de costo y pérdida de tiempo y recursos para las personas que utilizan el correo electrónico. Generalmente, el spam es enviado por empresas de mercadotecnia o simplemente por individuos contratados específicamente por empresas ilegítimas que se especializan en elaborar listas de distribución de correos electrónicos para enviarlos directamente a las carpetas de los usuarios y dichos mensajes comúnmente se filtran cuando el usuario no cuenta con las herramientas necesarias para identificar, controlar y eliminar el spam. Aún y cuando el usuario cuenta con las herramientas para controlar el spam, muchas veces los mensajes normalmente se filtran a las carpetas conocidas como "bulkmail". Es a través del spam, que muchas empresas y proveedores de bienes y servicios llevan a cabo prácticas comerciales engañosas y fraudulentas hacia los consumidores y sobre todo ahora se ha convertido en un conducto para cometer otros ilícitos tales como el robo de identidad. El spam es el equivalente a recibir llamadas telefónicas que se utilizan para comercializar toda clase de productos o servicios de alguna empresa, sin embargo, la diferencia radica que en el Internet, el usuario termina pagando parte de estos

se estima que más del 85% de todos los correos electrónicos que circulan en la red son de naturaleza spam, no existiendo aun alguna manera para poder contrarrestar este problema, siendo no sólo un problema nacional sino que además global. Sólo existen soluciones preventivas y educativas para poder disminuirlo, pero no eliminarlo. A su vez, el *spam*, evoluciona con mucha facilidad y además tiene la particularidad que no sólo puede ser distribuido, a través de internet, sino que también por el uso de otras tecnologías, como pueden ser voz sobre protocolo IP y que actualmente es utilizado como el principal conducto para la distribución de sitios *phishing*, *virus*, *spyware* y otros software maliciosos[250].

La Corte Suprema de EEUU, en su afán de regular los spam, ha tratado de conceptualizar dichos correos de una manera casuística, por la variabilidad que demuestran los spammers, para seguir lanzando este tipo de correos. Ahora bien, la doctrina y las organizaciones internacionales, para referirse al spam, hacen una distinción de los elementos que le son comunes, como son la *masividad* y el carácter *comercial*, sin tomar en consideración si los envíos son o no *correos deseados o no solicitados.* Es decir, para tacharlo de spam debe estarse, a si resulta legítimo el envío de este correo no solicitado y cuando no. Ahora bien, al respecto se discute sobre el carácter comercial de dichos correos, tomando en cuenta que las definiciones de *comunicación comercial*[251], varían en cada legislación, cuando nos

---

mensajes ya que casi todos los cibernautas comparten en cierta medida el costo de mantener el Internet.

[250] Al respecto, se refiere a las estadísticas de spam, que indica la empresa Sophos que pública año una lista de los doce países que producen mayores volúmenes de spam. [en línea], <http://www.junk-o-meter.com_stats/index.php>.

[251] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. Artículo 2 Definiciones: A efectos de la presente Directiva, se entenderá por: f) "comunicación comercial": todas las formas de comunicación destinadas a proporcionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización o persona con una actividad comercial, industrial, artesanal o de

referimos a la promoción de algún bien o servicio, como ocurre en Europa[252]. De esta manera muchas veces se desechan las denuncias sobre estos correos, porque no son considerados comerciales[253] [254].

---

profesiones reguladas. No se consideran comunicaciones comerciales en sí mismas las siguientes: los datos que permiten acceder directamente a la actividad de dicha empresa, organización o persona y, concretamente el nombre de dominio o la dirección de correo electrónico; las comunicaciones relativas a los bienes, servicios o a la imagen de dicha empresa, organización o persona, elaboradas de forma independiente de ella, en particular cuando estos se realizan sin contrapartida económica.

[252] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)

[253] Al respecto se refiere AEPD, en resolución de archivo de actuaciones. De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la *asociación foro arbil,* en virtud de denuncia presentada ante la misma por D. J. F. U., l: Dicha sentencia, resuelva el caso en que se enviaban correos electrónicos con contenido periodístico a distintos usuarios en España. En lo medular indica: En cuanto a los fundamentos de derecho: 1° Es competente para resolver el "Cargo 1" de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 43 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (en lo sucesivo LSSI). 2° Actualmente, se denomina "Spam" o "correo basura" a todo tipo de comunicación comercial no solicitada, realizada por vía electrónica. De este modo, se entiende por "Spam" cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es el correo electrónico.

Esta conducta es particularmente grave cuando se realiza en forma masiva. El envío de mensajes comerciales sin el consentimiento previo está prohibido por la legislación española, tanto por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico (en lo sucesivo LSSI), como por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD). El bajo coste de los envíos vía Internet (mediante el correo electrónico) o mediante telefonía móvil (SMS y MMS), su posible anonimato, la velocidad con que llega a los destinatarios y las posibilidades que ofrece en cuanto a volumen de las transmisiones, han permitido que esta práctica se realice de forma abusiva e indiscriminada. 3° La LSSI, en su artículo 21.1, prohíbe de forma expresa el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. Es decir, se desautorizan las comunicaciones dirigidas a la promoción directa o indirecta de los bienes y servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional, si bien esta prohibición encuentra la excepción en el segundo párrafo del artículo, que autoriza el envío cuando exista una relación contractual previa y se refiera a productos similares. De este modo, el envío de comunicaciones comerciales no solicitadas puede constituir una infracción leve o grave de la LSSI. Además de suponer una infracción a la LSSI, la práctica del "Spam" puede significar una

A pesar de ello, al recibir estos correos que no han sido solicitados, por las personas o usuarios, no puede porque existir la necesidad de los mismos, es decir de tener que solicitar por la misma vía electrónica, la eliminación de la lista de envíos masivos, vulnerando con ello, derechos tanto legales como constitucionales. En definitiva lo que se comercializa es la dirección de correo electrónico, sin la autorización correspondiente, por ejemplo sería la similar situación, en el plano distinto a lo virtual, cuando un vendedor insistentemente, llega a nuestra puerta, y una y otra vez golpea para ofrecer un producto determinado, por ello se razona sobre

---

vulneración del derecho a protección de datos, ya que hay que tener en cuenta que la dirección de correo electrónico puede ser considerada, en determinados casos, como un dato de carácter personal. La Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, actualmente transpuesta en la Ley 32/2003, de 3 de marzo, General de Telecomunicaciones, que modifica varios artículos de la LSSI, introdujo en el conjunto de la Unión Europea el principio de "opt in", es decir, el consentimiento previo de la persona para el envío de correo electrónico con fines comerciales. De este modo, cualquier envío con fines de publicidad queda supeditado a la prestación del consentimiento, salvo que exista una relación contractual previa y el interesado no manifieste su voluntad en contra. En el supuesto examinado, se ha acreditado que en el período comprendido entre el 10/02/2004 y 12/03/2004, el denunciante recibió, en su buzón de correo electrónico profesional, ocho correos electrónicos no deseados remitidos desde diferentes dominios. En tres de ellos se hace referencia al "Foro Arbil" o bien a la revista digital denominada "Arbil". En los correos de fechas 11 y 12/03/2004, el dominio remitente corresponde a "AB. AB". Asimismo, consta que en los correos de fechas 10/02/2004 y 3/03/2004, se incita a acceder al dominio "...a@...a...". Sin embargo, de las actuaciones realizadas no ha podido acreditarse de forma cierta la persona o entidad que realizó los envíos denunciados. Por otro lado, del contenido de los correos se desprende que el denunciado no desempeña ninguna actividad comercial, industrial, artesanal o profesional, por lo que estos correos no pueden ser calificados como "comunicación comercial", a tenor de la definición contenida en el citado apartado f) del Anexo de la LSSI, pues no van dirigidos a promocionar una actividad comercial, industrial, artesanal o profesional. Por lo tanto, de acuerdo con el apartado a) del mismo Anexo, tampoco se trata de un servicio de la sociedad de la información, ya que para ello se requiere que la comunicación comercial se realice por una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional. Así las cosas, la remisión de estos correos electrónicos no ha podido acreditarse que supusiera infracción de la LSSI. Por lo tanto, de acuerdo con lo señalado, Por el Director de la Agencia Española de Protección de Datos, se acuerda: 1. *proceder al archivo de las presentes actuaciones*. AEPD, Expediente Nº: E/00075/2005, 29. XII. 2005 (Ponente: Sr. José Luis Piñar Mañas)

[254] Agencia Española de Protección de Datos: tiene encomendadas entre sus funciones la tarea de fomentar una cultura de protección de los datos personales que incluya la asistencia y tutela al ciudadano en el ejercicio de sus derechos y a los responsables de ficheros en el cumplimiento de sus obligaciones legales. [en línea], <www.agepd.es>.

en base al hecho que desde ya, es una intromisión a la intimidad, y de paso un daño posible a los equipos, a los ISP's, MSP's, o servidores.

Es del caso distinguir, otras figuras que pesar que pueden ser consideradas spam, no lo son como es el caso de los *abusos de correo electrónico*, ACE, que vienen afectar el fin para el cual está concebido en correo electrónico y por ende va afectar a los usuarios. Así, muchas veces se cree que es spam, correos comerciales los cuales no son solicitados por las personas como son los que ofrecen defensas ciudadanas, algunos con algún tipo de mensaje político o religioso, de asesoría financiera u otro grupo. Por esta razón hay que diferenciar la finalidad, puesto que si se trata de un fraude, este mismo es una conducta ilícita que debe ser sancionada, pero si se trata de un spam, que tiene una finalidad comercial, no es necesario que esta conducta que tiene las características ya indicadas anteriormente, se trate de una conducta que se encuentre tipificada y por ende sancionada en alguna legislación[255].

Cuando hablamos de spam, la doctrina internacional entrega a distinciones, como son *Scam o Junk mail*[256], el cual tiene mucha semejanza le spam, pero son aquellos que se refieren a correos relacionados con publicidad engañosa, como son los premios falsos, cadenas donde se indica que se tienen que reenviar para que se cumpla algún deseo, enriquecimiento al instante etcétera. A su vez también existen, la *difusión de contenido inadecuado*, y que por su naturaleza son ilegales, porque involucra la autoría o complicidad con algún tipo de hecho delictivo, como son aquellos que contienen programas piratas o que vulneren los derechos de propiedad de los softwares; los que contienen algún tipo de defensa o propaganda al

[255] FONSECA MARTÍNEZ, Claudia, *El spam y el ejercicio de la libertad*, en la 258 Red. Revista de Derecho Informático, número 081 de abril de 2005, accesible en: <http://www.alfa-redi.org/rdi-articulo>.

[256] TÉLLEZ VALDÉS, Julio, *Regulación del spam en México.* [en línea] Disponible en: <htpp: //www.razonypalabra.org.mx>.

terrorismo; los que contienen pornografía infantil o qué dirección en de alguna manera a dichos sitios; los que contienen estafas o fraudes; los que traen algún tipo de virus, etcétera. A su vez, se puede mencionar los *ataques con objeto imposibilitar o dificultar el servicio correo electrónico*, qué consisten en enviar un gran número de mensajes por segundo con el fin de paralizar el servicio por la saturación de las líneas, o la incapacidad de la CPU[257] del servidor, o el espacio disponible en el ordenador de la persona destinatario del usuario[258].

Por último, nos encontramos con combinaciones entre los mencionados, los cuales van a constituir delito dependiendo del fin para el cual ha sido enviado el correo electrónico ya mencionado naciendo con ello múltiples figuras como son el *phishing, camuflaje o munging*[259].

[257] La CPU es la parte central del procesamiento de un ordenador, encargada del procesamiento de todas las instrucciones que provienen del hardware y del software. Dicho termino proviene en ingles de las palabras *central processing unit*, (unidad central de procesamiento o unidad de procesamiento central). Físicamente la CPU es un circuito electrónico que realiza cálculos aritméticos, lógicos y operaciones de entrada-salida para las instrucciones. Usualmente al referirnos a CPU hablamos del procesador y más específicamente a sus unidades de procesamiento y de control, por ello según lo indicado en la CPU, no entran elementos como la memoria principal o la circuitería de entrada-salida. La CPU esta en directa relación con la memoria principal, es decir trabaja con ella, aunque físicamente está separada del microprocesador. Se suele llamar CPU al gabinete del ordenador, e incluso a todo el mismo ordenador, lo cual es un error. Ahora bien, cuando se habla de valor y rendimiento de un ordenador, estos dependen mucho de la CPU, puesto que algunos ordenadores emplean procesadores de múltiples núcleos, es decir un único chip contiene dos o más CPUs. También se utiliza las palabras, procesador central, microprocesador, o cerebro del ordenador para referirse a la CPU.

[258] Al respecto se refiere: Considerando que la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos (4) insta a los Estados miembros a garantizar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de los datos personales y, en especial, su derecho a la intimidad, de forma que los datos personales puedan circular libremente en la Comunidad. Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

[259] AEDI. Asociación Española para la Dirección Informática. Glosario de Spam. [en línea] España. Disponible en <http://www.aedi.es/asp/>.

B) Breve referencia al virus informático

El virus informático[260], a modo general es un programa que transporta una serie de instrucciones, que tenía la particularidad de producir algún daño contra un programa de uso normal. Éstos tienen por fin, alterar los sistemas automatizados de información, puesto que el ordenador del usuario se encuentra en desprotección o inseguro frente al dicho virus informático. Este programa al hacer ejecutable, por la unidad central del ordenador, lugar donde se aloja y que posteriormente puede ser acoplado al sistema para ser ejecutado por un ordenador distinto. Estos virus, también pueden ser activados según lo desee o no el delincuente informático, según sea la forma del diseño ya sea en proceso de espera o de ejecución obligada, impartiendo instrucciones distintas al ordenador infectado, con ello atentando contra los programas del mismo.

Determinante es su capacidad de multiplicarse, propagándose de ordenador en ordenador generando así a modo de emboscada una epidemia, produciendo anulación de archivos pérdida información entre otros daños. Se dice que los creadores decidieron otorgarle el nombre de virus, debido a su gran parecido en su forma de actuar con virus biológicos puesto que al igual que ellos, atacan en cualquier momento, destruyen toda la información que éstos alcancen y deben ser eliminados antes que causen más daños irreversibles, en el ordenador en el cual

[260] Principales características de un virus informático: dañino, toda vez, todo virus causa daño, ya sea de forma implícita, borrando archivos o modificando información, o bien disminuyendo el rendimiento del sistema; auto-reproductor, ningún otro programa tiene la capacidad de auto replicarse en el sistema; subrepticio puesto que le permite ocultarse al usuario mediante diferentes técnicas, como puede ser mostrarse como una imagen, incrustarse en librerías o en programas.

reciben. Este programa, invisible para el usuario y que no lo detecta el sistema operativo, tiene un actor específico y subrepticio, cuyo proclama incluye un código suficiente y necesario para que utilizando los mecanismos especiales de ejecución, que tienen los ordenadores de los usuarios, puedan reproducirse formando réplica pesimismo, réplicas completas y que en forma secreta o discreta se alojan, en un archivo, disco u ordenador distinto al que ocupa y además con la capacidad de mutar.

Aunque no existe claridad sobre el nacimiento del virus informático se puede señalar que se ha dicho que nació aproximadamente el año 1949, con el ingeniero John VON NEWMAN[261], al crear algunos programas cuya estructura básica, tenían por objeto insertar programas para que se puedan multiplicar y reproducirse sin parar. Por otro lado, cuando David GERROLDEN[262], en su novela de nombre *when herlie was one*, en la cual existía un ordenador o computadora que se suponía que se había creado semejante al cerebro humano, y cuando pretendía enlazarse con otras computadoras, lo realizaba a través de un virus[263]. Dicha, palabra es utilizada en la biología, y de acuerdo a las semejanzas con dicha ciencia se comenzó a utilizar en la

[261] Fue un matemático húngaro - estadounidense VON NEUMANN le dio su nombre a la arquitectura de que lleva su nombre, utilizada en casi todos los computadores, por su publicación del concepto. Entre 1944 y 1946 colaboró en la elaboración de un informe para el ejército sobre las posibilidades que ofrecía el desarrollo de las primeras computadoras electrónicas y de su contribución a dicho desarrollo, destacando la concepción de una memoria que actuase secuencialmente y no sólo que registrara los datos numéricos de un problema, sino que además almacenase un programa con las instrucciones para la resolución del mismo. En 1955, tras solicitar la excedencia de Princeton, fue nombrado miembro de la Comisión de Energía Atómica del gobierno Estadounidense. www.biagrafíayvidas.com

[262] GERROLD David (1944), cuyo verdadero nombre es David FRIEDMAN JERROLD, es un autor Estadounidense de ciencia ficción. Comenzó su carrera en 1966 cuando era estudiante universitario mediante la presentación de unos esbozos de historia para la serie de televisión Star Trek.

[263] Virus: según sus siglas en inglés, (Vital information resources under siege) *recurso de información vital bajo acoso.*

informática[264]. Ahora bien, estos virus informáticos, van naciendo de acuerdo a lo que requiere el usuario, el cual en la finalidad que el mismo posea, teniendo por fin atacar diferentes partes de un equipo informático, como por ejemplo sería la manera que comienza dicho equipo, el procesador de órdenes, la memoria libre y los recursos de internet etcétera.

Existen otros registros como son del año 1987, cuando en la Universidad de Delaware, en los disquetes encontraron virus, proviniendo de la casa de computación paquistaní, (brain computer services), quienes tenían por fin vender copias ilegales de software infectados para dar una lección a los piratas, por ello ofrecían sus servicios en forma posterior, para poder eliminar el virus del ordenador, a éste se le llamó *Brain,* y afectaba al sector del arranque del ordenador. Podemos decir entonces, que técnicamente existen *software,* que tienen por finalidad, o que fueron creados con el objeto de ejecutar alguna acción dañina, o también con el fin de alterar el funcionamiento normal y tranquilo del sistema informático, en el cual se introducen existiendo distintos tipos de software, de manera tal, que de las clasificaciones de los mismos pueden derivar a distintos tipos y en sus sub-clasificaciones, se pueden encontrar el denominado virus informático. Teniendo claro ello, podemos concluir que el virus informático, es sólo un tipo o variedad dentro de los programas dañinos, teniendo claro que al hablar desde un *punto de vista jurídico,* el software dañino es sinónimo de virus informático[265]. Para finalizar,

[264] En los años 70, en Xerox, Estados Unidos de América, en Palo Alto, fue creado por John F SCOTT, algo denominado *worm*, que tenía por misión enlazar varios equipos, es decir interconectarlos en ese momento alrededor de 100 equipos en red, sin embargo sólo fue instalado en seis equipos, el día siguiente todos los equipos encontraban infectados, con lo que el sistema fue reiniciado y reinstalado la red, pero al ser re encendido el problema volvió a surgir, por ello se decidió crear el primer anti-virus informático del planeta. Dicho programa *worm*, no fue creado como un virus propiamente dicho, sino que sólo fue un accidente de trabajo.

[265]Información sobre técnicas utilizadas por los virus y cómo eliminarlos, [En línea], <http://www.publispain.com/antivirus/que_son_los_virus.html>.

se puede señalar que para la RAE, en cuanto al virus informático se refiere, es un programa introducido subrepticiamente en la memoria de una computadora que, al activarse, afecta a su funcionamiento destruyendo total o parcialmente la información almacenada[266]. A su vez, para Julio TÉLLEZ, virus informático es un programa que puede infectar a otros, modificándolos para incluirles una copia ejecutable de sí mismo o cambiar parte del código[267].

C) Gusanos informáticos

Son conocidos con el término *worm*[268] [269]. Se puede señalar que los gusanos informáticos, son similares a los virus, sin embargo los gusanos no dependen de archivos portadores para poder contaminar otros sistemas, teniendo como principal característica que pueden modificar el sistema operativo, con el objeto de ejecutarse por sí mismo como parte del proceso de inicio del sistema. Los gusanos

[266] Diccionario de la Real Academia Española, [en línea], disponible en. www.rae.es.

[267] TÉLLEZ VALDÉS, Julio, *Aspectos legales de lo virus informáticos*, En actas del III Congreso Iberoamericano de informática y derecho, México, 1994, pág. 516.

[268] Worm: Gusano. Un programa destructivo que se copia a sí mismo a lo largo del disco y la memoria, consumiendo los recursos del computador y eventualmente inhabilitando el sistema. Programa que se mueve por toda una red y deposita información en cada nodo con propósitos de diagnóstico, o hace que los computadores inactivos compartan algo de la carga de procesamiento. Es programa similar a un virus que se diferencia de éste, en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos. www.iawebdelprogramador.com (diccionario informático)

[269] Nótese que el término inglés worm, también tiene otra acepción dentro del mundo de la informática: [en línea], Worm (de write once, read many), perteneciente a las tecnologías de almacenamiento de datos. No debe ser confundido con el de gusano informático. (diccionario informático), <www.iawebdelprogramador.com>.

informáticos, buscan vulnerabilidades del sistema buscando ingeniería social, con el fin de engañar a los usuarios y poder ejecutar, y poder reenviarse a sí mismo. Sólo hay que insertar el gusano en un sistema, infectarlo, dejar que se active, siendo la propagación rápida y masiva.

Por ello, los gusanos, consumen amplios recursos de denso sistema ya que los utilizan como lanzadera para infectar otros equipos, saturando incluso bloqueando por exceso de tráfico los sitios web, aunque estén adecuadamente protegidos por un antivirus actualizado esa es la capacidad mayor o más importante del gusano informático. Es dable señalar, que otra de las características importante del gusano informático es que se encuentran ocultos o enmascarados en un correo electrónico, que puede llegar de una fuente conocida. Estos programas que utilizan la red para expandirse de un sistema informático a otro que como se indicó, no necesariamente producen un daño, y presentan un crecimiento exponencial, con lo que puede infectar en muy corto tiempo a una red completa, un ejemplo de ello, son algunos gusanos informáticos conocidos en el mundo entero, *Melissa*[270], *I love you*[271], *Kournikova.*

[270] Melissa es un macrovirus que infecta documentos de Microsoft Office. El 26 de marzo de 1999 y en apenas unos días, protagonizó uno de los casos de infección masiva más importantes de la historia de los virus informáticos. De hecho, compañías como Microsoft, Intel o Lucent Technologies tuvieron que bloquear sus conexiones a Internet debido a la acción de Melissa. Fue creado por David SMITH de Aberdeen, Nueva Jersey, el cual causó más de 80 millones de dólares en daños a las empresas. SMITH fue condenado a 10 años de prisión, posteriormente colaboraría para ayudar al FBI en la búsqueda del creador del virus informático Kournikova.

[271] Virus informático I love you: Conocido por los usuarios como el *virus del amor*, pertenece a la categoría de gusano, capaz de reproducirse, a través de las redes electrónicas, modificando los ficheros del ordenador infectado y se transmite, por medio de correo electrónico cuando el internauta abre el fichero donde se aloja. Primeramente fue una tesis que realizó Onel de GUZMÁN, un joven filipino de 24 años que estudió en la facultad de informática del colegio universitario AMA, en la capital de Filipinas. El texto final, entregado el 1 de febrero del 2000, era toda una guía sobre cómo robar códigos secretos a través de Internet o cómo introducirse en un ordenador ajeno y tomar su control. Era, en definitiva, una copia del virus *I love you*, que tres meses después iba a dejar en evidencia la vulnerabilidad del nuevo orden mundial de internet y las tecnologías informáticas. Tuvo problemas con los profesores por su trabajo, rechazando la tesis. El

IV. Modalidades más frecuentes utilizadas a través de internet para la estafa informática

La ingeniería social[272], detrás de un virus informático, como dijimos tiene por fin que un programa informático tenga la capacidad de causar daño, y que utilice su principal característica que no es otra que puede replicarse asimismo y propagarse

4 de mayo de 2000 Onel de GUZMÁN decidió, probar por su cuenta el proyecto que había preparado para su tesis, el resultado final fue un virus capaz de infectar aproximadamente 50 millones de computadores en todo el mundo, causando pérdidas de más de 5500 millones de dólares en daños. A través de un título como *te quiero* o *te amo*, acompañado de un archivo adjunto, GUZMÁN consiguió crear el pánico, incluso entre los expertos de seguridad informática. En España, llegaron a varios medios de comunicación españoles como el diario *El País*, interrumpiendo durante varias horas su actividad, *la Cadena Ser y los periódicos La Razón y Abc*, entre otros, que registraron anomalías en los correos electrónicos, sin repercusiones en su trabajo. Iberia informó que también registraron la entrada del virus antes que produjera problemas, mientras que fuentes del Ministerio de Ciencia y Tecnología aseguraron no tener constancia, que se hubieran producido anomalías en los sistemas informáticos de la administración. A pesar de los problemas causados por este virus, su creador nunca fue condenado por un tribunal, ya que en el momento de probar su experimento, todavía no existían leyes específicas para estos ataques en Filipinas. I love you se instala en el ordenador y borra ficheros de gráficos y de sonido extensiones JPG, JPEG, MP3 y MP2, sustituyéndolos por otros con el mismo nombre y la extensión VBS e introduciendo el código malicioso. Existe un detalle preocupante en este virus que lo diferencia de su predecesor Melissa, puesto que a diferencia de éste, que se incluía en un documento elaborado con el procesador de textos Microsoft Word, el código del virus del amor es perfectamente legible y puede ser modificado sin dificultades por un usuario. De este modo, cualquiera que tenga unos conocimientos mínimos de programación, podría modificar el código y alterar la firma del virus, de modo que no fuera reconocido por la vacuna. En definitiva causó en dólares, 100 millones en daños.

[272] Ingeniería social, es la acción o práctica que tiene por fin de obtener información confidencial, a través de la manipulación de usuarios legítimos. Esta práctica es utilizada por investigadores privados, delincuentes informáticos, para tener información o acceso a sistemas de información que les permitan realizar algún acto que perjudique o exponga a la persona u organismo comprometido a riesgos o abusos. La ingeniería social se sustenta en que es vulnerable y por ende el eslabón débil es el usuario. Se utiliza comúnmente el teléfono Internet para engañar a la persona, fingiendo ser, por ejemplo empleado de algún banco, compañero de trabajo o algún técnico de alguna empresa de Internet. Por vía de Internet también se utiliza, la renovación de permisos o acceso a páginas web o correos electrónicos falsos que solicitan respuestas e incluso cadenas de ayuda, revelando con ello información útil violando políticas de seguridad y datos personales. En definitiva, utilizan la reacción común del usuario a ciertas situaciones, evitando con ello tener que usar otros recursos informáticos más riesgosos o engorrosos para poder vulnerar uno encontrar los agujeros de seguridad de los sistemas informáticos.

en la red, por ello las conductas que son especialmente favorecidas por el medio internet pueden combinarse entre ellas, y utilizarse independientemente.

Los virus activan cuando se ejecuta el programa respectivo o el mismo archivo que lo contiene, y si el ordenador que tiene el virus intercambien formación con otros ordenadores, es casi seguro que se produzca la infección con los otros, ya instalado el virus va reproduciéndose, o copiándose una y otra vez en los discos duros, o en programas, ficheros, medios de almacenamiento externo de información, y también en los mismos correos electrónicos etc.

Los ordenadores al momento de tener estos virus, presentan síntomas o características como por ejemplo, su mayor lentitud, mensajes que prestan irracionalidad, pérdida de información o merma en la utilización del sistema total o parcial del mismo ordenador. Por ello, se hace tan necesario los servicios de seguridad, con el fin de corporal alguna capa de protocolo, las cuales conllevan algún cifrado, firma digital, control de acceso que tienen por fin aplicar la *criptografía*[273], la cual es una herramienta básica para todos los servicios de seguridad, ocupándose que las comunicaciones no pierdan dicha característica en presencia de delincuentes informáticos.

A) Malware (software malicioso)

[273] Estudio, de las técnicas matemáticas relacionadas con la seguridad de la información, confidencialidad, integridad de datos, autentificación de reconocimiento del origen de los datos. Por ello un sistema computacional mente seguro se cumple alguna de las condiciones siguientes: el coste del Cristo análisis excede el valor de la información obtenida; el tiempo necesario para el Cristo análisis excede el tiempo de vida útil del información. Universidad de Sevilla, *Ingeniería Informática, Curso N° 5° de Criptografía*, (Doc-Tec), 2007/2008, [en línea] <http://ma1.eii.us.es>.

Denominación genérica para hablar o referirse a cualquier tipo de programa o archivo dañino para el ordenador. Existen otras formas de descargas en los ordenadores, de todos estos programas como seria en el caso de la aparición en la pantalla, de una determinada página web la cual informa o da a conocer a los usuarios del sistema futuros premios o advertencia de detección de virus, o asimismo advertencia de alguna situación pendiente del usuario para retirar algún tipo de encomienda o carta, provocando en la persona que se genere en la persona que se genere una preocupación o llamada de atención la cual trae como consecuencia que él mismo ejecute la descarga de la aplicación, estando entonces en presencia de un *malware*[274].

Es dable recalcar, que una de las funciones principales del malware, y que puede obtener el control del acceso remoto a sistema de cómputo, y así como grabar y enviar información y datos a los de los usuarios a terceras personas sin su conocimiento y consentimiento, con ello rastreando los hábitos del usuario Internet y los portales que visita trasmitiendo la información necesaria a una fuente central para poder defraudar[275]. Podemos hablar en forma variada de distintos tipos de software malware, como son en forma genérica los llamados virus como gusanos, troyanos, puerta trasera spyware, keyloggers, etcétera.

[274] Este término es utilizado para referirse al software o programa de computo que son introducidos en los sistemas de información de los usuarios para causarles algún daño o simplemente para modificar su uso y obtener su control. Siendo una de las funciones principales del *malware* que el ciberdelincuente, puede obtener el control y el acceso remoto al sistema de cómputos, y así poder grabar y enviar información y datos de los distintos usuarios a terceras personas sin tener conocimiento ni consentimiento alguno de los mismos, de esta manera se rastrean los hábitos de una persona en internet y todos los portales que visitan pudiendo transmitir a una fuente central. Palabra que proviene de la agrupación de *malicious software*.

[275] OECD, Malicous software (malware): A segurity therat to the Internet economy, What is a malware?, pág. 10 y sigs. [en línea], <http://www.oecd.org/sti/40724457.pdf>.

B) Spyware (programa espía)

Estos son conocidos como archivos espías, *spyware*, mediante los cuales se logra la obtención de datos para suplantar a una víctima, reemplazando su personalidad para utilizar un servicio con alguna naturaleza económica, así por ejemplo, tenemos las claves bancarias o de otro tipo de acceso, como son los números de tarjetas de créditos u otros similares. Al obtener la fórmula de acceso, estos mismos son posteriormente utilizados para recaudar y obtener alguna ventaja económica. Esa forma de obtención de clave, se realiza ingresando al sistema operativo del ordenador de la víctima. Nos encontramos con una forma de obtención de clave usando la propia red, y por supuesto no teniendo autorización del titular o también teniendo acceso a la información en forma material es decir sustrayendo físicamente los mismos números o claves de acceso.

La manera que se obtienen de las claves pueden ser muy variadas, ya sea en forma remota ingresando a un ordenador, puesto que se utiliza su IP para ello, o simplemente introduciendo en dicho ordenador estos archivos espías, para que posteriormente se puedan enviar al delincuente de la red los datos informáticos del sistema donde los han instalado, logrando con ello poder acceder al ordenador de la víctima.

Podemos señalar entonces, que a través de estos software espías, que pueden ser instalados en los ordenadores múltiples programas, para tener el conocimiento de las claves o números de acceso, los cuales incluso pueden ser activados por la propia

víctima, a través de ciertos controladores *activex*[276]. En definitiva, estos software espías tienen la capacidad de auto instalarse en los ordenadores personales de los usuarios, con el objeto de conocer su identidad monitoreando el comportamiento de la persona al utilizar los distintos sistemas o navegar por internet, estos software al igual que los cookies[277], son capaces de crear bases de datos y proporcionar la información correspondiente, esto lo hacen a base de las distintas preferencias o hábitos de los usuarios. Al respecto se puede citar a Steven Gibson[278], quien descubrió algunos mecanismos espías en una gran cantidad de programas software, todos ellos utilizados tanto por los gobiernos, las empresas y las personas, afirmando que en un ordenador personal, es muy altamente probable que contenga algunos programas espías escondidos en sí mismo, puesto que en el mundo existen millones de archivos espías instalados, sin que sepan las personas[279].

C) Troyanos

Es un software dañino disfrazado de software legítimo. Un programa caballo de Troya es capaz de replicarse por sí mismo y por tanto, son aplicados con

[276] CHOCLAN MONTALVO, José, *Fraude informático y estafa por computación, en internet y derecho penal*, Cuadernos de derecho judicial, 2001, pág. 330 y siguientes.

[277] En inglés significa galleta, sin embargo relacionado con la informática, es un servidor que guarda información sobre un usuario en un equipo determinado.

[278] Ingeniero de software estadounidense, investigador de seguridad.

[279] Existe un programa de Scareware, un tipo de programa maligno que se vende empleando prácticas de publicidad engañosa y antiética, usualmente recurriendo a amenazas inexistentes. Se aprovecha del miedo, ingresando al ordenador mediante *pop-ups*, estos advierten de virus que se apoderado del sistema. Posteriormente obligan a descargar varias aplicaciones de seguridad que eliminan los supuestos virus, sin embargo llevan dichas descargas llevan envueltos malware.

cualquier tipo de software por un programador o puede contaminarlo el equipo por medio del engaño. Debe su nombre al hecho histórico en el cual los griegos invadieron la ciudad de Troya, utilizando el engaño, mediante un caballo de madera, donde en su interior ingresaron los griegos para invadir dicha ciudad. Estos programas encubiertos, parecen que fueran útiles, pero sin embargo, ellos ocultan un código para ejecutar acciones indeseables sobre el ordenador, activándose cuando el usuario utiliza la aplicación, que piensa o cree que es útil.

En definitiva, estos programas muestran lo que el usuario ve en su ordenador, son técnicas para espiar a personas, mediante un acceso remoto monitoreando lo que el usuario está haciendo en cada instante, capturando por ejemplo la digitación que se usa en ese momento en el teclado, obteniendo las contraseñas que captura la pantalla. Siendo la contra respuesta de los usuarios a los ataques troyanos, la educación informática, en el sentido de no ejecutar nada que sea desconocido manteniendo su vez los antivirus actualizados en el equipo correspondiente.

D) Puerta trasera

Se han denominado puerta trasera o en inglés *backdoor*, un software que tiene la particularidad, que permite a quien conoce el funcionamiento, el acceso al sistema del ordenador, poder saltar los métodos usuales de auténtica aplicación, con algún fin delictivo. Estos programas son incluidos deliberadamente para uso legítimo, también son un riesgo para la seguridad, ya que cualquier persona que la descubre pues era sistema en el que están ejecutando.

Para bien la configuración del mismo ordenador, puede involuntariamente crear el mismo efecto de una puerta trasera, por lo mismo involuntariamente se

puede ser ejecutando estos programas infectando sistema, para instalarse permanentemente. También se puede infectar el sistema con estas puertas traseras por medio de gusanos que los llevan como carga y se ejecutan como un procedimiento de inicialización del sistema. Igualmente puede ocurrir que al no retirar estas puertas traseras de la versión de lanzamiento del ordenador, quiere el acceso vulnerado por vulneración permanente. Antiguamente se utilizaba como una práctica común en los primeros días de las redes de computadoras, para permitir que los proveedores dieran servicio a las instalaciones de clientes sin que estar físicamente el lugar.

E) Redes zombies

Cuando hablamos de zombies, identificamos a los ordenadores que de alguna manera es infectado por algún tipo de malware, las formas de infección pueden ser muchas pero normalmente es una puerta trasera, entrada que ha sido encontrada por la vulnerabilidad del ordenador del usuario. Al hablar de red zombies, consecuentemente con el fraude no ha sido autorizado por el usuario del ordenador correspondiente, hablando en términos de secuestro del equipo.

En este caso lo primero que hace es el delincuente informático, toma la máquina, arma una red de miles de PCs, y después analiza cuál es el uso que le dará. Al hablar de *botnets*[280] [281], (anglicismo que se refiere a la asociación en red),

[280] Término que hace referencia a una colección de *software robots, o bots*, que se ejecutan de manera autónoma (normalmente es un gusano que corre en un servidor infectado con la capacidad de infectar a otros servidores). El artífice de la *botnet* puede controlar todos los ordenadores o servidores infectados de forma remota. A través de ellas, se realiza envío masivo de *spam*, espionaje informático, robo de identidades, descarga de material ilegal, apropiación

hablamos de máquinas autónomas, puesto que ellos concentran un gran número de máquinas zombies que se coordinan, pudiendo usar todas ellas una vez tomadas y en un segundo inundar miles de casillas de correo con spam. También pueden alojar, en los ordenadores, sitios de phishing, o páginas de pornografía, igualmente pueden sustraer información, y propagar malware, pudiendo en la misma red ir variando el delito. Un dato necesario es que la red botnets, se venden o se rematan en foros de hackers[282] [283].

F) keyloggers (registrador de teclas)

---

fraudulenta de datos confidenciales, y otras actividades de índole delictiva, atacando en forma masiva la red. [en línea] <https://www.shadowserver.org>.

[281] Las *botnets* se utilizan principalmente para los siguientes propósitos: 1. Localiza e infecta otros sistemas de información con programas de bot (y otro malware). Esta funcionalidad, en particular, permite a los atacantes mantener y construir su oferta de nuevos robots para que puedan realizar las siguientes funciones, entre otras cosas. 2. Realizar ataques de denegación de servicio distribuidos (DDoS). 3. Como un servicio que se puede comprar, vender o alquilar. 4. Gira las direcciones IP bajo uno o más nombres de dominio con el fin de aumentar la longevidad de los sitios web fraudulentos, en los que, por ejemplo, los sitios de phishing o malware. 5. Enviar spam, que a su vez puede distribuir más malware. 6. Robar información confidencial de cada computadora comprometida que pertenece a la botnet. 7. Hosting del sitio de phishing malicioso en sí, a menudo en conjunto con otros miembros de la botnet para proporcionar redundancia. 8. Muchos clientes de botnet permiten al atacante ejecutar cualquier código adicional de su elección, haciendo que el cliente de botnet sea muy flexible para agregar nuevos ataques. Pág. Malicius Software (malware): A security threat to the internet economy, Ministerial Background Report, DSTI/CCP/REG (2007) 5 Final, 2008. Disponible en: <http://www.oecd.org/datao-ecd.pdf>.

[282] En marzo de 2016 la Guardia civil española, y el FBI, desarticularon en Madrid la red *mariposa*, una red zombi que tenía bajo control 13 millones de ordenadores, de los cuales 180,000 estaban en la República de Argentina.

[283] DUNHAM, Ken / MELNICK, Jim, *Malicious Bots, An Inside Look into the Cyber-criminal Underground of the internet*, Editorial Taylor& Francis Group, Nueva York 2009. [disponible], http://taylorloranfrancis.com>.

O también registro de tecleo, es otras de las formas que se hace necesario mencionar y que comúnmente se encuentra en los denominados cibercafé, son los llamados *keyloggers*[284], (vendría siendo un programa malvare), que tienen como fin registrar todo lo que la persona digite en el teclado, pudiendo con ello posteriormente el ciberdelincuente, acceder a las claves abriendo dichos programas. Es un tipo especial de software espía o spyware, instalándose comúnmente junto a otros que prometen mejorar de alguna forma el ordenador[285].

Este modalidad también es constantemente usada con fines lícitos, toda vez que estos monitorizadores a distancia o teclados keyloggers, son utilizados como una *técnica nueva de investigación* penal, la cual ha sido tema de debate al analizar las medidas restrictivas de libertad o restrictivas de derecho que pugnan con la investigación criminal informática actual, valorando los derechos que se tienen sobre el secreto en las telecomunicaciones y la intimidad.

Estos programas informáticos que son capaces de duplicar la información tele comunicativa del contenido de los archivos y terminar en otro, donde la policía con autorización judicial, puede obtener información para verificar o descartar algún ilícito que se esté cometiendo y que además tenga directa relación con la

[284] Existen dos tipos de keyloggers, siendo el primero, el KEYLOGGER POR HARDWARE que se refieren a dispositivos físicos que se encargan de registrar las pulsaciones, y el KEYLOGGER POR SOFTWARE que se refieren a programas informáticos que se encargan de registrar las pulsaciones. [accesible en], <www.alegsa.com>.

[285] SAP de Santa Cruz de Tenerife, Sección 2ª, Nº 248, 29. V. 2014, (Ponente**:** María Jesús GARCÍA SÁNCHEZ), Explica dicha sentencia acerca de esta técnica, refiriéndose que "También la captura de claves puede realizarse a través de programas que interceptan la información en el momento que se introducen en la banca on- line real, técnicas denominadas "Man In Thee Middle" como el uso de keyloggers (programas que capturan las pulsaciones del teclado) o el uso de programas de control remoto".

investigación penal de que se trata. La base de lo anterior o su fundamento legal estaba en la regulación del artículo 579.3 LECrim.[286][287], pero sin embargo, se planteaba que dicho artículo era insuficiente para fundar una resolución judicial que afectará garantías constitucionales, porque se refería a las intervenciones telefónicas, vulnerando con ello lo indicado en la carta fundamental de España, en su artículo 18.3[288], referente al secreto de las comunicaciones, también relacionado con el apartado segundo del artículo 10 de la misma Constitución[289], que además se enlaza con el artículo 96[290], que dice relación con los tratados o convenios internacionales

[286] Dicho artículo 579 señalaba: 1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa. 2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa. *3. De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos.* 4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación.

[287] VELASCO NÚÑEZ, Eloy, *Delitos cometidos a través de internet, cuestiones procesales*, 1ª edición, Editorial Ley, Madrid, 2010, pág. 213 y sigs.

[288] Constitución española de 1978: artículo 18 N° 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución. Disponible es: <http://www.congreso.es/consti/constitucion/indice/index.htm>.

[289] Constitución española de 1978: artículo 10 N° 2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

[290] La Constitución española de 1978: Artículo 96 N° 1. Los tratados internacionales válidamente celebrados, una vez publicados oficialmente en España, formarán parte del ordenamiento interno. Sus disposiciones sólo podrán ser derogadas, modificadas o suspendidas en

debidamente ratificados por España, debiendo respectar el artículo 12[291], de la Declaración Universal de Derechos Humanos, y también el Pacto Internacional de los Derechos Civiles y Políticos[292].

La jurisprudencia reiterada declaraba que la legislación ya no tenía la fuerza necesaria, para hacer frente a las nuevas tecnologías, por ello insuficiente eran, las normas, para fundamentar una resolución judicial que afectara derechos fundamentales[293].

El artículo 579 LECrim.[294], fue puesto al día según la legislación internacional vigente por la Ley Orgánica 13/2015, de 5 de octubre, de modificación

---

la forma prevista en los propios tratados o de acuerdo con las normas generales del Derecho internacional. Disponible es: <http://www.congreso.es/consti/constitucion/indice/index.htm>.

[291] *Declaración Universal de Derechos Humanos*, adoptada y proclamada por la Resolución de la Asamblea General N° 217 A (iii) del 10 de diciembre de 1948, artículo 12: nadie será objeto de injerencias arbitrarias a su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a protección de la ley contra tales injerencias o ataques. <http://www.derechoshumanos.net>.

[292] *Pacto Internacional de los Derechos Civiles y Políticos*, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966, artículo 17 dispone: 1. Nadie será objeto de injerencias arbitrarias ilegales en su vida privada, su familia su domicilio o su correspondencia ni de ataques ilegales a su onda de reputación. [en línea], <http://www.derechoshumanos.net/normativa>.

[293] STC N° 49, de 5 IV. 199, (Ponente: Magistrado don Tomas S. VIVES ANTÓN). Tráfico de drogas y contrabando. Secreto de las comunicaciones telefónicas y presunción de inocencia. Reserva de ley sobre toda inherencia sobre los derechos fundamentales. Dicha sentencia en lo medular analiza el deber genérico de motivación de las resoluciones judiciales y en especial rigor cuando se trata de limitar derechos fundamentales. A su vez, refiere respecto del principio de proporcionalidad sobre la injerencia en el secreto de las telecomunicaciones. Declarando que han sido vulnerados los derechos de los recurrentes al secreto de las comunicaciones telefónicas y a un proceso con todas las garantías.

[294] *LECrim.* Artículo 579. De la correspondencia escrita o telegráfica. 1. El juez podrá acordar la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, que el investigado remita o reciba, así como su apertura o examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa, siempre que la investigación tenga por objeto alguno de los siguientes

de la *Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*.

De acuerdo a dicha modificación lo que se pretendía, era actualizar dicho cuerpo normativo de acuerdo a la Directiva 2013/48/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, y con ello reformar distintas temáticas relativas a los derechos fundamentales y garantía procesales y de paso actualizar dicha ley de acuerdo al uso de las nuevas tecnologías, proporcionando herramientas necesarias para la investigación de los delitos que se cometen al amparo de los sistemas de comunicación telemática.

La forma en que los delincuentes informáticos utilizan dicha modalidad de fraude, puede ser utilizada para labores investigativas siempre y cuando la resolución del tribunal se encuentre suficientemente motivada, puesto que las

---

delitos: 1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión. 2 º Delitos cometidos en el seno de un grupo u organización criminal. 3.º Delitos de terrorismo. 2. El juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales o inferiores períodos hasta un máximo de dieciocho meses, la observación de las comunicaciones postales y telegráficas del investigado, así como de las comunicaciones de las que se sirva para la realización de sus fines delictivos. 3. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida. 4. No se requerirá autorización judicial en los siguientes casos: a) Envíos postales que, por sus propias características externas, no sean usualmente utilizados para contener correspondencia individual sino para servir al transporte y tráfico de mercancías o en cuyo exterior se haga constar su contenido. b) Aquellas otras formas de envío de la correspondencia bajo el formato legal de comunicación abierta, en las que resulte obligatoria una declaración externa de contenido o que incorporen la indicación expresa de que se autoriza su inspección. c) Cuando la inspección se lleve a cabo de acuerdo con la normativa aduanera o proceda con arreglo a las normas postales que regulan una determinada clase de envío. 5. La solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa.

adaptaciones normativas y la forma de investigar deben ir de acuerdo a la realidad tecnológica, cuyo tratamiento sólo debe adecuarse a las telecomunicaciones que ahora toman una forma distinta de la correspondencia clásica. De acuerdo a ello, la única manera que exista por ejemplo una orden de detención suficiente fundamentada, y con indicios suficientes para otorgarla, es que previamente se haya monitoreado la terminal correspondiente, sin que el presunto delincuente se entere, y además antes que dicha información desparezca, porque los soportes al ser intangible, la información de torna volátil y debe ser conservada.

G) Bombas lógicas y bombas de tiempo

Son programas que se ejecutan en unos momentos específicos o cuando o existen condiciones óptimas para ejecutarlos, utilizando una rutina programada posterior a su instalación, esperando circunstancias apropiadas de tiempo, de fecha, de realización de algún pago etc. en este caso es necesario realizar una determinada conducta, como sería por ejemplo digitar una palabra determinada o cierta combinación en las teclas para que se active, o también ejecutan un programa especial.

Ahora bien, en cuanto al virus troyano, que aparenta una función que pudiera ser útil para el usuario, pero sin embargo en forma posterior es completamente dañina, se diferencia de las bombas lógicas, en cuanto que el troyano solamente se activa cuando se ejecuta el programa, en cambio las bombas lógicas, requiere además un número mayor de condiciones, permaneciendo inactivas esperando el momento adecuado. En cuanto las *bombas de tiempo*, podemos señalar que son programas altamente destructivos, creado para ser ejecutados en determinado tiempo

incluso a cierta hora del día, y que son capaces de destruir e inutilizar equipos, redes y servidores tanto física como lógicamente.

H) Camaleón

Son similares a los virus troyanos, siendo programas malignos disfrazados como otros programas generalmente enviados por correo electrónico, actuando como un programa similar a otro que sea de confianza del usuario, pero con la diferencia que produce inmediatamente los daños, no basándose en un programa que ya existe en el ordenador del usuario sino que diseña otro completamente nuevo, utilizándose en aplicaciones concretas, y no en programas comerciales. Es decir estos imitan fielmente el programa que reproducen. Un programa de tipo camaleón dañino, se puede utilizar como por ejemplo, con el fin de derivar dinero de una cuenta a otra, a través de una transacción bancaria pero utilizando la técnica del centavo, es decir poco a poco sin que el usuario se dé cuenta van sustrayendo dinero, con este programa similar al real.

I) Phishing[295] [296] (cosecha y pesca de contraseñas)

[295] APWG: Anti-Phishing Working Group, se refiere a una asociación de industrias cuyo principal objetivo es acabar con el robo de identidad y fraudes resultantes del creciente problema del phishing, en correos electrónicos fraudulentos. Se puede decir que la industria mundial, se organizó para la aplicación de la ley, y la coalición gubernamental centrándose en la unificación de la respuesta mundial a la delincuencia cibernética mediante el desarrollo de los recursos de datos, normas de datos y modelos de sistemas de respuesta y protocolos para los sectores público y privado. Dicho organización define qué fraude como mecanismo que emplea tanto técnicas de ingeniería social y técnicas evasivas para sustraer la identidad, los datos personales y la información financiera de los consumidores.

El phishing es un tipo de engaño creado por hackers, pero en este caso con fines delictivos, para obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc. Generalmente, el engaño se basa en la ignorancia del usuario, porque ingresa a un sitio que presume real, auténtico o que es el legal[297].

El TS, al *phishing* lo ha definido o expresado como el correo recibido, que proviene de grupos organizados que utilizaban la red informática para la captación de los datos confidenciales de los titulares de las cuentas, y consistente en envío masivo de correos electrónicos que simulan proceder de entidades bancarias, cuyo mensaje imita exactamente el diseño, logotipo, firma, utilizado por la entidad bancaria para comunicarse con sus clientes, y a través de los cuales obtienen datos personales que, al ser introducidos en la página falsa, son captados para ser utilizados de forma fraudulenta. En dichos correos se apremia al internauta a actualizar datos personales, como nombres de usuarios y contraseña de motivos de seguridad, mantenimiento, mejora en el servicio, etc., redirigiéndoles a una página que imita a la original e introduciendo sus datos en dicha página falsa, lo que permite a los autores de la misma tomar los datos y utilizarlos de forma fraudulenta[298].

---

[296] MILLETARY, Jason, *Tendencias técnicas en los ataques de phishing*, Documento del Centro de Coordinación (CERT), 2005, Universidad de Carnegie Mellon. ubica en la ciudad de Pittsburgh (Pensilvania). Destacado centro de investigación superior de los Estados Unidos en el área de ciencias de la computación y robótica. [accesible en:] http://resources.sei.cmu.edu/

[297] RODRÍGUEZ-MAGARIÑOS, Fautino, *Nuevos delitos informáticos: phising, pharming, hacking y cracking,* 2009, Recuperado, en <htpp:/web.icam.es/index.php>.

[298] STS N° 559, Sala 2ª de lo Penal, de 16. III. 2009, (Ponente: Sr. Siro Francisco GARCÍA PÉREZ). SAP de Vizcaya, Sección 3ª, Nº 429, de 10. XI. 2016, (Ponente: Sra. María Concepción MARCO CACHO). Antecedentes del hecho Número tercero: En el presente caso, el *phishing* se origina con la suplantación de la identidad del banco por parte del phisher con la finalidad de

El *phishing*[299] *o pescado de datos*, hoy por hoy es una de las técnicas más frecuentes usadas por los delincuentes informáticos. Dicho terminó proviene de las palabras del idioma inglés *password harvesting y fishing*, que en su conjunto sería *cosecha y pesca de contraseñas*, por ende *phicher*, hace alució a la persona que realiza este tipo de acciones. Desde los años 90 en adelante, se comenzó a utilizar esta técnica, la cual se centraba en el envío en gran cantidad de correos electrónicos con un contenido fraudulento, tanto a personas naturales como jurídicas, tomando el nombre de *smishing*[300] o vishing[301] según la modalidad cuando los mismos son remitidos, a través de mensajes o llamadas telefónicas. La información enviada al usuario, va en directa relación con sus identidades en línea y con las credenciales de

adquirir información confidencial sobre contraseñas de cuentas bancarias, tarjetas de crédito o cualquier otra información en relación con el banco, que permita entrar en las cuentas de los usuarios en Internet de banca electrónica. El internauta recibe un correo electrónico o cualquier mensaje instantáneo, a través del cual se le informa de que debe cambiar sus claves bancarias, proporcionándole un link a través del cual pueda acceder a la página Web de la supuesta entidad bancaria y allí realizar la modificación aconsejada. En la mayoría de los métodos de phishing se utilizan técnicas de engaño, a través de las cuales el phisher utiliza contra la víctima el propio código de programa del banco o servicio similar, adquiriendo la página Web la verdadera apariencia de la entidad bancaria. Igualmente, resulta muy habitual que el internauta reciba un correo en el que se le informe de que debe verificar sus cuentas, seguido por un enlace que parece la página Web oficial de la entidad bancaria. También definición SAP Nº 178, 04. V. 2015, (Ponente: Beatriz Patiño Alves), Madrid, en fundamento de Derecho numeral segundo.

[299] Phishing: Fisching, del inglés pescar, las letras ph son utilizadas por hackers para sustituir la f, como raíz de otra forma anterior de hacking conocida como *phone phreaking*.

[300] El smishing es una variante del phishing pero con el uso de los mensajes cortos o SMS. También es llamado SMS phishing. La técnica smishing consiste del envío de mensajes de texto (SMS) cuya actividad criminal es la de obtener, mediante engaños a los usuarios de telefonía móvil, información privada o suscripciones falsas online y ofertas de trabajo en sitios web, para luego introducir spyware o programas con intenciones maliciosas sin el consentimiento del usuario.

[301] El vishing es una variante del phishing pero con teléfono. Consiste en el envío de un correo electrónico en el cual los delincuentes consiguen detalles de datos bancarios mediante un número telefónico gratuito, en la cual una voz computarizada de aspecto profesional requiere de las víctimas la confirmación de su cuenta bancaria, solicitándoles el número de cuenta, tarjeta, PIN, etc.

acceso que la persona utiliza parta acceder a la red, *logins*[302] *y passwords*[303] de mensajería instantánea, también claves ingresar a su perfiles que activados en la redes sociales o las contraseñas de sus correos electrónicos. Las técnicas del *phisher* han ido variando en el tiempo y no sólo se limitan a ser aplicadas en menajes telefónicos, sino que también en la colocación de post en facebook o twitter, en los cuales se trata de motivar a la víctima que ingrese por los beneficios que ello traerá, siempre y cuando se digite la información personal para posteriormente cometer la acción delictiva.

Esta técnica de captación ilícita de datos personales, se basa en la confianza de las entidades suplantadas, pudiendo tener muchas variantes y métodos para usar, toda vez que a través de *malware*, se puede lograr instalar programas maliciosos, como los ya estudiados (troyanos, gusanos, etc.) en el sistema donde la víctima tiene sus diversas claves de acceso.

Al realizar el envío de correos masivos, que aparentan provenir de instituciones financieras confiables, los datos son proporcionados por la víctima, utilizando para ello el engaño, puesto que dichos correos enmascaran bajo imágenes de instituciones normalmente conocidas, cuyas páginas son emuladas y difícil de detectar comparándolas con las originales o verdaderas, con ello hacer una oferta o invitan al usuario a digitar sus claves para posteriormente acceder a las cuentas de los clientes. Estos correos al ser masivos son enviados a miles de personas, por ello

[302] Login es nombre dado al momento de autentificación al ingresar a un servicio o sistema. De esta manera al momento que se inicia el login, el usuario entra en una sesión, empleando usualmente un nombre de usuario y contraseña. Por ejemplo, cuando debe ingresar a un portal o página de jurisprudencia por la cual se paga, el sistema pide el *login*, entonces está pidiendo el nombre de usuario y contraseña que se eligió cuando el usuario se registró en dicha página de internet. Suele usarse como verbo y conjugarse al españolizarse, *loguearse*, quedando en inglés como la acción de loguearse es *logging in*. Un término más apropiado para loguearse sería "Iniciar sesión" o "Autentificarse".

[303] En informática, la palabra password significa contraseña, clave, key o llave.

se asemejan a una pesca con red, donde la gran cantidad de usuarios que son posibles víctimas, los delincuentes informáticos apuestan a la probabilidad que más de alguno accederá o creerá que la página que se envía es la verdadera, tratando que siempre o casi siempre sea alguna entidad bancaria, evitando con ello la responsabilidad civil. En cuanto a la responsabilidad civil, la inclusión financiera o de crédito, en la mayoría de los casos es condenada a reintegrar o resarcir el daño que sea causado al cliente, puesto que la misma debe probar la negligencia del mismo cliente, y muchas veces para mantener su credibilidad asumen los cost es del fraude, además de ello obligan o promueven a los clientes adquirir seguros contra este tipo de fraudes, evitando con ello asumir los propios daños, traspasando la responsabilidad otro, toda vez que la cifra en este tipo de delitos es muy elevada[304].

Al obtener las claves de ingreso, a los distintos productos de los usuarios, estas mismas claves pueden ser utilizadas tanto para sustraer dinero haciendo transferencias de una cuenta a otra, o inclusive para transar estas claves tanto en el país donde se cometió el delito como en el extranjero, haciendo inclusive más difícil la persecución del delito, puesto que se suma, a la complejidad técnica de encontrar el delincuente que accedió a las claves del usuario, el problema de la internacionalidad, y por ende de la territorialidad del derecho penal, y los principios que todos sabemos que rigen en esta materia[305].

[304] FERNÁNDEZ TERUELO, Javier, *Derecho penal e internet*, Editorial Lex Nova, España, 2011, pág. 38.

[305] En los Estados Unidos de Norteamérica, el senador Patrick Leahy, propuso la Ley Anti-Phishing el 1 de marzo de 2005. Esta ley federal de anti-phishing establecía que aquellos criminales que crearan páginas web falsas o enviaran spam a cuentas de correo electrónico con la intención de estafar a los usuarios, podrían recibir una multa de hasta $250,000 USD y penas de cárcel por un término de hasta cinco años. Además de ello, existen otros Estados de dicho país que abordan el crimen informático, prácticas fraudulentas o engañosas o robo de identidad, que también podrían aplicarse a los delitos de phishing. De esta manera existe por ejemplo el Código Penal de Alabama, el cual en su Sección 13 A-8-114 *Phishing*: (A) Una persona comete el delito de phishing si la persona por medio de una página web de Internet, un mensaje de correo electrónico, o de alguna otra manera utilizando Internet, solicita, solicita o toma cualquier acción para inducir a otra persona

1. Algunos tipos de phisching[306]

a proporcionar información de identificación representando a la persona, directa o implícitamente, es un negocio, sin la autoridad o aprobación del negocio. (B) Cualquier persona que viole esta sección, por convicción, será culpable de un delito mayor de Clase C. Las violaciones múltiples resultantes de una sola acción o acto constituirán una violación a los efectos de esta sección. (C) Las siguientes personas pueden entablar una acción contra una persona que viole esta sección: (1) Una persona que se dedica al negocio de proporcionar servicios de acceso a Internet al público, es propietaria de una página web o posee una marca comercial, y se ve afectada negativamente por una violación de esta sección. (2) Un individuo que es afectado negativamente por una violación de esta sección. D) En cualquier procedimiento penal interpuesto de conformidad con esta sección, se considerará que el delito se comete en cualquier condado en el cual haya ocurrido alguna parte del crimen, sin importar si el acusado estuvo alguna vez presente en ese condado o en el Condado de residencia de la persona que es el sujeto de los documentos de identificación o información de identificación. (E) El Procurador General o el fiscal de distrito pueden presentar una acción civil en el tribunal de circuito para hacer cumplir esta sección y para prohibir otras infracciones de esta sección. El Procurador General o el fiscal de distrito pueden recuperar los daños reales o veinticinco mil dólares ($ 25,000), lo que sea mayor, por cada violación de la subsección (a). (F) En una acción civil bajo el inciso (e), el tribunal puede aumentar la indemnización por daños y perjuicios a un monto igual a no más de tres veces el premio otorgado en el inciso (d) si el tribunal determina que el demandado ha participado en un patrón Y la práctica de violar el inciso (a). (G) El producto de una acción bajo la subsección (e) se utilizará primero para el pago de todos los gastos apropiados, incluyendo los costos judiciales, de los procedimientos para la acción civil con el resto del producto pagaderos primero para la restitución de cualquier víctima, La corte. Cualquier ganancia restante se otorgará igualmente entre el Fondo General del Estado y la oficina del Procurador General, la oficina del fiscal de distrito que presenta la acción, o ambas. (H) Un proveedor de servicios de computación interactivo no será considerado responsable ni encontrado en violación de esta sección para identificar, eliminar o inhabilitar el acceso a una página web u otra ubicación en línea que dicho proveedor razonablemente crea por evidencia clara y convincente de que es Siendo utilizado para participar en una violación de esta sección.

[306] Aspectos a considerar en el *phisching*: Todo malware ataca en forma masiva, sin embargo todos estos programas maliciosos, contienen un defecto, que no es otro que el delincuente informático no tiene el conocimiento total de la persona respecto de la cual se quiere engañar, por lo mismo utilizan una técnica basada en el azar y forma aleatoria, esperando encontrar a la víctima de modo casual. Existen tres aspectos a considerar, para entender cómo opera este fraude. Primero se debe considerar el remitente, puesto que si se recibe algún correo electrónico, de un proveedor que no tiene vínculo alguno con la persona, debería ser un aspecto ya sospechoso. Aunque existe la posibilidad, que se reciban por error correos electrónicos, que en realidad van dirigidos a otra persona, la generalidad de las veces se trata de una estafa, puesto que si el mensaje incluye archivo adjunto o vínculo web, debe asumirse que es malicioso. Por esta razón, la recomendación general, es que nunca se debe acceder algún tipo de archivo adjunto vínculo, sino que por el contrario el usuario debería tomar contacto telefónico o de alguna otra manera para corroborar la información, aumentando con ello la seguridad. Por otro lado, se debe considerar la cuenta de correo electrónico, porque la mayoría las personas sólo una cuenta, para todas sus transacciones, sin embargo crearon

Como se ha venido señalando, los atacantes se hacen pasar por entidades conocidas, tanto que podría ser una multiplicidad de ellas, como la red social, entidades financieras, cualquier sitio de ventas en línea, con el fin de sustraer la información que es confidencial y tener acceso a ella, sin embargo existen distintas modalidades de este fraude informático, siendo las más conocidas son más utilizadas las siguientes.

1.1. Phishing Tradicional

En esta modalidad, el fraude es más simple, desde el punto de vista técnico, porqué está vinculado a una simple copia de un sitio, que es familiar para la víctima, en el cual se reemplaza la dirección del mismo, dirección a la cual llegan los datos ingresados por el usuario, momento en el cual las claves de ingresadas, pueden estar en algún archivo de texto o ser enviadas algún correo electrónico. La diferencia con los otros, que está vinculado solamente a un sitio web, donde en el cual se instalan los contenidos de la página emulada.

---

en dirección de correo electrónicos separada aumenta la seguridad, sin tener que publicar la en la red. En este caso si el mensaje no es personal es decir que no está dirigido con los nombres propios o corrientes, puede tratarse de un engaño. Aunque este método, no entrego una máxima seguridad, si se tiene sólo una cuenta con la institución que está enviando el correo, pero el mensaje no es personal se puede dudar de su procedencia. Además, es necesario *verificar el encabezado de los mensajes*, puesto que si el correo no va dirigido a alguna persona específica, o a nadie os envió con copia oculta, se trata de un fraude. Aunque parezca dirigido a personas donde el usuario ha intervenido como cliente alguna vez, desde ya se debe desconfiar de la falta de personalidad del mismo encabezado.

1.2. Phishing redirector

En este caso, estilizado a través de correos electrónicos masivos, que se basan en que a pesar que son pocos los usuarios comprometidos o las víctimas afectadas, igualmente se comete el fraude. Esta modalidad requiere que el delincuente informático, realice un mayor esfuerzo técnico para crear las páginas falsas, en este caso se crean dos o más sitios o dominios para realizar el fraude[307].

1.3. Spear phishing

Esta forma de ataque, tiene la característica que va dirigido a un cierto número de personas, se utiliza la ingeniería social y un estudio previo complejo de las víctimas, es decir son métodos personificados y a la vez con un alto porcentaje resultado delictivo. En este caso no buscan que sea algo masivo, sino que apunta a determinados perfiles de usuarios, donde se envían correos electrónicos con todos los datos para que la víctima crea, que es un correo verdadero, es van creando todo un escenario de direcciones conocidas para generar en la persona la confianza que se necesita para ingresar los datos necesarios. En este caso el delincuente cibernético, busca el eslabón más débil dentro de la institución que quiere defraudar, buscando

[307] Se pueden destacar tres técnicas, que corresponden al uso de acortadores en las URLs, la inyección de Iframes y la explotación de técnicas ligadas a los marcos en el código HTML. Si bien son conceptos distintos, todos tienen en común que utilizan una redirección para reflejar un sitio almacenado en determinado servidor desde otro servidor. Este será visible sólo bajo un estudio del código fuente. De esta manera, los delincuentes intentan alargar el tiempo que le toma a los equipos de seguridad detectar y eliminar el contenido de los sitios fraudulentos. [en línea], <https://www.welivesecurity.com>.

siempre personas que no estén vinculadas a la informática, para así lograr su cometido.

1.4. Smishing SMS

Mediante el smishing SMS, se utilizan el servicio relacionado con el canal digital, como son los teléfonos celulares. Mediante ellos los usuarios de telefonía móvil recibe mensajes donde se falsifica los sitios y vínculos de portales para sustraer información personal del usuario, comúnmente entregando algún tipo de código o número especial para validar algún premio. Lo que se busca con ello es la ganancia económica, que puede revestir múltiples formas de estafa. Hoy en día también se utiliza, las aplicaciones como son Telegram o WhatsApp, aprovechando que en estas nuevas aplicaciones de comunicación, no es necesario algún pago para enviar el mensaje respectivo, sólo es necesario estar conectado a Internet.

1.5. Vishing

Esta es una técnica reciente que está basada en la telefonía que utiliza el protocolo IP, en la cual se envía mensajes de correo imitando el nombre marca alguna intrusión bancaria o de pago, le indican a la persona que marque un número determinado de teléfono, respondiéndole un sistema automatizado donde contestan solicitando información personal. Estos falsos centros de detención telefónica, en

ocasiones están vinculados a otro, de tal forma que se complementan para dar mayor veracidad a la llamada respectiva confines de engaño, teniendo mayor efectividad.

J) Pharming[308] (granja de servidores o DNS)

El pharming es una modalidad en la cual el delincuente informático desvía el tráfico de internet de un sitio web hacia otro con apariencia semejante[309]. Esta modalidad se considera una variante del phishing, en la cual se manipula las direcciones DNS[310], que utiliza el usuario. Esto se realiza, modificando un archivo

[308] La palabra pharming, deriva del término *farm* en español significa granja y está relacionado con el término phishing. En el diccionario de inglés el término pharming, lo encontraremos definido *como la producción de fármacos desde plantas y animales genéticamente alterados*. En una conferencia organizada por el Antiphishing Working Group, Phillip HALLAM-BAKER definió este término como un neologismo de mercadotecnia diseñado para convencer a banqueros y empresarios de comprar nuevos equipos o accesorios de seguridad. RODRÍGUEZ MAGARIÑOS, Faustino, *Nuevos delitos informáticos: phising, pharming, hacking y cracking.* Sólo disponible en: <httpweb.icam.es/Faustino>.

[309] SAP de Madrid de N° 12, de 25. I. 2016, (Ponente: Juan Antonio TORO PEÑA). Dicha sentencia no habla del pharming, y su modalidad. SAP de Zaragoza, Sección 6ª, Nº 358 de 02. XI. 2010, (Ponente: Rubén BLASCO OBEDE), Dicha sentencia se refiere al *pharming*, e indica que "se infectan ordenadores indiscriminadamente, de modo que cuando el usurario teclea en la barra de direcciones del navegador, la dirección de su banco, automáticamente el navegador lo conecta con una página web falsa, copia de la entidad bancaria, en ella el usuario intentar realizar sus operaciones introduciendo sus claves sin éxito, recibiendo mensajes de error, error en la conexión, etc...los autores de esta modalidad consiguen así sus claves y contraseñas".

[310] Corresponden a las siglas en inglés: Domain Name System, que significa Sistema de nombres de dominio. En la URL, en esta dirección podemos distinguir los niveles, como sería por ejemplo, *.es* como nivel 1 o de nivel superior, dominio territorial. *.ua* como nivel 2 y *www.dlsi* como nombre de máquina o host. En cuando a los nombres de dominio y las direcciones IP, existe una correspondencia, realizándose la misma puesto que los nombres de dominio se transforman en direcciones IP mediante el sistema llamado DNS, o Sistema de Nombres de Dominio en español. El DNS es una base de datos distribuida entre diferentes ordenadores, los servidores de DNS, que se comunican entre sí, y cada servidor DNS posee una tabla con la correspondencia entre los nombres de dominio y las direcciones IP, y cuando un servidor no dispone de una correspondencia concreta, sabe a qué servidor le tiene que preguntar para obtener la respuesta, la correspondencia entre

llamado Hosts, que puede encontrarse en cualquier ordenador que funcione bajo Windows, y que además utilice internet explores, de esta manera el usuario digital su navegador la dirección de la página a la que quiere acceder, y es reenviado a otra creada por el defraudador que tiene el mismo aspecto que la original, ingresando los datos necesarios sin que se percate, que dicha página no es la verdadera. Lo más reciente en esta modalidad, se trata que para no ser descubierto, se envía un enlace en el correo electrónico remitido, por la supuesta entidad financiera en el cual va un archivo adjunto HTML[311] para que el destinatario lo descargue, así ocultando su verdadera URL. Así las cosas, una vez que la víctima ha picado, descarga y abre el archivo que contiene un formulario que recoge los datos, el delincuente ingresa al sistema informático de la entidad bancaria, pudiendo disponer de la cuenta.

Esta técnica tiene su fundamento en los ordenadores que se encuentren conectados a Internet y tienen una dirección IP única. Las URLs, sólo direcciones que se utilizan para localizar los recursos en Internet, esta misma se compone de varias partes, (protocolo de acceso o de comunicación, el nombre de dominio, que puede contener en su dominio, la ruta al documento y el documento)[312]. Ahora bien

---

nombre de dominio y dirección IP. Los nombres de dominio son más fáciles de recordar, al contrario de la IP, siendo además fiable. En cuanto a la dirección IP puede cambiar con el tiempo por diversas razones sin que tenga que cambiar el nombre de dominio. Extracto de curso realizado en: [Actívate, Google España 2016], <http://google.es/activate>.

[311] Corresponde las siglas en inglés: Hyper Text Mark-up Language, o Lenguaje de Marcas de Hipertexto. Lenguaje desarrollado que sirve para modelar texto y agregarle funciones especiales, como por ejemplo hipervínculos, siendo la base para la creación de páginas web tradicionales.

[312] El nombre de dominio puede identificar a toda una red o a un ordenador o dispositivo de red en particular. Como existe una correspondencia entre los nombres de dominios y las direcciones IP, en una URL también se puede escribir una dirección IP en vez del nombre de dominio. Un nombre de dominio puede ser el nombre de una empresa, el nombre de una institución, el nombre de una organización, el nombre de una persona o cualquier cosa que uno quiera. Estos nombres de dominio se organizan en diferentes niveles. Dominios de *primer nivel* se organizan en genéricos y territoriales. Los *genéricos* son dominios de propósito general y eran inicialmente los que acababan en .com, .edu, .gob, .mil, .net y .org, pero posteriormente se han añadido otros como .biz, .mobi y .xxx. Ahora bien, el registro de nombres de dominio bajo .com, .org y .net no está sometido a

el dominio es un hombre único que normalmente se emplea para identificar un sitio web en internet, hoy en día se ha introducido el nombre de dominio internacionalizado, por ello es posible utilizar nombres de dominio con caracteres en otros idiomas.

De esta manera, aunque se pueda identificar un ordenador por su nombre de dominio, en realidad internamente en internet identifican los ordenadores por medio de la dirección IP, es decir cualquier dispositivo que se conecta a Internet, ya sea un ordenador, una tableta, un teléfono móvil tiene asignada una dirección IP. La nombre de dominio van asociados a la dirección IP, algo así como un número telefónico y la dirección de una casa. Cuando se utiliza el pharming, se ataca, ya sea directamente a un ordenador específico o directamente a los servidores DNS, donde varios usuarios se verían afectados.

K) Mulas o muleros[313] *(money –mules, phishing-mules o pharming-mules)*

Esta conducta se refiere a la cooperación que existe con posterioridad a la consumación de la defraudación patrimonial. Estas personas se van haciendo más

ningún tipo de comprobación previa, se asignan siguiendo el principio de "primero en llegar primero servido". Los *territoriales* son los que identifican el país, como *.es para España, .fr para Francia o .de para Alemania.* Dicho registro de nombres de dominio territoriales está sometido a las normas de cada país, así por ejemplo, en España lo gestiona la organización red.es. Los dominios de nivel 2 son los que normalmente se registran al solicitar un domino, como por ejemplo idesweb.es En algunos países existe un tercer nivel de organización. Por ejemplo, en España existen los dominios controlados .com.es, .nom.es, .org.es, .gob.es y .edu.es que permiten que existan dominios como datos.gob.es o mecd.gob.es. Extracto de curso realizado en: [Actívate, Google España 2016], <http://google.es/activate>.

[313] (argot o en la jerga policial, referente al tráfico de drogas)

comunes en este tipo de delitos. Mula, se referir a la persona que facilita su cuenta bancaria, para recibir dinero o para recibir mercancías que han sido obtenidas de forma ilegal. La mula, transfiere el dinero que ha recibido y se queda con un porcentaje.

El defraudador principal, el *phisher* tiene que contar con alguna cuenta que le pueda servir de destino de lo sustraído. Dicha cuenta corriente, debe tener algunas características para le pueda servir con fines ilícitos. Primero no pueda provocar sospecha o alarma en la entidad financiera, por ello casi siempre son cuentas en el extranjero, y como segundo requisito ilícito, es que la cuenta debe pertenecer a un tercero, el llamado *mulero*. Estas personas les ofrecen una estupenda oferta para trabajar cómodamente desde casa con su ordenador, lo que se denomina *Scam*[314]. Con esta denominación operan empresas ficticias que ofrecen trabajar cómodamente desde casa y cobrando unos beneficios muy altos, para esto las empresas ofrecen la posibilidad de ganar dinero fácil, o arguyen la imposibilidad de poder abrir una cuenta a no ser un sujeto residente del país al cual se está realizando el fraude. En estos casos, la víctima es contactada y se le solicita rellenar algún tipo de formulario donde ingresan sus datos de cuenta bancaria ya su vez se indica la cuenta de la víctima phisching. Una vez que los estafadores ingresan el dinero de la otra víctima a la cuenta del *mulero,* le indican que se quede con un porcentaje de dicha transferencia o depósito, el dinero restante es enviado casi siempre en dinero efectivo por algún otro medio postal, como por ejemplo Western Union o MoneyGram, toda vez que dichas empresas para que las personas puedan recibir dicho dinero se les entregan códigos alfa numéricos, que a su vez tienen la dificultad del rastreo de dicho dinero. Muchas veces los muleros no tienen conocimiento de lo

[314] Scam en ingles estafa, que sería tipo de fraude informático, híbrido entre el phishing y las pirámides de valor. El Scam es la captación de personas por medio de correos electrónicos, chats, etcétera.

que se está realizando, entendiendo que son algún tipo de comisionista financiero, sin embargo estarían ya involucrados en algún caso de estafa informática.

Es dable señalar que desde el punto de vista penal se hace dificultosa la responsabilidad de estas personas, la jurisprudencia no ha sido coincidente, puesto que hay que distinguir distintas situaciones, como es el grado de conocimiento que tuvo en la conducta delictiva. Es decir, dicha conducta puede en muchos casos subsumirse, en otros tipos penales como son la estafa tradicional, blanqueo de capitales e incluso la receptación[315] [316].

[315] STS, Sala 2ª de lo Penal, Nº 834, de 25. X. 2012, (Ponente: Sr. Manuel MARCHENA GÓMEZ). En lo medular dicha sentencia, nos refiere acerca de las distintas posiciones acerca de la cuestión debatida acerca de la figura del mulero. "Se reclama contra la sentencia que condenó a la acusada como autora de un delito de blanqueo de capitales cometido por imprudencia. Estamos en presencia de una actuación fraudulenta que toma como punto de partida el envío masivo de mensajes de correo electrónico desde diversos sitios en la web, que tiene como destinatarios a usuarios de la banca informática banca on-line, a quienes se les redirecciona a una página web que es una réplica casi perfecta del original y en la que se les requiere, normalmente con el aviso amenazante de perder el depósito y la disponibilidad de las tarjetas de crédito, a que entreguen sus claves personales de acceso con el fin de verificar su operatividad. De forma gráfica se dice que el autor " pesca los datos protegidos" -de ahí la denominación phishing-, que permiten el libre acceso a las cuentas del particulares y, a partir de ahí, el desapoderamiento. No hay razón que justifique que la acusada sólo deba responder de la parte del lucro propio. Es cierto que en los delitos de receptación, la responsabilidad civil se señala en función del lucro experimentado por el receptador. Pero en este caso, no estamos ante una receptación, en la cual la intervención del reo es independiente del alcance del tipo principal. Aquí la acusada interviene en el blanqueo de todo el dinero que es sustraído a la víctima. Por ello debe responder civilmente del total sustraído.

[316] SAP de León, Sección 3ª, Nº 524, de 15. X. 2014, (Ponente: Miguel Ángel AMEZ MARTÍNEZ). En lo medular dicha sentencia indica al tener que decir si corresponde o no, el tipo penal de estafa informática, en directa relación con la apropiación indebida, razonado de la siguiente manera en alguno de sus considerandos: "se afirmaba en tal sentido que siempre que no exista acuerdo expreso o tácito con los scammers, (que son los sujetos que transfieren el dinero inconsentidamente apropiado) y *que los muleros ignoren que están inmersos en un delito de estafa informática, es decir, que no sepan que el dinero proviene de la sustracción a un tercero*, ha de señalarse que no tienen responsabilidad penal por ese delito de estafa informática y terminaba absolviendo en el caso enjuiciado a la acusada por considerar que no estaba probado que hubiera participado en la manipulación informática, base de dicha defraudación, ni que conociera que la transferencia hecha a su cuenta se hubiera realizado de forma fraudulenta, elemento preciso en tanto que estamos hablando de conductas eminentemente dolosas". "En definitiva, y por las razones que dejamos expresadas, consideramos que no se ha probado que el acusado ahora apelante *prestara su colaboración eficiente, de modo consciente y deliberado en la estafa cometida, ni que se hubiera*

L) Blanqueo de capitales

Es dable hacer una breve alusión al tema, toda vez que este es uno de los delitos que más se ha incrementado con la llamada revolución informática, internacionalmente esta modalidad delictiva es conocida como *money laundering.* En este caso se realizan transferencias de dinero, de fondos y capitales, con destinos distintos es decir a varias cuentas bancarias ubicadas en distintos países o llamados paraísos fiscales, y con ello dificultan el rastreo del origen de la transacción. Más recientemente, el blanqueo de capitales ha sido utilizado para obtener responsabilidad penal de los *muleros bancarios*[317].

---

representado el carácter fraudulento de la actividad que realizó como, tampoco, que la hubiera llevado a cabo, tal como se afirma en la sentencia recurrida, con intención de enriquecerse ilícitamente, todo lo cual excluye en su conducta el elemento de la culpabilidad y hace que deba ser absuelto del delito de estafa informática por el que viene condenado y, también del de blanqueo de capitales por imprudencia grave del que había sido acusado alternativamente una vez que, como hemos dejado reiterado, desconocía el origen ilícito del dinero que recibió en su cuenta y que, tras reintegrarlo y quedarse con la comisión pactada, reenvió a un tal Norberto, en Moscú.

[317] SAP de Cáceres, Sección 2ª, Nº 344, de 30. VII. 2015, (Ponente: Valentín, PÉREZ APARICIO). El fallo condena al acusado como autor penalmente responsable conforme al art. 28 del CP de un delito de blanqueo de capitales en su modalidad de imprudencia grave. La sentencia en lo medular indica que: El acusado Romualdo, de nacionalidad venezolana, sin que conste su residencia irregular en España, mayor de edad y cuyos antecedentes penales no constan, mientras buscaba trabajo a través de internet, contactó con la empresa *Lombardalia Inc*, quien le propuso un trabajo de agente financiero para lo cual debía abrir una cuenta bancaria en la que recibir cantidades que la entidad le transferiría y a cambio realizar envíos siguiendo las instrucciones de aquella, todo ello a cambio de una comisión calculada sobre el 6,9% de la cantidad ingresada. El acusado suscribió dicho contrato y facilitó los datos de la cuenta bancaria número NUM000 de la entidad bancaria C.E. Terrasa, que tenía abierta en la sucursal de la calle Santa Mª de la Cabeza número 68 de Madrid, remitiendo esta información a *Lombardalia Inc*, sin preocuparse en conocer la trascendencia o significación económica o jurídica del encargo a realizar, ni la legalidad en la procedencia de tales cantidades de dinero, guiada del propósito de obtener recursos económicos adicionales de forma sencilla. Una vez recibida tal transferencia el acusado inmediatamente recibió una serie de mensajes de texto en el que se le indicaban instrucciones sobre el destinatario y la forma de efectuar los envíos. La entidad *Lombardalia Inc*, está domiciliada fuera del territorio

Se han creado empresas con fachadas falsas, que intentan acercar a sus filas personas, llamados teltrabajadores, los cuales aceptan estas ofertas de trabajo puesto que ofrecen grandes ganancias y además pueden trabajar desde su casa, sin embargo incurren en un fraude[318]. Lo que está ocurriendo hoy en día es que cuando las policía, trata de averiguar el titular de la cuenta, se encuentran con el *mulero*, y con ello se dificulta muchísimo descubrir al verdadero *phisher*. Estas personas hacen que el delito el defraudador pueda llevar acabo el delito, siendo imprescindibles para ellos, toda vez que sin su cooperación quedan expuestos a ser descubiertos.

M) Distributed dos (denegación de servicios distribuida)

nacional desconociéndose la identidad real de sus representantes, siendo que las cantidades recibidas en la cuenta bancaria del acusado procedían de estafas realizadas mediante manipulaciones informáticas denominadas phishing, con virus troyanos o la técnica pharming, contra cuentas corrientes operadas a través de la banca on-line, tras lo cual conseguían su remisión a otras cuentas bancarias de personas con las que previamente contactaban, en este caso mediante un contrato laboral.

[318] Conferencia Octopus Interface. La Unión Europea, Francia y otros países han adoptado las directrices sobre cooperación policial en la investigación de la ciberdelincuencia, cooperación contra la ciberdelincuencia, para los países también deben asegurarse de que los diferentes tipos de ciberdelincuencia constituyan delitos subyacentes para el lavado de dinero. Más de 100 países de todo el mundo utilizan la convención como una guía para su legislación. De esta forma en la conferencia antes indicada, se ha tratado de la cooperación en términos de tipologías de ingresos que generan delincuencia, flujos de dinero y lavado de dinero; estrategias, técnicas y herramientas para buscar, seguir, incautar y confiscar fondos, provenientes de dichos ilícitos. La conferencia aborda el tema de la necesidad de establecer la confianza entre los diferentes actores públicos y privados involucrados en medidas contra el delito cibernético y contra el lavado de dinero y el terrorismo y para tender puentes entre las comunidades anti-ciberdelincuencia y de lucha contra el lavado de dinero. Se refuerzan los roles que toman, los diferentes grupo de acción como son; el Grupo de Acción Financiera, Moneyval, el Grupo de Trabajo Anti-Phishing, el Plan de Acción de Londres, la coalición Advance Fee Fraud o el Hi-tech Crime Forum en Irlanda. [disponible], <www.coe.int/cybercrime>.

Distributed denial of service o denegación de servicios distribuida, o DDos (siglas en ingles), este de conforma por un ataque a un sistema de ordenadores o red, que tiene como efecto que el servicio sea inaccesible para los usuarios afectados. La situación anterior podemos graficarla con un ejemplo en el cual si nos imaginamos un funcionario que atiende público, el cual es muy eficiente y capacitado para atender a varias personas a la vez sin que repercuta en su estado emocional ni físico, toda vez que es una carga normal de trabajo, sin embargo si la situación cambia y comienzan a llegar cientos de personas a solicitarle, distintas tareas al funcionario, como podría pensarse, y como cualquier humano normal, no puede atender a todos y comenzaría desempeñarse más lento de lo normal, por el cansancio y porque debe resolver solicitudes diversas al mismo momento, y si se suma que viene muchas más personas, probablemente comience a equivocarse y después ya no se presentará a trabajar y no atenderá más, negándose a despachar información.

Con el servidor sucede algo similar, puesto que cuando hay demasiadas solicitudes se queda sin recursos, y deja de funcionar, pudiendo apagarse directamente o que sólo deje de responder conexiones. Vale señalar que el servidor no volverá a la normalidad, hasta que el ataque se detenga, e intentar volver a dar inicio a todo lo que haya dejado de funcionar. Este es el concepto básico del DDoS, aunque se puede modificar para que sea más efectivo.

Los delincuentes informáticos cobran una suerte de peaje, para liberar el sistema. Este se logra puesto que se instala un *malware*, en cada uno de los ordenadores, el programa aceptará los comandos que le envía el atacante, y con la debida coordinación, permite ordenar a la red que comience el ataque, y sólo el usuario percibe una merma o latitud en el sistema. Por otro lado en dable considera que cuando se habla de 100 sitios, no significa que sean la misma cantidad de personas, que estén organizadas para esto, lo normal es que estén bajo el mismo control una única persona o sólo una organización delictiva. Estos ataques provocan

perdida de productiva, con la saturación de los puertos con múltiples flujos de información, como por ejemplo cuando inundan la red con correos basura. En definitiva los atacantes construyen redes de computadoras infectadas, *botnets*, mediante la difusión de software malicioso a través de correos electrónicos, sitios web y medios sociales.

Una vez infectadas, estas máquinas pueden ser controladas remotamente, sin el conocimiento de sus propietarios, y utilizadas como un ejército para lanzar un ataque contra cualquier objetivo, por ello una vez que se controla la máquina, ésta da aviso al atacante. Aunque el éxito sea sólo en un porcentaje pequeño, cuando existen decenas de millones de máquinas conectadas las posibilidades de poder reunir recursos es ilimitada[319].

N) Cartas nigerianas

Las llamadas *cartas nigerianas,* consistente en una inesperada comunicación mediante cartas sobre todo a través de correos electrónicos el remitente, promete negocio muy rentable. Toman este nombre porque en un principios remitente se hacían pasar por ciudadanos de Nigeria o de otros países africanos. Dicho mensajes entregan la expectativa de poder obtener dinero mediante sencillas gestiones, utilizando este ardid para que los estafadores logren en las potenciales víctimas descuidos, y así que las mismas olviden los más elementales resguardos. Este tipo de estafa puede ser considerado como tradicional sin embargo hago alusión al mismo

[319] VELASCO NÚÑEZ, Eloy (dir.), CONSEJO GENERAL DEL PODER JUDICIAL, *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?,* Cuadernos de Derecho Judicial, 2006, pág. 74.

por que el tipo de fraude se ha adaptado a los nuevos tiempos, conociéndose hoy en día dicha modalidad a nivel internacional como *Scam 419,* en referencia a la sección del código penal de Nigeria en la que se tipifica. España, si bien es cierto no existe un número mayor de víctimas, tradicionalmente se utiliza el prestigio de las loterías del país, para enviar las cartas, dando el lugar de origen de España, utilizándose antiguamente el correo postal, hoy en día existen distintas modalidades de la misma, donde se explican versiones de pariente cercano fallecidos para tener herencias, aprovechándose de una mezcla de avaricia, ingenuidad y desconocimiento de las víctimas.

El fraude se lleva acabo convenciendo la víctima para que realice la transferencia de dinero, enviando documentos aparentemente oficiales y movimientos bancarios falsos[320].

Ñ) Técnica del salami (cortado en rodajas, salami)

Consiste en la sustracción o desvío de pequeñas cantidades de activos de un número importante de cuentas a la del sujeto activo. Toma su nombre, toda vez que la técnica utilizada o patrón comisivo, es través del minucioso o porcionado en rodajas, hace alusión a las láminas muy delgadas al cortar un embutido, en este caso son múltiples y pequeñas porciones de dinero que se traspasan a la cuenta del delincuente, todo lo cual se aprovecha del redondeo de intereses[321]. Por ejemplo,

[320] CONSEJO GENERAL DEL PODER JUDICIAL, (como en nota 133), pág, 141.

[321] HERRERA MORENO, Mirian, *El fraude informático en el derecho penal español*, *Revista de* Actualidad Penal, número 39, Sevilla, 2001, pág. 938.

unas líneas adicionales de código introducidas en un programa de cálculo de intereses bancarios para redondeo de intereses, han servido para acreditar a las cuentas particulares de defraudadores las pequeñas diferencias de dinero fruto de esos redondeos. Este tipo de fraude ha sido utilizado con éxito por programadores para aumentar su sueldo, como agentes de cambio y por empleado de banco, siendo estos fraudes difíciles de detectar por las pequeñas sumas llegan número de operaciones que se realizan[322]. Para realizar esta técnica para realizar esta técnica, se utiliza un programa denominado *superzap*[323], con el cual se alegró un programador o técnico que tenga acceso a las cuentas corrientes puede utilizarlo en forma fraudulenta, pudiendo cambiar el saldo de la cuenta corriente del fichero, por ello la importancia de la restricción en el acceso a los programadores es de vital importancia.

[322] SNEYERS, Alfredo, el fraude y otros delitos informáticos, Editorial tecnologías de gerencia producción S. A., Madrid, 1990, pág. 112.

[323] Superzap: es un programa software de IBM, que permite el cambio programa del sistema operativo. A nivel de código de máquina o código de objeto, tales cambios son rápidos y generalmente no registrados. Sin embargo, superzap para el mantenimiento más alto de niveles de producción, y presentan programa de seguridad de control. IBM indica que el programa de modificación de sistema, se recomienda usarlo, toda vez que ofrece control sobre cuántos cambios hechos. El control de tales herramientas como súperzap por un grupo de control de cambio, afirma las propiedades de contabilidad y auditabilidades sistema total. Si se utiliza en forma ilícita Este programa puede ser usada para cambiar parte de datos en ficheros o programas. FISCHER, Royal P, *Seguridad en los sistemas informáticos*, Editorial Díaz Santos, S. A., Madrid, 1988, pág. 10.

CAPÍTULO IV

Estafa informática en el Derecho comparado. Convenio de Budapest, Alemania, Italia y en especial referencias al ordenamiento jurídico de Chile

I. Antecedentes

Cuando hablamos de estafa, siempre nos referíamos al delito en contra de las personas, donde el engañado era un hombre, sin embargo hoy en día existen sistemas de procesamiento de datos donde existe patrimonio de un modo distinto o independiente, como en el caso de los cajero automático, de esta manera el engaño es hacia un sistema. Como se habló anteriormente, la mayoría de los ordenamientos hablan del tipo penal de estafa básico, y hoy en día contemplan el tipo especial de estafa informática, como una segunda variante al básico. Hay autores que indican que resulta aceptable como principio la equiparación entre la estafa contra hombres y contra sistema de procesamiento de datos, sin que para ello sea necesario seguir avanzando en teorías filosóficas y cibernética relativas a la existencia de autoconciencia máquinas complejas[324].

[324] VOGEL TÜBINGEN, JOACHIM, *Fraude y corrupción en el derecho penal económico europeo, Eurodelitos de corrupción y fraude*. (Coordinadores), Luis ARROYO ZAPATERO/Adán NIETO MARTÍN, Ediciones de la Universidad de Castilla- La mancha, Cuenca, 2006, pág. 41. El autor además agrega, que resulta incluso necesario mantener que la estafa informática no sólo debe equipararse la estafa desde el punto de vista de la técnica legislativa sino que también en su esencia debe entenderse en un modo similar, sólo lo que resulta engañoso en relación un hombre, puede considerarse como un comportamiento punible a los efectos de la estafa informática.

La directriz general para el delito de estafa informática lo entrega el artículo 8[325], de la Convención de Budapest. En dicho convenio, se establecen distintos objetivos, a saber armonizar el derecho penal material; establecer medidas procesales o cautelares acomodadas al medio digital, que facilite la extensión, la investigación en la obtención de pruebas de infracciones cometidas contra o mediante un sistema informático o cuyas fuentes de prueba se encuentren en soporte electrónico; instaurar un régimen expedito y poderoso de cooperación internacional, (extradición)[326].

Según indica ROVIRA DEL CANTO, existen tres métodos legislativos usados por el legislador al momento de establecer el ilícito informático, así divide en tres las categorías. La *complementación*, donde se amplía con una categoría nueva de objetos sobre los cuales puede recaer la acción del sujeto activo, y con respecto a los cuales pueden cometerse los actos ilícitos, pero tiene problema que no siempre reconoce la naturaleza del delito informático y puede surgir lagunas legales cuando otro elemento de la figura tradicional no pueden darse o cumplirse en un ámbito informático. Indica también que existe la *extensión o evolutivo*, donde se elaboró una figura especial, paralela pero con base a las ya existentes, tomando en consideración los bienes jurídicos nuevos protegidos como el sistema informático, los datos y software, teniendo el inconveniente que también pueden existir lagunas legales, cuando se protege un interés especial y no tradicional. Por último, nos indica la modalidad *especial*, donde existe una norma especial, donde se criminaliza por

[325] La norma señala: Fraude informático. Las partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. La introducción, alteración, borrado o supresión de datos informáticos; b. Cualquier interferencia del funcionamiento de un sistema informático. Con intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona. Convenio 185, Del *Consejo de Europa, sobre la Ciberdelincuencia, Budapest, 23. XI. 2001.*

[326] BALMACEDA HOYOS, Gustavo, *El delito de estafa…o*p. cit. pág. 115.

medio de una disposición penal, un compendio de normas de la misma clase, donde existe una interrelación entre ellas, según la autora indica que es la manera más eficaz de criminalizar el delito informático[327].

De acuerdo a lo anterior en el Derecho europeo continental, los sistemas legislativos sobre la estafa informática, se dividen entre aquellos países que efectúan una descripción enumerativa de la norma, con un catálogo de conductas consideradas que cumplen las modalidades de este tipo de delitos, como en el caso de Alemania y por otro lado existen aquellos que utilizan descripciones generales, como es el caso de España, Italia y Chile pero en este último con distintas dificultades.

A) La estafa o fraude informático conforme el Convenio de Budapest

En cuanto los delitos informáticos, la principal herramienta internacional que existe en el marco del esfuerzo europeo para regular la materia, es el convenio sobre la ciberdelincuencia de 21 de noviembre de 2001, documento firmado por los representantes de cada país miembro del Consejo de Europa, y que a pesar que es un convenio que tiene que ser ratificado posteriormente por los países pertenecientes al Consejo, casi todos los países ya lo han refrendado, puesto que su eficacia depende de los órganos internos de cada país firmante. Este convenio, dio pie para la definición de varios delitos informáticos, y algunos conceptos técnicos y elementos relacionados con los mismos, como por ejemplo sistemas informáticos, datos informáticos, o proveedor de servicios. Dicho convenio agrupó los delitos

[327] ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Editorial Comares, Granada, 2002, pág. 342.

informáticos en cuatro grupos: delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; acceso ilícito a sistemas informáticos; interceptación ilícita de datos informáticos; interferencia en el sistema mediante la introducción, transmisión provocación de daños, borrado, alteración o supresión de estos; abuso de dispositivos que faciliten la Comisión de delitos; falsificación informática que provocan alteración, borrado o supresión de datos informáticos que ocasionen datos no auténticos; fraudes informáticos.

En cuanto el Derecho penal se trata, dentro de las medidas que deben ser adoptadas, como indica en el capítulo II, sección I, título 2[328] [329], se encuentra el texto expreso del artículo octavo, sin embargo vale indicar que la redacción típica, no tiene una redacción precisa, por el contrario lo que se expresa son acciones o conductas y valiosas con modalidades de comisión sin tipificación rigurosa. En cuanto a la materia se trata, se critica igualmente porque no entrega una definición de estafa, ni tampoco alude al uso fraudulento de tarjetas de crédito o débito[330].

[328] Expresamente existe el artículo octavo, el cual indica lo siguiente: "las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para proveer como infracción penal, conforme a su derecho interno, la producción de perjuicio patrimonial a otro de forma dolosa y sin autorización, a través de: a. La introducción, alteración, borrado o supresión de datos informáticos, b. Cualquier forma atentado el funcionamiento sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.

[329] VELASCO SAN MARTÍN, Cristos señala, "[…] Este artículo pretende sancionar alguno de los delitos más comunes en el ciberespacio, como son el fraude tarjeta de crédito y el fraude cometido en los medios de pago en sitios de subasta Internet. Otros fraudes comunes bajo este rubro sólo llamados *online acction fruad,* que se refiere a cualquier actividad fraudulenta que involucra el uso de plataformas electrónica para realizar subasta en Internet; y el *avanced fee fraud,* que son aquellos delitos en los que los infractores buscan convencer a sus víctimas para que desembolsos en pequeñas cantidades de dinero con la esperanza recibir posteriormente mayores cantidades de dinero". VELASCO SAN MARTÍN, Cristos, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet,* Editorial Tirant Lo Blanch, Valencia, 2012, pág, 63.

[330] De esta manera lo indica GARCÍA GARCÍA, Josefina, *El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico*, pub. en "ICADE. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales", UNED, N° 74, mayo-agosto 2008, pág. 291 y nota al pie 8.

Dicha convención al no ser acertada en la definición de estafa informática lo que pide a los estados que se adhieren, es que legislen en cuanto a la provocación dolosa del daño patrimonial a un tercero mediante la introducción, alteración borrado o supresión de datos informáticos sin autorización, dejando abierta la posibilidad de cualquier atentado contra el normal funcionamiento de un sistema informático, con la intención fraudulenta de conseguir beneficio económico ya sea para el delincuente informático o para otra persona un tercero, todo ello sin autorización de la persona con el derecho autorizar. Se ha señalado por la doctrina, que se trata un requerimiento abierto de tipicidad, tomando en consideración la delincuencia informática cambiante, con respecto a las modalidades de defraudación, que día a día van cambiando con las nuevas tecnologías[331]. A pesar de lo señalado, el legislador español partió de la base de esta convención, y eligió modificar los tipos penales tradicionales completándolos de acuerdo a la necesidades actuales, adecuando en el caso en concreto la estafa tradicional, con todas las características del delito informático[332].

[331] Se ha dicho que el Convenio de Budapest al referirse a este tema, ha seguido como ejemplo la doctrina legislación alemana, específicamente en el parágrafo, 263a, del Código Penal Alemán, "[…] Como puede observarse, la convención recoge en esta definición del tipo la propuesta de la doctrina y determinadas legislaciones nacionales, que habían definido el fraude informático como toda defraudación cometida, a través del sistema informático, fundamentalmente por la introducción de datos falsos o manipulaciones del programa. Sin embargo, el alcance del precepto de la convención es mucho más amplio que el que resulta del Código Penal Español". El § 263a del StGB alemán dispone: 1. El que, con la intención de obtener un beneficio patrimonial ilícito para sí o para un tercero, lesión del patrimonio de otro interfiriendo en el resultado de un tratamiento de datos, mediante una estructuración incorrecta el programa, la utilización incorrecta o incompleta de datos, la utilización de datos sin autorización, o la intervención de cualquier otro modo no autorizado en el proceso, será castigado con la pena de privación de libertad de hasta cinco años o con multa. CHOCLÁN MONTALVO, José, *Delincuencia Informática, Problemas de responsabilidad, Infracciones patrimoniales en los procesos de transferencia de datos*, (director) *Morales García*, Oscar, Cuadernos de Derecho Judicial IX-2002, Consejo General del Poder Judicial, Madrid, 2002, pág 247.

[332] Al respecto, vale señalar lo que indica el Convenio sobre la Ciberdelincuencia, en su informe explicativo, en su *título fraude informático:* párrafo 88. Las manipulaciones relacionadas con el fraude informático constituyeron delito si causan a otra persona perjuicio patrimonial directo, pérdida de la posesión de un bien, y si el autor actuó de manera deliberada por obtener de manera

Vale indicar que según señala ROVIRA DEL CANTO, que critica la redacción del Convenio al referirse a la presunta estafa informática, puesto que al tratar de garantizar la integridad de los sistemas informáticos no acierta del todo en la configuración de este ilícito, puesto que en el apartado a) ya referido anteriormente se describe no al tipo penal de defraudación estafa, sino un delito de daños. Refiere el autor "ellos ciertamente sucedería si no se estuviera presente que ambos apartados a) y b), que recogen en sí mismo los medios comisivos, tienen de común lo dispuesto en el párrafo siguiente, y que no viene referido únicamente al apartado b), de efectuar las acciones descritas "con intención fraudulenta o engañosa de procurarse, sin derecho a ello, un beneficio con único para sí mismo o para un tercero"[333][334]. Por ello, se dice que en estricto rigor únicamente constituiría una

ilegítima un beneficio económico para sí mismo para otra persona. El término *perjuicio patrimonial*, que es un concepto amplio, incluye la pérdida de dinero y de cosas tangibles e intangibles que tengan un valor económico. Párrafo 89. El delito debe ser cometido de forma *ilegítima* y el beneficio económico debe obtenerse de manera legítima. Por supuesto, no se pretende incluir en el delito establecido en este artículo aquellas prácticas comerciales comunes legítima, destinadas a obtener un beneficio económico, ya que las mismas se realiza legítimamente. Por ejemplo, son legítimas las actividades llevadas a cabo en virtud de un contrato válido entre las personas afectadas (por ejemplo, inhabilitar un sitio web a realizar las funciones conferidas en los términos del contrato). Párrafo 90. El delito debe ser cometido de manera *deliberada*. El elemento general de la intención deliberada se refiere a la manipulación o la interferencia de lo equipo informático que cause un perjuicio patrimonial a un tercero. El delito requiere también la existencia de una intención deliberada específica de índole fraudulenta dolosa para obtener un beneficio económico o de otro tipo para sí o para otra persona. Así, por ejemplo, no se pretende incluir en el delito establecido por este artículo aquellas prácticas comerciales con respecto a la competencia del mercado, que puedan causar un perjuicio patrimonial a una persona y beneficiará otra, pero que no son llevadas a cabo con una intención fraudulenta dolosa. Por ejemplo, no se pretende establecer como delito el uso de programas que reúnan información para comparar los precios de las compras que se pueden hacer por internet (bots), incluso si no son autorizados por un sitio visitado por el "bot". *Es* El Convenio y su Informe explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión (8 de noviembre de 2001).

[333] ROVIRA DEL CANTO, Enrique, *Revista de derecho y nuevas tecnologías*, *Hacia una expansión doctrinal y táctica del fraude informático*, número 3, Editorial Aranzadi, 2003, pág. 128.

[334] Nos dice ROVIRA DEL CANTO, "[…] No obstante considera que el precepto, aunque no claramente, da una respuesta en pro de las nuevas posturas, sino también en el punto de vista táctico, dirigidas a un tratamiento unitario y armónico respecto del gran elenco de conductas que

estafa informática, el apartado b), es decir, por lo se refiere a *cualquier forma de atentado al funcionamiento de un sistema informático,* estaría aludiendo a un concepto amplio de manipulación informática, y, al referirse *con la intención, fraudulento delictiva, de obtener sin autorización un beneficio con único para sí mismo o para un tercero,* aludiría a la obtención no consentida de una ventaja patrimonial ilícita[335].

Por último, el aludido Convenio, toma una postura respecto al concepto de carácter amplia, la cual se basa en una mirada unitaria para referirse al fraude informático, tomando en consideración siempre el término de manipulaciones informáticas con fines de fraude que lleven envuelto un carácter económico y que afecten el patrimonio de las víctimas.

B) Regulación legal de la estafa informática en Alemania[336]

convergen en la problemática de la utilización ilícita o abusivo de tarjetas magnéticas de crédito o débito bajo una misma figura delictiva defraudatoria, pues a pesar de que pudiera parecer que únicamente obliga a sancionar un actuar directamente sobre los datos es un sistema informático, la amplitud, indeterminación y generalidad de los términos usados, a pesar de favorecerle seguridad jurídica, permite asimismo la subsunción en la figura de supuestos en que se consigue una actuación correcta del sistema pero con cambios accesorios (de identidad del sujeto activo, cantidad destino). Tal sería supuesto, previsto en el precepto al tenor de su redacción, de quien intencionadamente sin derecho a ello, causar una lesión en la propia un tercero mediante cualquier introducción de datos informáticos con la intención fraudulenta de procurarse un beneficio económico ilícito para sí mismo o un tercero. Beneficio con único que, por supuesto no sólo comprenderá una transferencia electrónica de fondos, sino de cualquier activo, bien material o dinero en efectivo". ROVIRA DEL CANTO, Enrique, *Revista de derecho y nuevas tecnologías, Hacia una expansión doctrinal y táctica del fraude informático,* Número 3, Editorial Aranzadi, 2003, pág. 128 y sigs.

[335] Tanto Balmaceda Hoyos, nos explica el mismo problema….op. cit., pág. 96.

[336] La Ley Alemana, también sanciona: el espionaje de datos (párrafo 202 .a); falsificación de datos probatorios (párrafo 269); modificaciones complementarias del resto de las falsedades documentales (párrafo 270, 271, 273, 274 y 348); engaño en el tráfico jurídico mediante sistemas de procesamiento de datos (párrafo 270); modificación de datos (párrafo 303. a) y sabotaje informático (párrafo 303. b).

En Alemania en cuanto la política criminal, existía la necesidad introducir el fraude informático por la progresiva mecanización, automatización y el nacimiento de nuevas formas de delincuencia. Las estadísticas de la ciberdelincuencia en los años de la reforma iban en aumento, existía un número no declarado de delito informático puesto que las empresas afectadas a menudo se abstenían de los cargos criminales por temor a que dicha publicidad resultará perjudicial para su reputación. Al igual que en otros países, las reformas penales en este tipo de delitos, relacionados con los medios informáticos, tuvo su origen en la insuficiencia y deficiencia de lo que ya existía, es decir las normas tradicionales, los tipos básicos o clásicos que no daban el ancho, para combatir la criminalidad informática. Desde ya los años 70, en Alemania se discutía acerca de este tipo de delitos, trayendo como consecuencia que naciera *La segunda ley de lucha contra la criminalidad económica de 1986,* la cual introdujo al Código Penal Alemán, modificaciones relacionadas con los medios informáticos, no limitándose exclusivamente a la modificación de normas ya existentes en dicho código, sino que por lo contrario en algunos casos incluso se crearon figuras o tipos penales totalmente nuevos.

En cuanto al tipo básico que existía, se planteaba que indiscutiblemente engaño, error y disposición del § 263 del Código Penal Alemán, están adaptados sólo a las personas, puesto que se entendía que en el particular, la característica de error tiene que ver con un proceso psicológico que no puede adecuarse a ningún sistema de procesamiento de datos.

De esta manera antes de la introducción § 263a en el Código penal alemán existía una interpretación más amplia del tipo básico, entendiendo que cualquier manipulación del sistema informático, sería confundir al programador, que entendía

que realizaba una operación correcta[337]. Podemos decir entonces que existía un estiramiento excesivo del § 263 del código referido, y además algunos casos no estaban siendo reconocidos por los tribunales, y se utilizaba incluso el § 242 del StGB[338].

Así las cosas, entre las figuras que regula esta ley se incluyó, el engaño en el tráfico jurídico mediante sistemas de procesamiento de datos. Por otro lado, entre los años 2000 y 2006, el derecho penal alemán tuvo variadas modificaciones, tanto en materia Penal como Procesal penal, ello debido a la implementación de la Decisión Marco[339], *sobre la lucha contra el fraude y la falsificación de los medios de pago distinto del efectivo*. Como consecuencia de dicha Decisión Marco, se introdujeron modificaciones a diversas disposiciones penales, § 146 StGB y siguientes en cuanto la falsificación de dinero, ampliando los objetos que pueden ser materia del delito a tarjetas de crédito sin función de garantía, cheques y letras de cambio, los cuales pasan a ser ahora protegidos por medio del § 152 a StGB. Dicho parágrafo, que se refiere a la falsificación de tarjetas de crédito con función de garantía y cheques, fue regulada parcialmente como tipo calificado en el nuevo § 152 b StGB, a fin de evitar posibles lagunas de punibilidad en casos de error. A su vez, la misma ley modificó, el §260 a StGB, en relación a la estafa informática, incorporando diversos actos

[337] CARSTEN ULRICH, Computerbetrug (§ 263a StGB) JurPC: Internet-Zeitschrift für Rechtsinformatik (revista de informática jurídica) JurPC Web-Dok. 189/1999, Abs. 1 – 45. [disponible en] http://www.jurpc.de/aufsatz/.

[338] § 242. Código Penal Alemán: Hurto (1) Quien sustraiga una cosa mueble ajena a otro en la intención de apoderarse antijurídicamente de ella para sí o para un tercero, será castigado con pena privativa de la libertad hasta cinco años o con multa. (2) La tentativa es punible.

[339] Decisión Marco 2001/413 del Consejo, de 28 de mayo de 2001, *Sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.*

preparatorios como punibles e introduciendo el arrepentimiento activo como causa de exclusión de pena[340].

La estafa informática, se encuentra regulada en el §263a del Código Penal Alemán[341], siendo creada dicha norma por el artículo 1 N° 9 de la 2ª Ley de Lucha Contra La Criminalidad Económica[342], ampliada por el artículo 1 N° 10 de la 35ª Ley de modificación del Derecho Penal de fecha 22 de noviembre de 2003. Al respecto por una cuestión político criminal se decía que se debía incluirse un delito paralelo al de estafa, cuyo inicio tiene relación con la abundante utilización de procedimiento de datos manejados por el ámbito bancario, creciendo aún más el peligro para estas entidades de ser atacadas por delincuentes informáticos. Los tipos penales existentes al igual que el resto del mundo, eran insuficientes para encuadrar este tipo de comportamiento, teniendo en consideración que un daño patrimonial no

[340] MEDINA SCHULZ, Gonzalo, *Principales reformas en la legislación penal y procesal, (Alemania),* Revista Penal, Universidad de Friburgo en Brisgovia, 2006. [accesible en], <http://www.uhu.es/revistapenal>.

[341] §263a Estafa informática (1) quien, con el propósito de obtener una ventaja patrimonial antijurídica para sí o para un tercero, perjudica el patrimonio de otro, influyendo en el resultado de un proceso de tratamiento de datos, a través de una errónea configuración del programa, a través del uso de datos incorrectos incompletos, a través del uso no autorizado de datos, o de otra manera a través de una intervención no autorizada en el proceso, se castiga con privación de libertad de hasta cinco años o con multa. (2) Los párrafos dos a siete §263a, son aplicables según corresponda. (3) Quién prepara un delito según el párrafo 1, mientras produce un programa informático cuyo objetivo en la comisión de tal hecho, proporcionado para sí o para un tercero, lo ofrece, guarda, o se lo deja otro, se castiga con privación de libertad de hasta tres años o con multa. (4) E los casos del párrafo 3 son aplicables, según corresponda, los párrafos 2 y 3 del §149.

[342] Gesetz Zur Bekämpfung Der Wirtschaftskrimninalität. (Ley para combatir la delincuencia) la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos: Espionaje de datos (202 a); Estafa informática (263 a); Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(270, 271, 273); Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible; Sabotaje informático (303 b). Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, Inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa; Utilización abusiva de cheques o tarjetas de crédito (266 b).

se originaría por la disposición condicionada del error de una persona, toda vez que ocurrido el perjuicio patrimonial con la intervención ilícita en el sistema de procesamiento de datos, no se produce un engaño en la persona que tiene a cargo su control[343].

El § 263a del Código Penal Alemán tiene su vinculación u origen en el §263 del mismo código[344], el cual se extendió también a los casos de uso no autorizado de datos, esto impulsado por la norma sobre elementos estructurales de la estafa y también por los delitos contra la propiedad, que incluye los tipos de apropiación indebida e infidelidad. Es dable hacer presente, como se dijo anteriormente, que en el §263a del Código Penal Alemán se contiene penalidad de actos preparatorios debido a una decisión en el marco del Consejo de la Unión Europea de fecha 28 de mayo de 2001, contra la lucha de la estafa y falsificación en relación con los medios de pago ilícitos.

[343] Op. cit. pág. 23.

[344] § 263. Estafa (1) Quien con la intención de obtener para sí o para un tercero una ventaja patrimonial antijurídico, perjudique el patrimonio de otro por medio de simulación de falsos hechos, suscite o mantenga un error la desfiguración o la supresión de hechos verídicos, será castigado con pena privativa de la libertad hasta cinco años o con multa. (2) La tentativa es punible. (3) En casos especialmente graves, el castigo será de pena privativa de la libertad de uno hasta diez años. Un caso especialmente grave se presenta cuando el autor 1. actúe profesionalmente o como miembro de una banda que se ha asociado para la comisión continuada de falsificación de documentos o estafa, 2. ocasione una pérdida patrimonial de grandes dimensiones o actúe con el propósito de conducir a un gran número de personas al peligro de la pérdida de activos mediante la comisión continuada de estafa, 3. conduzca a una persona a necesidad económica, 4. abuse de sus competencias, de su posición como titular de cargo, o 5. simule una contingencia de seguro después de haber puesto fuego él u otro con este fin a una cosa de significativo valor o haberla destruido total o parcialmente por incendio o haber hecho hundir o naufragar un buque (4) El § 243 inciso 2, así como los §§. 247 y 248 a rigen en lo pertinente. (5) Con pena privativa de la libertad de un año hasta diez años, en casos menos graves con pena privativa de la libertad de seis meses a cinco años, será castigado quien cometa profesionalmente la estafa como miembro de una banda que se ha asociado para la comisión continuada de hechos punibles según los §§ 263 hasta 264 o 267 hasta 269. (6) El tribunal puede ordenar la sujeción a vigilancia de autoridad (§ 68 inciso 1) (7) Deben aplicarse los §§ 43 a y 73 d, cuando el autor actúe como miembro de una banda que se ha asociado para la comisión continuada de hechos punibles según los §§ 263 hasta 264 o 267 hasta 269. El § 73 d debe aplicarse también cuando el autor actúe profesionalmente.

Ahora, en forma general, lo que se pretendió castigar con el párrafo fueron las acciones similares a la estafa común, pero no podían ser subsumidas por esta, toda vez que faltaban los elementos esenciales de la estafa que son *engaño y error y la disposición patrimonial,* los cuales no se encuentran activos en el fraude informático, ya que en este no presenta una relación directa y personal entre dos seres humanos, como lo exige el tipo de estafa, ni tampoco concurre una persona que sufre un error, desde el punto de vista psicológico, es decir derivado de la acción de la gente, por lo mismo al realizar estas acciones no es necesario que la disposición patrimonial sea efectuada por una persona engañada.

Por lo mismo entonces, el legislador alemán, tomando en consideración estas lagunas que exigen una relación personal para que se configure el tipo penal de estafa, introdujo un texto nuevo complementario al §263a del Código Penal Alemán, que contiene un tipo nuevo denominado fraude informático[345]. Cuando se creó nuevo tipo penal la dificultad que existió fue encontrar un equivalente al triple requisito de acción engañosa, con causa acción de error y disposición patrimonial cuando se producía un engaño de un ordenador, y con ello poder controlar y garantizar una nueva idea legislativa que se exprese de manera adecuada en la ley, tomando el legislador una equivalencia en la forma como se influye en un proceso de resultado de datos, a través de las distintas manipulaciones descritas en la norma penal que se hace referencia.

En cuanto a la estafa informática, el nuevo tipo penal tuvo que adecuarse y hacer frente a los requisitos penales del tipo básico, es decir acción engañosa, que se produzca error y la vez que exista disposición patrimonial. De esta manera Alemania, en general utiliza un criterio restrictivo para la aplicación del delito de

[345] MAGLIONA MARKOVITH, Claudio / LÓPEZ MEDEL, Macarena, *Delincuencia y fraude informático,* 1ª edición, Editorial jurídica de Chile, Santiago, 1999, págs. 240.

estafa informática, por ello hacer corresponder dicho comportamiento a un engaño, sólo existiría cuando tales procesos sean relevantes para el patrimonio y el perjuicio patrimonial, y debe ser consecuencia directa de la disposición patrimonial. No se requeriría entonces, que el operador del sistema y el perjudicado sean idénticos, por ello sería entonces un delito de fraude notorio y no de apropiación.

El Código Penal Alemán, en el §263a, sigue líneas generales de la estructura del §263, pero sin embargo estas fueron creadas específicamente para el pensamiento humano, por ello se tuvo que cambiar dichos criterios de actuación y reemplazando por la técnica de ejemplos. De la norma de la estafa informática se puede desprender cuatro posibles diferentes modalidades con misiva, a saber; *incorrecta configuración del programa; utilización de datos incorrectos incompletos; utilización no autorizada de datos; y, cualquier otra forma de influencia no autorizada en el proceso de tratamiento de datos.*

De esta manera en el § 263ª, refiere la conceptualización de la figura como tipo básico el inciso primero y la sanción de la forma imperfecta de ejecución, es decir, tentativa y un supuesto de agravación del tipo, en razón de la gravedad del hecho por la remisión que se efectúa al §263. Dicho modelo legislativo deja de lado los elementos clásicos de la estafa, puesto que se entiende que las defraudaciones de este tipo que son realizadas mediante un ordenador son de difícil aplicación o dificultaría aún más su aplicación si se toma en consideración los elementos de la estafa clásica. De esta manera el engaño hacia una persona, situación que no aparece la estructura del tipo, el error en la misma que desaparece de esta manera el requisito de provocación o manutención del error en tercero y el acto de disposición patrimonial que siendo lesivo y que además en este tipo de delito puede concurrir y puede ser realizado tanto por una persona como por el propio ordenador en forma automática, solamente entonces, requiriéndose el resultado de un perjuicio patrimonial para otro.

Al referirnos a la *incorrecta configuración del programa*, existen posiciones contrapuestas para poder entender cuando estamos frente a un programa de ordenador y cuál es su correcta configuración. Por esta razón cuando se modifica el programa para que sus instrucciones sean de otra manera, distinta o incompleta a la concebida primitivamente por el dueño o propietario de dicho aparato, vendría siendo una configuración incorrecta como en el caso cuando se introduce una instrucción o función en el programa, eliminando alterando un proceso de funcionamiento, siendo la intención del usuario del mismo cuando éste, de alguna manera lo haya puesto en funcionamiento por desconocer la incorrecta configuración, sería el criterio para determinar la incorrección del programa, no eximiendo de manera alguna al sujeto activo del delito.

Explica BALMACEDA HOYOS, que la doctrina dominante indica que se debe hacer una comparación entre el tratamiento realizado, y el resultado finalmente obtenido con el mismo de aquellos que no deberían haber producido en el sistema mediante el uso de datos correctos, y por otro lado existe una opinión minoritaria que indica que un programa es incorrecto cuando corresponde la voluntad del autorizado para exponer con la formación de las ideas[346]. Es dable se presente que se ha discutido el *tema en relación a las zonas de tensión del derecho penal de la seguridad,* al señalar que un derecho penal de la seguridad tratada, antes que todo, de mitigar la exigencias probatorias del derecho penal del Estado liberal de derecho, puesto que el estrecho apego al tenor literal de la ley ya los límites interpretativos, vienen en oponerse a dicho derecho Penal de la seguridad, señalando que el legislador muchas veces en las nuevas leyes en materia penal, se incluyen muchas palabras que no son precisas ni exactas, abordado por necesidades sociales y no tomando en consideración las futuras consecuencias de los preceptos legales que no

[346] BALMACEDA HOYOS, Gustavo…*Estafa Informática*…op., cit., pág. 23.

son definidos adecuadamente, por el contrario existen conceptos indefinidos y cláusulas generales[347].

El § 263a, teniendo en consideración el concepto de manipulación, y de modo similar a la estafa tradicional, nos habla de *uso de datos incorrectos incompletos* para estos efectos, el legislador al referirse al *proceso de datos*, lo entendió como los procesos que alcanzan determinadas conclusiones de trabajo, a partir de la toma de datos y de supuesta en relación según determinados programas técnicos. Contemplándose el proceso automático de datos, puesto que según las normas de este país, se entiende por programa una instrucción completa para la resolución de una tarea junto con todos los ajustes precisos para ello, es decir como ya se indicó anteriormente dichos programas informáticos son órdenes instrucciones para que el ordenador realice una determinada tarea. A mayor abundamiento, cuando se está en presencia de la manipulación de datos incorrectos o incompletos, la manipulación en entradas, no sólo por lo operador un usuario de la terminal que suministra de modo inmediato datos falsos a la instalación del proceso electrónico de datos, también por quienes manipulan los programas de modo inmediato, como el personal de clasificación de datos, incluyéndose también los casos de determinación, a través de

[347] "Quien, con la intención de conseguir para sí o para un tercero una ventaja patrimonial antijurídica, influyen el resultado en operación de procesamiento de datos mediante la configuración incorrecta el programa, mediante el empleo de datos incorrectos incompletos, mediante el empleo no autorizado de datos, o en general, mediante influencia ilícita en el curso del proceso, menoscabando así el patrimonio de otro, será penado…". La pregunta acerca de cómo se configura *incorrectamente*, un programa bien podría ser vista como un acertijo que algún día resolverá la jurisprudencia la ciencia. Mucho más problemático desde el punto de vista del Estado de derecho la fórmula indefinida del *empleo no autorizado de datos*. Y la expresión *en general, mediante influencia ilícita* representa, por supuesto, una traza infracción del principio anclado a nivel jurídico constitucional de determinación. Con ella, el legislador le saca el quite de manera y inconstitucional a su responsabilidad y le transfiere a los tribunales, a discreción, la facultad agrupar aquello que sea tenido por adecuado bajo la disposiciones en cuestión. KINDHÄUSER Urs, *Derecho penal de la seguridad, los peligros del derecho penal en la sociedad del riesgo*, Instituto de Derecho Penal de la Rheinische Friedrich-Wilhelms-Universität de Bonn, Cuadernos de Derecho Penal, ISSN: 2027-1743, 2014. Pág. 19.

terceros ajenos, como cuando se clasifican datos primarios, como los casos de algún suministro de manera inmediata donde se intercambien terceros que no practica ninguna comprobación material de los mismos, de esta manera el que utiliza una tarjeta falsificada de acceso al ordenador, emplea datos incorrectos del mismo modo de quien falsifica datos de alguna cuenta. Sin embargo la explicación anterior, la mayoría de la doctrina alemana tiene en cuenta el §202 a, del Código Penal Alemán, en cuanto al espionaje de datos se refiere y a la norma DIN[348] 44300-2, puesto se entiende por *dato*, aquella representación informaciones en las cuales se efectúa la representación por signos o funciones continuas, por *datos incorrectos*, aquellos que no corresponden con realidad, resultando de tal manera, información de los mismos falsa; y, por *datos incompletos*, aquellos que no dejan conocer suficientemente el supuesto de la realidad.

Cuando hablamos *de influencia en el resultado de un proceso de elaboración de datos*, a través de un uso no autorizado de los mismos, la doctrina alemana considera que de este modo se cumple, con el supuesto de, el que mediante uso ilegítimo de tarjeta y de códigos ajenos consiga, de alguna manera ingresar o acceder a los sistemas informáticos con las consecuencias que eso tiene o que tendrá para el patrimonio, siendo la influencia en el resultado de un proceso elaboración de datos, a través de la intervención, ingreso no autorizado en el proceso de la misma, por ello la doctrina la considera una fórmula amplia que pretende evitar posibles lagunas legales, marcando los supuestos que no son presumibles en las alternativas anteriores o de dudosa subsunción. Lo indicado el artículo 263a al referirse *sobre*

[348] DIN acrónimo de Deutsches Institut für Normung (Instituto Alemán de Normalización). El Deutsches Institut für Normung e.V. con sede en Berlín, es el organismo nacional de normalización de Alemania. Elabora, en cooperación con el comercio, la industria, la ciencia, los consumidores e instituciones públicas, estándares técnicos, para la racionalización y el aseguramiento de la calidad. El DIN representa los intereses alemanes en las organizaciones internacionales de normalización.

cualquier otra forma de influencia no autorizada sobre el proceso, siendo una fórmula muy indeterminada, según la historia fidedigna de la ley, "las palabras *efectos sobre el proceso* deberían asegurar que se comprendan las especialmente peligrosa manipulaciones en la consola, que no siempre presuponen datos incorrectos, y que de cualquier manera influyen en la introducción para el proceso de tratamiento de datos o cambien el proceso automático del programa"[349]. El elemento insertado más tarde *no autorizada,* una variante del tipo, un elemento que constituye el contenido del injusto del comportamiento, y una peculiaridad del delito, no solamente general.

De esta forma el hecho punible tiene que influir en el proceso de tratamiento de datos informáticos, es decir el autor influye con el fin, de llegar a cambiar el resultado de los datos que se almacenan en el ordenador, y además de aquellos utilizados por el programa de trabajo[350]. El legislador alemán trató incluir el abuso de tarjetas bancarias, de otras tarjetas de código de procedimientos técnicos de pago similares, en el mismo artículo que sanciona la estafa informática.

En cuanto al lado subjetivo, el parágrafo 263a StGB, exige la concurrencia de un elemento subjetivo del tipo, como lo es la intención de procurarse asimismo o a un tercero un beneficio patrimonial antijurídico o ánimo de lucro, tragándose entonces una figura dolosa. Se debe indicar que el legislador alemán no se refiere, en

[349] BALMACEDA HOYOS, Gustavo, Revista de derecho y ciencias penales, Número 17, Universidad San Sebastián, *El delito de estafa informática en el derecho europeo continental*, Chile, 2011. Pág. 124.

[350] "No basta con que un operador, su gobernado por la competencia, paralice el tratamiento de datos por medio de una programación defectuosa, ni tampoco con que los resultados erróneos de las operaciones del ordenador, debido a su defectuosa explotación, provocan por sí solos un daño patrimonial. Aquellos perjuicios patrimoniales en los que el ordenador no es más que un medio de ayuda para una acción lesiva que tiene lugar tras el proceso tratamiento de datos no se incluyen en el tipo". MAGLIONA MARKOVITH, Claudio / LÓPEZ MEDEL, Macarena, *Delincuencia y fraude informático*, Editorial jurídica de Chile, Santiago, 2010. pág. 244.

forma específica, al ordenador o al termino informático, teniendo cabida entonces en el precepto de las manipulaciones fraudulentas, que tienen que ver con el patrimonio cayendo entonces en cualquier tipo de sistemas automatizados de toma de decisión, y no solamente en el informático, de esta forma la acción típica vendría siendo la interferencia que realiza el sujeto en el resultado de un proceso de tratamiento de datos, la que trae como consecuencia una interferencia o intromisión en una disposición patrimonial[351].

En el artículo 202 b, podríamos decir que legislador alemán ha tratado una forma particular *phishing*[352], al tratar de proteger el *bien jurídico de privacidad de la información*, reforzando en este párrafo el hecho que el delincuente informático acceda a la información que se encuentra resguardada o protegida del acceso al público, pero la diferencia con la sección 202 a, es que apunta solamente a datos que si bien son privados no se encuentran de alguna forma especial protegidos por la persona que lo posee en forma legítima, resguardando el artículo en comento las situaciones que se encuentran fuera de la sección 202 a. De igual forma es conveniente hacer mención a los actos preparatorios del espionaje de datos, los trata en la sección 202c[353], aquí se destaca que se sanciona por el acto en grado de tentativa, puesto que la sustracción de información o difusión de ésta no requiere

[351] Por su parte, se estima que el concepto de dato es más amplio que el que se contiene en el artículo 202 a, pues no se limita a los datos que no sean perceptibles inmediatamente.

[352] CPA § 202 b: Toda persona que ilegalmente captura de datos (§ 202 a (2)) que no están destinados para él, para sí o para otros, por medios técnicos de un sistema de procesamiento de datos no pública o de la radiación electromagnética de un sistema de procesamiento de datos, la pena es de prisión no superior a dos años o multa si el acto causa un severo castigo en virtud de otras disposiciones.

[353] El que prepara la Comisión de un delito en virtud del § 202 o 202 b, a través, de la adquisición por sí mismos o para otros, la venta, el suministro a otro, difusión o cualquier otra puesta a disposición. Contraseñas u otros códigos de seguridad para acceder a datos (202 a (2)), o 2. Software con el propósito de cometer un delito, se castiga con hasta un año o una multa. (2) § 149 (2) y (3) se aplicarán mutatis mutandis.

que se encuentre consumado, sólo se exige o se perfecciona con la sola preparación de éste, recayendo el objeto del delito en las denominadas, *contraseñas u otros códigos de seguridad que permiten el acceso a los datos,* no siendo propiamente el dato o contenido de la información dicho objeto, sino cuando se accede a ella o ellos, para utilizarlo en beneficio propio o de terceros por cualquier medio. Asimismo como la misma norma lo indica con la creación de un software, que tenga por fin la comisión o que se utilice para perpetrar el delito propiamente tal. Una cosa que es importante señalar es que En el StGB en sus parágrafos §303 a y §303 b, se refiere a la idea de dañar datos y obstaculizar sistemas informáticos, pero a pesar que menciona dichos conceptos no explica o no entrega una solución respecto del modo de hacerlo, ni tampoco se hace cargo o menciona cuando el delincuente informático ha utilizado, algún tipo de virus informático o software malicioso malware para realizar el daño o la obstaculización.

C) Regulación legal de la estafa informática en Italia[354]

[354] El Código Penal italiano tipifica los siguientes delitos informáticos: Acceso abusivo a un sistema informático o telemático (artículo 615 tercero), en este caso protege sistemas informáticos o telemático protegidos por dispositivo de seguridad, donde se indique la privacidad del sistema y la voluntad del usuario de reservar el acceso al mismo, sólo a las personas autorizadas; Difusión de programas dirigidos a producir daños o interrumpir un sistema informático o telemático (artículo 615 quinto), se ponen el caso para el que difunde un programa informático que tenga por objeto el daño a un sistema informático telemático, datos o programas, o la interrupción total o parcial del funcionamiento; Atentado contra un sistema informático o telemático de utilidad pública (artículo 420), sanciona aquel daño destruya un sistema informático de utilidad pública; Abuso de la calidad de operador de sistema, el cual es un agravante del delito de acceso abusivo y lo comete quien tiene la posibilidad acceder y usar un sistema informático telemático de manera libre por la facilidad de comisión del delito; Detentación y difusión abusiva de códigos de acceso a sistemas informáticos o telemáticos (Artículo 615 cuarto), sanciona al que con el fin de obtener para sí o para otro un beneficio o causando un daño a otro, abusivamente se apodera, reproduce, difunde, comunica códigos, palabras claves u otro medio idóneo que permita el acceso sistema informático telemático; Difusión de programas dirigidos a dañar o interrumpir un sistema informático (Artículo 615 quinto); Violación de la correspondencia electrónica (artículo 616); Intercepción abusiva. (Artículo 617, cuarto, quinto); Falsificación informática (617 sexto).

El fraude informático, se regula en el en el artículo 640ter del Código Penal[355], dirigido a reprimir las hipótesis de enriquecimiento conseguidas por el empleo fraudulento de un sistema informático.

En Italia en cuanto delito de estafa informática se base en el esquema de estafa tradicional, se aplica entonces aquellos casos en que el ordenador reemplazaría el proceso de decisión del ser humano. De esta manera las tipologías de agresiones informáticas en Italia abordan la regulación del delito informático de una forma más o menos similar al español, haciéndose cargo de tipologías como el fraude informático[356].

El artículo 640ter del Código Penal italiano, indica *el que de cualquier modo altere el funcionamiento de un sistema informático o telemático o interviniendo sin derecho con cualquier modalidad sobre los datos, informaciones o programas contenidos en un sistema informático o telemático o a ellos concernientes, procurando para sí o a otro un injusto provecho con daño para otro, será castigado con reclusión de 6 meses a 3 años y con multa de 51 euros a 1032 euros. La pena se eleva si concurre alguna circunstancia del N° 1 del segundo párrafo del artículo 640 o bien si el hecho es cometido con abuso de la cualidad de operador del sistema. El delito es punible por querella de la parte ofendida, salvo que concurra*

[355] Artículo agregado el 23 de diciembre de 1993, Ley N° 547, sobre los cambios y adiciones a las reglas del código penal y el código de procedimiento penal sobre los delitos informáticos. Dicha ley en su artículo 10, establece, que el artículo 640 bis del código penal se inserta el artículo 640-ter, sobre (Fraude informático).

[356] El artículo 640 ter del Código Penal Italiano establece: el que de cualquier modo altere el funcionamiento de un sistema informático o telemático o interviniendo sin derecho con cualquier modalidad sobre los datos, informaciones o programas contenidos en un sistema informático o telemático o a ellos concernientes, procurando para sí o a otro un injusto provecho con daño para otro, será castigado con reclusión de seis meses a tres años y con multa de 51 euros a 1.032 euros.

alguna de las circunstancias del segundo párrafo o alguna otra circunstancia agravante.

La legislación italiana regula de una manera independiente aunque de cierta manera conectada con la estafa el fraude informático, denominándolo de esa manera, aunque la jurisprudencia de ese país se muestra o entiende que el fraude informático tiene los mismos elementos constitutivos de la estafa, sólo diferenciándolos en que la actividad del agente, es fraudulenta, no recae sobre una persona, sino recayendo sobre un sistema informático[357].

De la lectura del precepto se puede diferenciar con la legislación española en cuanto a que la regulación de la pena a diferencia del articulo 640.2 el cual no indica pena alguna, pero si se aplica la de la estafa genérica los artículos 249 y 250, podemos deducir que en el caso de Italia la concurrencia del delito para el fraude informático es o coincide con la estafa y que al hablar de agravaciones de la pena tendrá la misma que alguna de las agravaciones de la estafa, excluyéndose las del punto 2. En definitiva el ordenamiento jurídico español hace extensivo al fraude informático, a todos los supuestos agravados de la estafa genérica en cambio en el caso en estudio, sólo algunos.

Es del caso hacer presente, o indicar que la legislación italiana es más completa al referirse a dos hipótesis *alteración del funcionamiento de un sistema informático o telemático; intervención sobre los datos sin derecho.* La última expresión da lugar a problemas interpretativos y puede coincidir de alguna manera

[357] Un sector de la doctrina difiere al respecto, previéndose una conducta completamente diferente a la estafa, si bien otros autores estiman destacable los idénticos elementos con ésta y la diferencia vendría dada por la manipulación del sistema. GARCÍA-CERVIGÓN, Josefina, *El fraude informático en España e Italia, tratamiento jurídico-penal y criminológico,* Icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales, nº 74, mayo-agosto 2008, ISSN: 02 12-7377, pág. 299.

en el provecho para sí o para terceros como en el ánimo de lucro con el Código Penal Español. El bien jurídico tutelado en el ordenamiento italiano es el patrimonio y además también se habla que tendría que ser la libertad de negociar del perjudicado, la actividad bancaria, puesto que la norma viene en regular el funcionamiento correcto de los sistemas informáticos, negando la doctrina que se esté en presencia de una estafa distinta o especial [358]. Otro sector doctrinal estima que el sistema informático es un complejo o conjunto de aparatos unidos e integrados con un fin determinado, y el sistema telemático es un conjunto de aparatos interactuados y coordinados, unidos mediante estructuras comunicativas a distancia finalizada en datos.

El artículo en comento distingue 2 hipótesis de actuación. La primera de ella nos indica el objeto de la conducta en un sistema informático o telemático, en este caso existen dos tendencias donde la primera definición más restrictiva lo entiende como un complejo de muchas instalaciones, teniendo un nivel de estructuración y complejidad excluyendo al simple ordenador personal. Por otro lado se define más ampliamente incluyendo a ordenadores personales por la cantidad de datos y programas que pueden contener, se evalúa la autonomía del mismo, incluyendo incluso aparatos como el teléfonos, fotocopiadoras, cajeros, y a su vez entendido que un sistema telemático, es gestado como sistema de telecomunicaciones con cierta tecnología informática, entendiéndose incluso que al referirse el código penal, al sistema informático telemático e intervención sin derecho, no estaría haciendo alusión a dos conductas que son distintas o alternativas una de la otra, debiendo encuadrarse cada acción delictiva dependiendo de cómo ha sido desarrollada, sino

[358] CRESPI, Alberto, / STELLA, Federico / ZUCCALA, Giuseppe, C*omentario breve al códice penale, Milan*, Editorial Cedan, Milano, 2003. Citado por GARCÍA-CERVIGÓN, Josefina, El fraude informático en España e Italia, tratamiento jurídico-penal y criminológico, icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales, nº 74, mayo-agosto 2008, ISSN: 02 12-7377, pág. 301.

que estaríamos hablando de una especificación de la primera conducta. En esta primera hipótesis, la conducta fraudulenta tiene que consistir en alterar, de cualquier modo, el funcionamiento un sistema informático, o bien en intervenir, con cualquier modalidad, sobre determinada información el programa contenía el sistema o a ellos pertinentes. Esta intervención entonces, tiene por objeto el funcionamiento sistema informático telemático, y consiste en una modificación del desarrollo regular de proceso de elaboración o de transmisión de datos realizado por un sistema informático telemático[359]. Por otra parte la voz de cualquier modo tiene que ser la consecuencia de no intervención relativa, ya sea el componente mecánico del ordenador o bien el software en sí mismo.

Una segunda hipótesis de ejecución del fraude informático italiano es la intervención sobre los *datos sin derecho*, haciendo pensar que cuando se gestó dicha norma, el legislador italiano quiso incluir cualquier dato registrado informáticamente, recalcando la relevancia del eventual consenso del sujeto titular o responsable del sistema dándole importancia al carácter de injustica del provecho obtenido[360], es decir existe una conducta activa en el sentido de incluir datos en el interior de un ordenador, o incluirlo sobre el programa, con ello se configura la intervención sin derecho, teniendo en consideración que existe un doble elemento normativo referido a la conducta y al evento, refriéndose a datos, informaciones o programas obtenidos en un sistema informático. La alteración del sistema que tiene que ver con la expresión intervención, es distinta a un acto preparatorio incidiendo con ello en el funcionamiento de la máquina como seria en el hardware, cuando hablamos de modificar la estructura de la maquina o sobre el software, cuando

[359] BALMACEDA HOYOS., Gustavo, El Delito…Op. Cit. Pág. 74.

[360] LATTANZI, Giorgio / LUPO, Ernesto, *Codice penale rassegna delito informático geieurisprudenza e di doctrina*, Volumen I, Editorial Anno di, Giuffre Milano, 2015, pág. 539.

estamos hablando de los programas o datos registrados en la máquina. En este caso estamos hablando de manipulaciones del *input*, y manipulaciones del *output*.

Cuando hablamos de dolo en el fraude informático en el código italiano se habla de la voluntad con el ánimo de alterar el funcionamiento de los sistemas, interfiriendo en los datos, programas y la información contenida en ellos, pudiendo configurarse igualmente el dolo eventual.

Es necesario indicar que el fraude informática a diferencia de la estafa genérica no contempla el error considerándose que el tipo admite un requisito tácito, el cual es idóneo para individualizar un nexo entre la conducta fraudulenta y el provecho, de esta manera el provecho injusto encuentra su origen en el resultado regular en un proceso de elaboración que tiene como objeto una interferencia que es indebida. En cuanto a la consumación podemos decir que se da en el caso de tener disponibilidad electrónica sobre la suma defraudada, consumándose en el momento de la realización del provecho con el consecuente daño para otro, siendo factible el concurso con la falsedad informática, y respecto del fraude fiscal y la estafa, la relación seria compleja, destacándose eso sí, en Italia, el concurso con delito abusivo a un sistema informático.

II. Regulación legal de estafa tradicional e informática en Chile

Antes de analizar la estafa informática en el derecho chileno, se hace necesario entregar un somero análisis del delito estafa clásica en Chile, con ello se pretende que el lector pueda, tener una visión en lo medular, del tipo delictivo en cuestión, de manera tal, que al mismo tiempo pueda tener información global y

básica, en comparación con la legislaciones analizadas anteriormente sobre la materia.

A) El delito de estafa clásica en Chile. Comentarios

En esta materia, en relación a la estafa y otros engaños, el antecedente inmediato de nuestra ley penal es el Derecho Español. En 1874, nace el Código Penal Chileno, que regula su libro II, título IX, *los crímenes y siempre delitos contra la propiedad,* párrafo 8, lo que a su vez denomina en su epígrafe, *estafas y otros engaños,* entre los artículos 467 a 473, reproduciendo en su mayoría el Código Penal Español de 1848, manteniéndose hasta hoy la estructura del mismo sin muchas modificaciones salvo sólo en materia de penas. Nos dice Etcheverry[361], que se deduce del título, antes transcrito, en qué legislador habría querido trazar una línea divisoria entre la estafa propiamente tal del artículo 468 del Código Penal Chileno y los otros engaños del artículo 423 del mismo, excluyendo la aplicación de ésta, a los casos donde la actividad consiste en una mentira o un silencio que, por las circunstancia externa preexistente, no es creada por el autor, sino aprovechada por este, induce a una desposesión patrimonial; la actividad consistente en una mentira o un silencio, encontrándose el autor en la obligación de decir la verdad, como ocurre en el caso de los funcionarios públicos, y por lo mismo esto caso la actividad del agente no alcanza configuraron ardid o una maquinación que permita hablar de estafa, y por lo tanto, estaríamos ante unos otros engaños, ahora bien esta afirmación

[361] ETCHEVERRY, Alfredo, *Derecho Penal en la jurisprudencia*, tomo III, 3ª Edición, Editorial Jurídica de Chile, Santiago, 1987, págs. 391 y sigs.

supone naturalmente un concepto de estafa que la identifique con un ardid o maquinación fraudulenta, *la puesta en escena, mise en scene*[362].

El código de Chile no tiene un concepto general de estafa que de alguna manera mucho los requisitos típicos de la figura delictiva, lo que hace es establecer un sistema de casos ya además una figura residual que también tiene problemas hasta el día de hoy de interpretación, lo que lleva a pensar en una confusión del legislador al momento de crear el tipo penal de estafa y poder plasmar su característica principal es en la ley. La figura básica, de la estafa se encuentra en el artículo 468 del Código Penal chileno el que indica que "el que defraudar a otro usando de nombre fingido, atribuyéndose poder, influencia o créditos supuestos, aparentando bienes, créditos, comisión, empresa o negociación imaginarios, o valiéndose de cualquier otro engaño semejante"[363] [364]. Además de ello, este artículo

[362] POLITOFF, Sergio / MATUS, Jean Pierre / RAMÍREZ, Cecilia, *Lecciones de derecho penal chileno*, Editorial Jurídica de Chile, Santiago, 2004, págs. 412 y sigs. Al respecto, los autores al constatar, que dentro del Código Penal Chileno, y el hecho de que dentro del párrafo 9 del título IX libro segundo, se contemplan figuras que de ninguna forma pueden considerarse estafa, como la apropiación indebida y el mal llamado hurto de posesión, no se plantean una sistematización de los delitos allí contenidos: 1) Estafas propiamente tales. Figura básica artículo 473 Código Penal. 2) Figuras especiales. Artículo 468 Código Penal: estafa calificada por la clase de engaño empleado. Artículo 467.469 N° 1 y 469 N° 2 del Código Penal: fraudes en la entrega. Artículo cuatro 469 N° 5 y 470 N° 7: estafas con causa ilícita. Artículo 470 N° 4, 5,6 y 8 Código Penal: estafa por medio de falsificación instrumento privado. 2) Otros engaños. 1) fraudes por abuso de confianza. Artículo 469 N° 3, 469 N° 4 y 470 N° 2 del Código Penal: administración fraudulenta. Artículo 470 N° 3 Código Penal: abuso de firma en blanco. 3) delitos de estafa ni engaño (aquí la vos defraudación sólo indica perjuicio). Artículo 470 N° 1 Código Penal: apropiación indebida. Artículo cuatro 471 N° 1 Código Penal: hurto de posesión. Artículo 469 N° 5 Código Penal: destrucción de documentos. Artículo 469 N° 6 Código Penal: destrucción de la cosa embargada. 4) Celebración de contratos simulados. Artículo 471 N° 2 Código Penal. 5) Usura artículo 472 Código Penal., Alzamiento de bienes artículo 466 y otros fraudes contenidos en leyes especiales (Derecho Penal económico).

[363] Código Penal Chileno de 1874, artículo 468: incurrirá en las penas del artículo anterior es que defraudaré a otro usando un nombre fingido, atribuyéndose poder, influenciado crédito supuestos, aparentando bienes, créditos, comisión, empresa o negociación imaginarios, o valiéndose de cualquier otro engaño semejante.

[364] FERNANDEZ DÍAZ, Álvaro, *Engaño víctima en la estafa,* Revista de derecho de la Pontificia Universidad católica de Valparaíso XXVI, Semestre I, Valparaíso, 2005, págs. 181 y sigs.

está en directa relación con el artículo 473 del mismo código que establece una figura residual que sanciona al que "defraudare o perjudicar a otro usando de cualquier engaño que no se haya expresado el artículo anterior en este párrafo"[365]. Ahora bien, de los dos artículos antes mencionados no puede extraerse los requisitos de la estafa sólo se puede obtener la exigencia de un engaño y de un perjuicio, no refiriéndose al error ni al acto de disposición patrimonial que debe realizar la víctima. Por otro lado como se dijo anteriormente, el párrafo que reúne las conductas típicas, antes referidas muchas de ellas no serían constitutivas propiamente estafas, como por ejemplo el caso de la apropiación indebida regulada en el número 1° del artículo cuatro 470 del Código Penal, algo que no es adecuado por su naturaleza y además porque se despliegan distintas conductas confundiendo entonces la misma actividad que son propias del engaño con otras que son del abuso de confianza. En definitiva lo característico de legislador al tipificar las estafa, que por un lado no entrega todo sale los elementos característicos de ella también indica ejemplos, es decir nos entrega un método casuístico que viene a restringir aún más la forma correcta interpretación, que sería la más adecuada para poder tipificar este tipo de delito, como lo han hecho otras legislaciones que se refieren al tipo penal en forma general y no casuístico. Por esta razón es la doctrina la que ha tenido que elaborar los elementos típicos de la estafa a partir de los tipos penales entregados por el legislador.

Al respecto, nos dice el autor que si bien esta figura está tomada de forma textual del Código Penal español de 1848, es indudable que su redacción se vio influenciada por el artículo 405 del Código Penal francés de 1810.

[365] Código Penal chileno de 1874, artículo 473: el que defraudaré perjudicaría otro usando de cualquier engaño que no se haya expresado lo artículo anteriores de este párrafo, será castigado con presido relegación menores en sus grados mínimos y multas de once a veinte unidades tributarias mensuales.

1. Bien jurídico protegido

En cuanto al bien jurídico protegido, la jurisprudencia chilena en mayor medida se inclina por la teoría mixta- económica jurídica del patrimonio. Aunque en el código penal chileno la figura de la estafa se encuentra dentro de los delitos contra la propiedad, la doctrina indica que no es la propiedad lo que se afecta con este tipo de delito o no lo sería en el sentido del concepto de propiedad que vendrían a caer en mayor medida en los delitos de hurto, antaño o robo, puesto que ellos efectivamente recae sobre el objeto material preciso y que afectada la propiedad directamente por el delito.

Entonces a pesar que muchas veces se obtiene una cosa a través de un engaño no es en sí mismo el bien jurídico protegido. Por lo mismo, se reafirma la doctrina que el bien jurídico protegido en este tipo de delito en cuanto al código penal chileno se trata, sería el patrimonio. Ahora bien para determinar qué lo que se entiende por patrimonio derechamente hablaremos solamente del concepto mixto de patrimonio, el cual se entiende como un conjunto de bienes que se encuentran bajo la tutela y disposición de una persona, siendo este poder sobre dichas bienes jurídicamente reconocido.

2. Tipo objetivo

Como se dijo anteriormente el Código Penal en Chile en cuanto al delito de estafa se refiere poco claro utilizando un método en el cual entrega ejemplos en vez de una definición general, centrándose la jurisprudencia en aplicar la teoría de la *mise en scene*[366], en la cual en cualquiera de la hipótesis entregadas por el código habría que ponderar el engaño, tomando en consideración la puesta en escena externa, donde se aparentaba una falsa verdad, engañando esta manera la víctima[367].

[366] SCS. Rol N° 5128-2008, 06.10.2009, La cual nos indica en los concerniente: noveno: Que, al referirse al primer motivo de nulidad invocado, el recurrente afirma que no se ha demostrado el elemento perjuicio patrimonial de la víctima, indispensable para configurar el delito de estafa y que el daño moral concedido al acoger la sentencia la demanda civil no sirve para dicho efecto, de forma tal que al faltar este componente del tipo penal, o bien, no habiendo sido acreditado por los medios legales, la sentencia recurrida ha calificado como ilícito penal un hecho que la ley no considera como tal. Por otra parte, agrega el recurso, no habiéndose alcanzado el estándar requerido por el artículo 456 bis del Código de Procedimiento Penal, y por consiguiente habiéndose infringido las leyes reguladoras de la prueba, una de las cuales es el artículo 457 del Código de Procedimiento Penal (al considerarse probado el elemento perjuicio por medios distintos de aquéllos descritos en la disposición legal precitada), esto ha influido sustancialmente en lo dispositivo del fallo. Señala genéricamente como normas infringidas los artículos 1°, inciso 1° y 468 del Código Penal y 456 bis y 457 del Código de Procedimiento Penal y, finaliza su exposición pidiendo la invalidación de la sentencia y la dictación de la correspondiente de reemplazo que lo absuelva de todo cargo.

Causal 3ª del artículo 546 del Código de Procedimiento penal. Décimo: Que, en relación a la primera causal de casación invocada, calificar como delito un hecho que la Ley Penal no considera como tal por no haberse probado legalmente el elemento, perjuicio consustancial al delito de estafa, cabe precisar que tanto la doctrina como la jurisprudencia reconocen que la referida figura penal consiste en una apropiación por medios inmateriales que se apoya en un ardid o despliegue escénico ejecutado por el sujeto activo del delito destinado a producir un error en la víctima, la que movida por su equivocada percepción de esa realidad, dispone de su patrimonio con la consiguiente lesión pecuniaria. Elementos del injusto generalmente aceptados son el engaño, el error, la disposición patrimonial y el perjuicio, debiendo mediar entre todos ellos una relación de causalidad directa e inequívoca. Undécimo: Que, del estudio y análisis conjunto de la sentencia reprochada, por ejemplo, considerandos segundo y décimo, se desprende, con toda claridad, que los hechos establecidos por los sentenciadores de la instancia reúnen todos los componentes que integran el tipo penal de estafa, incluido el "perjuicio" al ser la víctima despojada jurídica y materialmente de sus bienes los que se encuentran debidamente identificados en la causa. El perjuicio propio del delito de estafa consiste en que la víctima realiza un acto de disposición patrimonial en virtud del cual se produce correlativamente un daño para ella y un enriquecimiento para el sujeto activo del delito: requiere de una conexión entre la pérdida de uno y la ganancia del agente del delito.

[367] BALMACEDA HOYOS, Gustavo, El delito de estafa la jurisprudencia chilena, en revista de derecho Universidad Austral de Chile, Vol. XXIV, núm. 1, 2011, págs. 59 y sigs. Nos dice el autor que se aplicaría el artículo 438 el código penal a los engaños que constituyan ardides o

De acuerdo lo anterior, la doctrina y también la jurisprudencia en forma general exigen cuatro elementos a la referida estafa, como son el engaño, error, disposición patrimonial y perjuicio[368], y algunos agregan también relación causal entre el engaño y el resultado.

2.1. Sujetos

En principio existe un sujeto activo y un sujeto pasivo. Ahora bien, en cuanto a la víctima en el mismo sentido que indica el artículo 108 del Código Procesal

maquinaciones. Y el artículo 473 del mismo código, en cambio, se destinaría al resto de engaños siempre cuando se trate de algo más que una simple mentira. Entonces, el tipo básico sumamente complejo, ya sea por la determinación de sus elementos o por la disposición de la relación que debería existir entre cada uno de ellos.

[368] SCA de San Miguel, Santiago de Chile, Rol Corte N° 303-2015, 11.04.2016. La cual nos indica en los concerniente al tema: "Cuarto: Que conviene tener presente que el engaño grande o pequeño, no influye para nada en la gravedad de la infracción, ya que puede haber maniobras del más burdo contenido, que producen el resultado apetecido sobre campesinos o personas de mínima cultura, de ahí que se acepta la relatividad y circunstancialidad del engaño en relación a las personas. (QUINTANO RIPOLLÉS A. Tratado de la Parte Especial del Derecho Penal, tomo II, Madrid, Ed Revista de Derecho Privado 1977, pp.590 ss.). Además, el error del que realiza el acto de disposición no se produce a causa del hecho futuro pronosticado, sino por la convicción de existir una correspondencia entre lo que dice y lo que piensa el engañador cuando se refiere al hecho futuro, así el engaño proviene de un hecho psicológico, como es el pensamiento y voluntad del embaucador en el momento presente. (ANTÓN ONECA, J, "Estafa". Nueva Enciclopedia Jurídica, Editorial Francisco Seix Barcelona, Tomo IX 1958, pág. 64). Quinto: Que la doctrina y jurisprudencia concuerdan en definir la estafa como la apreciación por medios inmateriales a consecuencia de un despliegue ejecutado por el sujeto activo con la intención de producir error en la víctima, que por su errada percepción de la situación, dispone de su patrimonio con la consiguiente lesión pecuniaria. De aquí se desprenden los elementos que tipifican el delito de estafa, esto es, el error, la disposición patrimonial, el engaño y el perjuicio, debiendo necesariamente existir un nexo causal entre tales elementos. En efecto, su tipificación radica en la defraudación causada mediante engaño, por lo que se ha entendido que se trata de un delito calificado por su resultado ya que el perjuicio patrimonial que experimenta la víctima constituye un elemento determinante, que por lo mismo debe ser susceptible de una apreciación pecuniaria".

penal, puede ser una persona natural o jurídica, derecho público privado, incluso una potencia extranjera. Ahora bien cuando estamos hablando de persona jurídica no se refiere a que sea esta la persona engañada sino que se afecte su patrimonio. Además de ello de acuerdo a la redacción del artículo 473 del código penal chileno, el medio utilizado para defraudar o perjudicar a otro puede o no recaer sobre la persona del perjudicado[369].

2. 2. La conducta típica

Al respecto debemos hablar del *engaño*[370]. Se exige que éste engaño, no sea una simple ilusión, se requiere que tenga el propósito o apariencia de verdad, de tal manera que con la mentira se altere la situación objetiva, es decir debe ser capaz de inducir a error, en el sujeto pasivo y con ello producir el acto de disposición patrimonial.

[369] Menciona ETCHEVERRY, es posible afirmar que ni aún la disposición patrimonial debe ser hecha materialmente por el perjudicado, como sería si alguien viene gente de banco pertenezco de un cheque extranjero falso pagándose posteriormente por la caja la cifra defraudada, aquí el sujeto pasivo es la institución financiera que sufre detrimento patrimonial, el que se produce mediante el engaño a la gente, quien ordena al cajero practicar una disposición patrimonial. POLITOFF, Sergio / MATUS, Jean Pierre / RAMÍREZ, María Cecilia, *Lecciones de Derecho penal Chileno*, Editorial Jurídica de Chile, 2004, pág, 421.

[370] FERNANDEZ DÍAZ, Álvaro, *Engaño víctima en la estafa*, Revista de derecho de la Pontificia Universidad católica de Valparaíso XXVI, Semestre I, Valparaíso, 2005, págs. 181 y sigs. El autor plantea que la opinión ampliamente dominante de la doctrina y jurisprudencia chilena exige una cierta idoneidad de la conducta engañosa para que ya sea típicamente relevante. En otras palabras, no todo engaño que produzca un acto de posesión por error sería punible. Nuestra doctrina y jurisprudencia fuertemente influenciada por CARRARA considera que el engaño típico no puede consistir en una simple mentira, sino que en una mentira inserta en un despliegue engañosa externo (esto regiría tanto para los artículos 468 473 del Código Penal Chileno, disposiciones que se distinguirían entre sí sólo por la gravedad de la preparación de escena desplegada, aunque esto último con matices en la doctrina). En lo que se conoce como la teoría de la mise en scene.

Se entiende que la estafa descansa, sobre la utilización del engaño por el sujeto activo por su naturaleza, entidades circunstancias, sea suficiente para producir un error del sujeto pasivo, induciéndole a realizar un acto de disposición patrimonial en detrimento propio ajeno. También es necesario señalar, que entre la tic y el acto de disposición deberá existir un nexo causal, por lo mismo el engaño o artificio debe ser causante del menoscabo originado, por esta razón importante no es la conducta activa u omisiva, que desarrolla la gente sino por la importancia, cual es la idoneidad para que ella produzca una representación distinta o falsa de la realidad y el resultado lucrativo buscado, por ello en el caso a caso, lo que lleva a que se configure el tipo penal de estafa no es otra cosa que su eficacia real. Además de ello es terror debe ser directamente imputable al truco o treta. Se debe dejar claro que en algunos casos, el acto puede ser casi instantáneo, coincidiendo en un momento temporal, tanto la maniobra que tiene por fin engañar y a su vez la defraudación. De esta forma afirma el profesor BALMACEDA HOYOS, que nuestro país se ha dicho que la simple mentira no es suficiente para componer una simulación por un lado, porque no existiría en materia penal una obligación genérica de decir la verdad y, por otra parte, porque consentir la contingencia de castigar como fraude Penal cualquier mentira en que otro haya creído, significaría ampliar excesivamente el ámbito del fraude Penal en deterioro del fraude civil.

Hoy en día la teoría aplicada constantemente por nuestra jurisprudencia, es decir la puesta en escena, es objeto de múltiples críticas, puesto que lo que se aplicaría para resolver los problemas en este caso debería ser estudiado respecto del problema de la tipicidad. El mismo profesor citado anteriormente, nos indica que sistemáticamente, existen graves contradicciones posterior por un lado, se sostiene que no se puede proteger a la víctima negligente y, de otra parte, se afirma que la aptitud del engaño se mide en atención a las creencias propios de la maniobra, y por ello de ser coherente, la aptitud del engañado se debería medir conforme con la

negligencia de la víctima. Añade, que no existe en la legislación chilena ninguna forma que impida castigar a la simple mentira cómo engaño típico, y además que el principio sobre lo que se fundamenta el cual es la *última ratio,* se encuentra dirigido al legislador y no al intérprete, incidiendo solamente la tipificación del engaño y no sobre el momento del caso a caso en que se deba interpretar[371].

2.3. El resultado típico de disposición patrimonial y perjuicio

Por el error, el engañado debe realizar una disposición patrimonial, para qué el tipo penal nazca siendo esta disposición patrimonial el hecho material que del propio engañado el estafador obtiene. Éste perjuicio patrimonial es una pérdida pecuniaria, que tiene un carácter económico tomado como una universalidad, es decir conjunto de bienes, de derechos, posiciones u otros valores de carácter económico respectos de los cuales la víctima tiene la facultad o poder de hecho para disponer de ellos. En este caso no son valores inmateriales, ideales morales o de afectación. Esta disposición material que realiza la víctima produce en ella un daño, y correlativamente enriquece a otro, siendo una merma en el patrimonio no siendo de relevancia que está merma de patrimonio tengan importancia en el propio engañado, o en el de otro distinto. Cuando estamos hablando de patrimonio estamos hablando de algo económico y a la vez jurídico, siendo esto un bien individual y por ello el legislador protege de alguna manera estos bienes y tipifica el delito, no habiendo delito en casos como por ejemplo de mera frustración de móviles o finalidades objetivas del reclamante, que no tienen algún efecto concreto en el

[371] BALMACEDA HOYOS, Gustavo, *El delito de estafa la jurisprudencia chilena*, en revista de derecho Universidad Austral de Chile, Vol. XXIV, núm. 1, 2011, págs. 59 y sigs.

sentido patrimonial, siendo protegido entonces, el patrimonio como bien jurídico individual o particular y no como algo colectivo o macro social.

2.4. Tipo subjetivo

En Chile según la doctrina general, el dolo comprende el conocimiento y la voluntad de engañar, producir un error, una disposición patrimonial y un perjuicio económico, por ende en Chile no existe la estafa imprudente, requiriendo dolo directo. Ahora bien, respecto del ánimo de lucro, en Chile se discute su procedencia, puesto que la ley al tipificar el delito, al parecer no lo exige como elemento subjetivo, sosteniéndose que dicho elemento debe exigirse como parte integrante de la estafa, siendo este la unión necesaria entre la participación del agente con la misma defraudación causada y a su vez el correlativo enriquecimiento que trae consigo el delito[372]. En cuanto al error, excluye al dolo, donde existe una falsa representación de la realidad, mediante la cual el sujeto activo, traspasa a la víctima en el supuesto que se está entregando la verdad. El controlador este mismo, representa una falsa realidad en que incurrió sujeto pasivo, como consecuencia directa de la maniobra engañosa. La escena desplegada determina la voluntad del sujeto pasivo, debe llevarlo formarse por sí mismo su propio juicio, y como se dijo anteriormente los requisito que la misma persona inducida o engañada sea o recaiga

[372] CONTRERAS TORRES, Raúl, *El delito de Estafa*, Editorial Jurídica Conosur Ltda., Santiago, Chile, 1992, págs. 74. El ánimo de lucro, no ha sido expresamente considerado en nuestra ley penal. En consecuencia, podrá sostenerse que él es ajeno al delito que nos ocupa. Empero debemos considerarlo como elemento integrante, puesto que esta finalidad de lucro es el nexo necesario que une la participación del agente con la defraudación causada y el correlativo beneficio que supone el delito de estafa.

en la del perjudicado, por ello siendo uno el sujeto de la acción, y el otro será sujeto pasivo del delito, y que por ende es titular del bien jurídico perjudicado.

2.5 Iter criminis

Cuando estamos en presencia del delito de estafa, éste se consuma con el perjuicio, de lo contrario estaríamos en presencia de tentativa frustración. En cuanto la tentativa esta comienza con el engaño que vendrían siendo actos directos conducentes al mismo o la obligación de despejar el error y que por ende se omitió si tenía la obligación hacerlo. Ahora bien en cuanto la frustración existe la misma, cuando la producción de perjuicio ya no dependa del autor. Por lo mismo la idoneidad del engaño depende de su apreciación antes, con independencia de si es descubierto no es solamente cuando el mismo engaño es capaz de producir el riesgo de error en el destinatario o víctima[373].

2.6. Intervención delictiva

En cuanto ella, se debe tener presente el grado participación de las mismas, es decir los partícipes en el delito de estafa. En este caso cree que ver con la llamada autoría mediata, otro de la participación es posible hasta el momento de la

[373] ETCHEBERRY ORTHUSTEGUY, Alfredo, *Derecho Penal en la jurisprudencia*, tomo III, 3ª Edición, Editorial Jurídica de Chile, Santiago, 1987, págs. 411 y sigs. El autor indica, sir engaño era idóneo, con independencia de su descubrimiento, puede admitirse tentativa y frustración.

producción de perjuicio, y puede consistir solo recibir la cosa por dinero estafado, aún sin haber tomado parte en el engaño. Ahora bien en el caso del que engaña a otro para que entre un donativo de caridad por ejemplo, que recibe el donativo, está de acuerdo con el engañado, en un partícipe punible de la estafa, conforme a lo dispuesto en los artículos 15 N° 3 o 16, del Código Penal Chileno[374][375], según su grado de aporte al hecho.

2.7. Referencia a la llamada estafa residual del artículo 473 del Código Penal Chileno

Conocida como estafa residual, establece el elemento engaño como determinante en la actuación del sujeto activo del delito, ya que castiga el fraude cuando se usa de cualquier otro engaño no expresado en las otras normas legales, es decir esta figura exige defraudación o perjuicio a un tercero usando de cualquier engaño que no se haya expresado el artículo anteriores como indica el mismo código, los cuales tipifican y sanciona la estafa y otros engaños. De esta manera para que exista el injusto en estudio es esencial la existencia de engaño que de acuerdo a lo sostenido por el autor Etcheverry, no puede consistir en una mentira sino que una farsa inserta en un despliegue engañoso externo, requisito que rige para toda la hipótesis de estafa entre ellas contempladas en los artículos 468 y cuatro 473 del

[374] Artículo 15 del Código Penal Chileno. Se consideran autores: 1° lo que toman parte la ejecución del hecho, sea de una manera inmediata y directa; será impidiendo o procurando impedir que se evite. 2° Los que fuerzan o inducen directamente otro a ejecutarlo. 3° Los que, concertados para su ejecución, facilitan los medios con que se lleva a efecto el hecho o lo presencian sin tomar parte inmediata en él.

[375] Artículo 16 Código Penal Chileno. Son cómplices los que, no hallándose comprendidos en el artículo anterior, cooperan a la ejecución del hecho por actos anteriores o simultáneos.

código penal[376]. La doctrina indica, que la estafa contenida en dicho artículo, tiene su fundamento en evitar la impunidad de todo perjuicio causado por un engaño no

[376] SCS de Chile, Rol N° 5.259-2008, 25/ 08/2009. La cual nos indica es lo relevante al tema: Que de esta manera, para la existencia del injusto en estudio, es esencial la existencia de un engaño que de acuerdo a lo sostenido por la opinión dominante en Chile sobre la materia -cuyo máximo exponente es Alfredo Etcheberry- no puede consistir en una simple mentira, sino que en una farsa inserta en un despliegue engañoso externo, requisito que rige para todas las hipótesis de estafa, entre ellas las contempladas en los artículos 468 y 473 del Código Punitivo -disposiciones alegadas por el recurrente como violentadas-, preceptos que se distinguen entre sí sólo por la gravedad o despliegue escénico del engaño -lo propio del art. 468 sería el ardid, maquinación o mise en scéne- pero siempre a partir de ese umbral mínimo común, cuestión que aquí no se ha logrado comprobar. Undécimo: Que, con mayor exactitud, la doctrina apunta a que la estructura de la estafa reposa sobre la utilización de un engaño por el sujeto activo que por su naturaleza, entidad y circunstancias, sea suficiente para producir un error en el sujeto pasivo, induciéndole a realizar un acto de disposición en detrimento propio o ajeno. A su vez, es necesaria que entre el artificio y el acto de disposición exista un enlace causal de tal manera que haya sido el desencadenante del comportamiento del engañado y el causante del deterioro originado. Undécimo: Que, desde un punto de vista semántico, engaño es hacer creer a alguien con palabra o cualquier manera, una cosa que no es realidad. Desde una perspectiva jurídica, lo verdaderamente relevante no es si el agente desarrolla una conducta activa u omisiva, sino su idoneidad para producir el resultado lucrativo buscado. Es su eficacia real en el caso concreto lo que determina la aparición de la estafa. Es evidente que la provocación del error en las personas afectadas puede conseguirse, tanto por medio de una conducta activa o bien a través de ocultaciones de la realidad, que provocan la captación de la voluntad del ofendido. Décimo tercero: Que, bajo este prisma, la estafa no sólo requiere que el autor induzca al perjudicado, mediante engaño, a realizar una disposición patrimonial perjudicial, sino que además demanda que el error sea directamente imputable al artificio, es decir, que sea el motivo por el cual el engañado realiza el acto de disposición patrimonial. Por lo demás, no podemos preterir que el ilícito de estafa presenta una variadísima multiformidad, de tal manera que, en algunos casos, se trata de un acto simple y casi instantáneo, en el que coinciden, en un mismo momento temporal, la maniobra engañosa y la defraudación, y, en otros, nos encontramos ante una estructura compleja que tiene sus orígenes en un momento anterior a la perfección del hecho delictivo, pero que se consuma cuando el engaño surte el efecto de desplazamiento patrimonial buscado. Décimo cuarto: Que así la cosas, según ya se expresó, los hechos determinados en la instancia no cumplen todos los componentes que integran el tipo de la estafa, en sus dos modalidades denunciadas, esto es, relativa a la hipótesis general de este tipo de delitos, comprendida en el injusto del artículo 468 del Código Penal, o bien en su figura residual, relativa a lo preceptuado en el artículo 473 del citado Código, ya que en ambas disposiciones se requiere por una parte, de la presencia del elemento "engaño" relativo a la presencia de una mentira inserta en un despliegue engañoso externo, y por otra, de la necesaria relación de causalidad directa e inequívoca que debe existir entre las maniobras engañosas y la disposición patrimonial, cuya ausencia se divisa en el conjunto de actos ejecutados por los acusados, según han explicado los sentenciadores en sus considerandos tercero a séptimo -refrendando lo manifestado por el a quo en sus basamentos noveno a undécimo-, que los llevan a razonar fundadamente que no está justificada la existencia de los delitos atribuidos a aquéllos, y por ese motivo se les absuelve, de manera que el presente recurso no puede prosperar, pues es de la esencia de la causal invocada que la absolución provenga no de la circunstancia de no estar acreditados los hechos constitutivos del delito, sino de su mala calificación

considera oficialmente por el legislador. De allí que se hable también que se trata de una figura supletoria que tiene por objeto recibir en su seno el engaño que pudiere el legislador ha permitido en alguna excepción especial. Siendo la diferencia fundamental en la naturaleza de los engaños a que hace referencia tanto el artículo 468 como el artículo 473 ambos del código penal chileno, la cual estriba en la potencialidad y deudor de los mismos, siendo de mayor entidad y fuerza el comprendido en la primera disposiciones legales; y de menor vehemencia el considerado la segunda. Asimismo requiere al mismo tiempo un despliegue mayor de artería en la figura penal del artículo cuatro 68 y menor tamaño en el artículo cuatro 73, siendo común en ambas normas el desarrollo psicológico intrínseco, entre víctima y víctima, de inducir a error a la víctima con el fin de que se despoje voluntariamente de la cosa o bien jurídico que meten del autor del delito y que causa un perjuicio ilícito al ofendido[377].

A manera de conclusión, y tomando en consideración que lo anteriormente expuesto es un barniz del tipo penal de estafa básica en Chile, sin embargo se puede destacar que el tipo penal de estafa clásica en Chile, tiene problemas en la técnica legislativa tanto él interpretación como donde se ubican los tipos penales en el mismo código, no entregando dicho código una definición general de estafa, sino que lo que hace es entregar ejemplos de la misma, o elaborando hipótesis de dicha conducta. En general es un delito de autolesión contra el patrimonio, donde la jurisprudencia se ha encargado de desarrollar sus elementos típicos, a saber, engaño, error, disposición patrimonial y el perjuicio con variantes. La teoría de la puesta en

jurídica, al considerar que no están sancionados penalmente o que no encuadran en alguna de las figuras delictivas contempladas en la ley.

[377] SCA San Miguel, Santiago de Chile, 16/ 08 /1993, Gaceta Jurídica, año 1993, Vol. 159, págs. 115, MAGLIONA MARKOVITH, Claudio / LÓPEZ MEDEL, Macarena, *Delincuencia y fraude informático*, 1 ª edición, Editorial jurídica de Chile, Santiago, 1999. citada por el autor págs. 218 y sigs.

escena o *mise en scene*, o ardid por parte del autor, se toma en cuenta el elemento engaño para qué se configure el tipo penal de estafa, no siendo suficiente que el error en la víctima se haya producido mediante una mentira o engaño, es decir además de la mentira en necesario que existan en el caso concreto los demás elementos de la estafa. Ahora bien, en cuanto al ánimo de lucro, se dice que como elemento subjetivo para configurar el tipo penal de estafa no sería necesario, a pesar que la jurisprudencia lo agrega, en contra de la doctrina.

Todos éstos aspectos, son relevantes para comprender a su vez el delito estafa informática en Chile, puesto que tienen directa relación con los elementos generales del tipo en cuestión, por lo mismo en el apartado siguiente se estudiará derechamente, este tipo de delito informático el cual podemos adelantar que en Chile tiene bastantes problemas de aplicación, puesto que la ley que regula los delitos informáticos, a pesar de ser una de las primeras que nacieron al mundo jurídico en Iberoamérica, no ha tenido ninguna reforma hasta el momento, teniendo que la jurisprudencia y la doctrina, adecuar la legislación existente tanto especial como general, para poder hacer efectivo de alguna manera el delito de estafa informática, debiendo la judicatura tener en consideración, para poder dar solución a los casos donde existe esta estafa especial en conjunto todos los elementos del tipo penal de estafa, junto con las demás herramientas legislativas que existen en Chile.

B) Tratamiento delito de estafa informática en Chile

1. Planteamientos

En primer lugar se debe señalar que la fraude informático en Chile no encuentra específicamente regulado, por lo mismo no seguiré el orden correspondiente respecto del tipo penal especial, sino que se entregarán breves consideración de la legislación Chilena, sobre la materia, deteniéndose en las más relevantes que tengan relación con la estafa, con el que se pueda obtener una visión general del tema.

En Chile, ingresó la ley a la Cámara de Diputados 16 de julio de 1991, siendo promulgada el 28 de mayo 1993, siendo ya ley de la República, publicada el 7 de junio del mismo año, generándose la *ley que tipifica las figuras penales relativas a la informática*, N° 19.923[378], siendo la primera norma legal nacional y también en Latinoamérica que regula los delitos informáticos, prefiriendo entonces el legislador chileno, regular este tipo de ilícitos en una ley especial, no incorporándolos al Código Penal propiamente tal. A pesar que significó un gran avance, la informática no se había desarrollado hasta como la echo los días de hoy, y además es dable hacer presente que el año 1995[379], la informática en un avance de suma importancia, y por

[378] Ley N° 19.923, *Tipifica figuras penales relativas informática*, Valparaíso, 7 de junio de 1993, Chile. "Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo. Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio. Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio. Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

[379] Navegador web desarrollado originalmente por la compañía Netscape Communications. Netscape fue el primer navegador comercial popular en 1995 y principal rival de Internet Explorer de Microsoft. Al perder la batalla contra Internet Explorer, decidieron liberar el código fuente de Netscape. Gran cantidad de colaboradores reescribieron el código y crearon Mozilla. Netscape dejó de desarrollarse el primero de febrero de 2008, debido a que no logró incrementar su cuota de mercado. Disponible:<www.alegsa.com>.

ende también en la generación delitos informáticos puesto que ingresa al mercado el navegador *Netscape,* y con el también nace la *World Wide Wed.* A pesar que hoy en día la tecnología es parte habitual de la mayoría las personas, esta ley sólo se enfoca en situaciones de espionaje, siendo actualizada únicamente en el año 2005, para regular los ilícitos relacionados con las tarjetas de crédito y débito.

Como se ha venido relatando, al igual que el resto de los países el desarrollo tecnológico ha posibilitado el empleo de inteligencia artificial, sistemas automatizados de tratamiento de la información, para todo tipo de administración contable y financiera, con el fin de entregar bienes y servicios, es decir donde antes existía un ser humano, hoy existe una máquina, siendo internet un fenómeno transnacional. La tecnología ha cambiado, sin embargo en el caso de Chile la legislación a pesar que fue pionera, no ha vuelto a innovar en la materia, quedando todos los procesos informáticos bajo la mira del ciber-delincuente.

Conforme a la legislación vigente en Chile, no existe una definición de delito informático en la ley precitada, sin embargo por su nombre, que tiene por fin amparar los datos informáticos en los sistemas que los contienen y no hacerse cargo de las vías tecnológicas como medio de comisión de delitos comunes[380]. De acuerdo lo anterior, al referirse el legislador chileno ha delito informático, se refiere a la protección mediante el derecho penal de los datos sistema informático, siguiendo el concepto de delito informático sostenido por la ONU, es decir más restringido.

[380] Conforme la historia documentada de la ley, en la moción parlamentaria que se dio origen al proyecto de ley, se expresa que la legislación debería proteger esa no bien jurídico que surge con el uso de las modernas tecnologías computacionales, (la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan), con mención expresa del cuidado de la información en cuanto tal ya la falta de referencias fenómeno delictivo por medios informáticos. LARA, Juan / MARTÍNEZ, Manuel, *Hacia una regulación de los delitos informáticos basada en la evidencia*, Revista chilena de derecho y tecnología, Vol. 3 núm. 1, 2014, 108.

1.2. Razones de la falta de regulación legal de la estafa informática en Chile

Existen varios autores, que indican que el fraude informático no fue incorporado a la ley antes indicada, puesto que se basan en la historia fidedigna de su establecimiento. De esta manera, cuando se discutió dicha ley habiendo indicaciones de otros parlamentarios y también del ministro justicia de la época, que tenían por fin incorporar en dicha legislación el llamado fraude informático, no fueron escuchadas o acogidas por la comisión de trabajo, encargada de la redacción de la misma[381].

Según se puede extraer del boletín oficial, la negación se basaba en que la solución era por una reforma al código penal incorporando dichas figuras dentro de la propiedad estafa. Además otra posición en contra señalaba que sí, se encontraría tipificado el fraude informático, en la Ley N° 19.223, específicamente en su artículo 3°, postura que no tenía mayor fundamento. Y por último, la ley Chilena tuvo su origen en la legislación francesa, que data de 1988, y a pesar que tiene es relativa al fraude informático, no tiene relación con lo regulado, es decir no lo trata, por ello al basarse en dicha ley, se omitió también en la Chilena, sin antes mencionar que en aquellos años, recién estaba irrumpiendo la red en todo el mundo, por ende el desconocimiento de la materia y su alcance era evidente. Además de las razones anteriores el legislador Chileno no dimensionó, los inmensos avances de la

[381] En Chile existen comisiones encargadas del estudio, y presentación de informes respecto de cada ley que se promueve, para que posteriormente sean aprobado por la cámara de Diputados y el Senado.

informática, y todo lo relacionado con el internet, debiendo todos los operadores jurídicos hacer esfuerzos en todo ámbito, para que alguna manera se investigue y sancionen los delitos informáticos, especialmente en cuanto al fraude se refiere.

1. 3. Fraude informático en Chile

Cuando se habla de estafa, como anteriormente se ha señalado se supone siempre que existe la persona engañada, y que además sea inducida a un error que le lleva realizar un acto de disposición patrimonial con carácter ilícito, sin embargo cuando estamos hablando de estafa informática en el sentido de manipulación, la realidad nos indica que no se puede engañar a un ordenador, el engaño supone entonces una relación psicológica entre el agente y el sujeto engañado.

En cuanto a Chile se refiere, al entender el fraude o estafa como un *engaño*, que produce un error, y que a su vez tiene como consecuencia una disposición patrimonial que resulta perjudicial, no cabe plantear la tipicidad del engaño a la máquina, puesto que el error se ha tratado como un fenómeno psicológico. En consecuencia, el error sólo puede predicarse del ser humano, lo que viene a significar que sólo él mismo, puede ser engañado típicamente, concluyendo entonces algunos autores con la atipicidad al menos a título de estafa de toda conducta que, valiéndose de cualquier manipulación o artificio aplicado sobre el sistema informático, acarree un perjuicio patrimonial para el tercero. Ahora bien la Ley N° 19.223 *sobre delitos informáticos*, por la indirecta vía de la sanción a la alteración de datos que indican su artículo tercero o la obstaculización o modificación del funcionamiento un sistema informático en su artículo uno, incrimina aunque posiblemente sin haberlo buscado, la gran mayoría de la conducta recién aludidas.

Sin embargo se hace cargo de manera inadecuada, excesiva, prescindiendo del resultado. En efecto, la ley mencionada sanciona los medios comisivos, las manipulaciones informáticas, pero no el resultado, es decir la cuestión del bien jurídico afectado, así, resulta que qué alterar datos.

En Chile, existen posiciones contrapuestas respecto de las conductas relacionadas con el fraude informático deben ser sancionadas, por la norma que regula el delito de estafa del artículo 468 del código penal chileno[382], sin embargo se presenta la dificultad que aquella conducta defraudadores realizada por medios informáticos, en sistemas de tratamientos automatizados de la información cuando no existen personas en su control o con accesos de persona puramente mecánicos[383]. Entonces, a diferencia de otros países, en Chile se ha utilizado la figura de la estafa clásica, adecuándola a nuestros tiempos, sin embargo ha sido totalmente cuestionada, discutiéndose que el delito de fraude contemplado en el código penal sería inadecuado, en virtud del principio de tipicidad, para sancionar algún tipo de fraude informático[384].

[382] Artículo 468 Código Penal de Chile: "el que defraudaré a otro usando de nombre fingido, atribuyéndose poder, influencia o créditos supuestos, aparentando bienes, créditos, Comisión, empresa o negociación imaginarios, o valiéndose de cualquier otro engaño semejante".

[383] En el marco de un procedimiento abreviado, en un caso de *phishing*, y con conductas desplegadas tanto en Chile como en el extranjero, siendo la modalidad en que el acusado con ánimo de apoderarse y usar la información contenida en un sistema de tratamiento de información, esto es, datos de cédulas de identidad, claves y cuentas bancarias accedió a dicho sistema , para lo cual creo una página web falsa que simulaba ser del Banco Santander, la envió mediante correos a varios cuentacorrentistas y estos bajo engaño ingresaron sus claves y datos, datos que por programación previa efectuada a la página por el acusado le eran enviados a su correo y con los cuales pudo efectuar transferencias de fondos a otras cuentas perjudicando a las víctimas . Se estimó por parte del ente acusador que en este caso se configuraban dos delitos informáticos del artículo 2 de la Ley N º 19223 y dos delitos de estafa del artículo 468 en relación al 467 N º 2 del Código Penal, ambos consumados y atribuyendo al acusado participación de autor, calificación que fue compartida por el tribunal estableciendo al efecto relación concursal medial entre los delitos informáticos y las estafas. Sentencia, Juzgado de Garantía de Concepción, Chile, RIT: 2294, 13. IV. 2010.

[384] Alteración de tarjetas de prepago por parte de personal de recaudación de dinero, los cuales fueron condenadas por alteración de sistema informático delito de Estafa del artículo 468 y

Tomando en cuenta, lo anteriormente analizado, respecto del fraude informático y la estafa informática en una relación de género a especie, la opinión mayoritaria, es que en Chile no existe regulación adecuada y vigente que se haga cargo de la estafa informática propiamente tal, pudiendo mencionar la opinión del profesor BALMACEDA HOYOS[385], el cual indica que tomando consideración el avance de los medios tecnológicos informáticos, en la actualidad, la naturaleza especial y además el componente transfronterizo, y al no existir texto expreso, que regule la materia, solamente podría aplicarse el delito de estafa en su modalidad tradicional, pues para dicho autor se pueden sancionar dicha defraudaciones por medios informáticos a través de esta figura, pero recordando que debe existir una legislación adecuada de acuerdo a estos tiempos.

Por otro lado, MAGLIONA MARKOVICH y LOPEZ MEDEL[386], nos indican que igualmente se reconoce la solución chilena inicialmente subsumir la estafa informática en la estafa propiamente tal o básica, sin embargo ello ha sido descartado en derecho comparado, llegando a la misma conclusión en el sentido que no puede ser sancionado penalmente la estafa informática toda vez que la ley en comento no lo comprenden forma expresa no pudiendo aplicarse en forma supletoria la figura de la estafa clásica. Argumentando también que el engaño y su consiguiente error, elementos propiamente característicos de la estafa básica, sólo pueden ser limitados al ámbito de las personas naturales, por el elemento psicológico que subyace a ello, no pudiendo aplicar dicho elemento a los fraudes informáticos, salvo en aquellos casos en que el ordenador no es más que un medio

467 N° 2, del Código Penal Chileno, en concurso medial con el delito Informático del artículo 1º de la Ley Nº 19223, Sentencia, TOP de Curicó, RIT: 81 acumulado a 86-2010, 07. III. 2010.

[385] BALMACEDA HOYOS, Gustavo, *Estafa informática*…op. cit. pág. 47.

[386] MAGLIONA, Claudio / LÓPEZ, Macarena, *Delincuencia y fraude informático*, Editorial jurídica de Chile, Santiago, 2010. pág. 244.

auxiliar en la toma de decisiones, es decir el engañado sería la persona que usa el medio auxiliar para tomar la decisión posterior de disposición patrimonial, no pudiendo entonces engañar a una máquina. Agregan dichos autores, que ninguna de las figuras tipificadas en la ley se puede apreciar la dinámica defraudador ya que suponen las conductas consecutivas del fraude informático, puesto que la defraudación informática tiene que tener previamente las notas configuradores de una defraudación, agregando que se puede distinguir el fraude informático de otros hechos delictivos que, no obstante ser realizado por medios informáticos, no constituyen defraudaciones, como por ejemplo sabotaje informático espionajes informáticos[387][388].

1.4. Ley N° 19.233 (delitos informáticos Chile)

La misma ley analizada, ha sido objeto de bastantes críticas como por el hecho de ser una materia que está fuera del código penal, puesto que el sistema penal chileno esencialmente codificado. Además de ello, vendría siendo un freno a la modificación del Código penal, debiendo haber complementado las figuras clásicas como ocurre en el tipo estafa básico, tal cual lo hizo España, lo cual resulta en una legislación más acorde a los tiempos y coordinada entre sí. Por otro lado, a pesar que dicha ley fue la primera en Latinoamérica, su forma de redacción y las referencias que hace sus artículos a distintos términos informáticos hace que sea

[387] MAGLIONA, Claudio / LÓPEZ, Macarena, *Delincuencia y fraude informático*…op. cit. pág. 244 y sigs.

[388] GUTIÉRREZ FRANCÉS, María luz, *Fraude informático y estafa*, Editorial 1ª Edición, Editorial Ministerio de Justicia, Secretaría técnica, Centro de publicaciones, Madrid, 1996, pág. 229 y sigs.

confusa y difícil su aplicación, por ejemplo al confundir el software con el hardware, ya además al referirse a sistema de tratamiento del información, sin referirse a un sistema automatizado, el cual no requiere para que funcione el manejo de un ser humano.

Por último, la ley no da el ancho suficiente para convertir el delito informático especialmente lo que se trata a fraude informático, existen entonces un vacío legal imposibilitándose con ello la sanción del delito en cuestión, debiendo tanto los tribunales como los operadores jurídicos tener que usar el articulado referente al delito de estafa contenido en el Código penal, el cual como ya se ha venido señalando no se condice con los elementos de la estafa informática.

1.5. Breves comentarios de la Ley N° 20.009, que regula o limita la responsabilidad de los usuarios de tarjetas de crédito y débito

Esta Ley responde a una necesidad, legislativa puesto que debía entregar protección al usuario, tanto como respecto del hurto, robo o extravío de dichos medios de pago, y además tratar el uso fraudulento de las mismas. Dicha ley, contiene cinco artículos, siendo el artículo 5[389], el que se hace cargo del uso

[389] Artículo 5: Las siguientes conductas constituyen delito de uso fraudulento de tarjeta de crédito o débito: a) Falsificar tarjetas de crédito o débito. b) Usar, vender, exportar, importar o distribuir tarjetas de crédito o débito falsificadas o sustraídas. c) Negociar, en cualquier forma, con tarjetas de crédito o débito falsificadas o sustraídas. d) Usar, vender, exportar, importar o distribuir los datos o el número de una tarjeta de crédito o débito, haciendo posible que terceros realicen operaciones de compra o de acceso al crédito o al débito que corresponden exclusivamente al titular. e) Negociar, en cualquier forma, con los datos o el número de la tarjeta de crédito o débito, para las operaciones señaladas en la letra anterior. f) Usar maliciosamente una tarjeta bloqueada, en cualquiera de las formas señaladas en las letras precedentes. La pena por este delito será de presidio menor en cualquiera de sus grados. Esta pena se aplicará en su grado máximo, si la acción realizada produce perjuicio a terceros. Ley 20.009. *Limita la responsabilidad de los usuarios de tarjetas de*

fraudulento de tarjeta de crédito. Este tipo penal es abierto, en cuanto la posibilidad de ejecución, puesto que son casos de sanción directa a la delincuencia informática o indirecta cuando existen reglas concursales conjuntamente con la aplicación de la Ley que regula los delitos informáticos en Chile N° 19.223. Por último, en el caso del uso fraudulento de tarjeta de crédito, regulado en el artículo quinto, como es un delito de mera actividad, no requiere consumación para la existencia de perjuicio, sólo los elementos se toman cuenta para aplicar la pena.

1.6. Proyectos de modificación Chilenos[390]

Por último, existen dos proyectos de ley que proponen modificar la Ley Chilena primero[391] que pretende modificar la ley N° 19.223, que tipifica figuras penales relativas a la informática, y segundo[392], destinado a introducir modificaciones al código penal de agregar nuevas figuras. Dichos proyectos, están en tramitación en forma conjunta con la idea de incorporar los tipos penales tanto a la ley de delitos informáticos como el Código penal de agregar nuevas figuras penales. Entonces, se trata de agregar al código penal las figuras penales de la ley

crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas, 01 de abril de 2005.

[390] Boletín N° 412-07, Segundo informe de La Comisión De Constitución, Legislación, Justicia y Reglamento, recaído en el proyecto de ley, en segundo trámite constitucional, sobre delito informático.

[391] Boletín número 2974-19, destinado a reformar la actual Ley N° 19.223. Accesible: <http://www.bcn.cl>.

[392] Boletín número 3083-07, destinado a introducir modificaciones al código penal, año 2002. Proyecto de ley a cargo del Ministerio de Justicia y la Subsecretaría de Telecomunicaciones. Accesible: <http://www.bcn.cl>.

19.223, adaptándolas a las figuras penales tradicionales de agregar el acceso no autorizado información contenía sistemas computacionales, es decir *hacking*. Del mismo modo se incorpora el tipo de acceso indebido, adecuar los tipos de sabotaje informático, alteración de datos y apoderamiento de información y además agregar también penas pecuniarias. También penaliza otros distintos delitos informáticos como son la falsificación de documento electrónico; la clonación de alteración tarjetas de crédito; los fraudes cometidos por medios informáticos y la obtención ilegítima servicio de telecomunicaciones, propiciándose regular el mismo código penal y no leyes especiales. Es dable señalar que los proyectos de ley que modifican la ley delito informático y el código penal, también aborda la clonación de celulares, el acceso a señales satelitales cifras sin pagar, y la obtención ilegítima de señal de televisión por cable o mediante cualquier maniobra técnica que permita neutralizar, eludir o burlado mecanismo de control del legítimo acceso servicio. Del mismo modo existe la hipótesis del uso de la moneda falsa en teléfonos públicos, y la creación del decodificador o el uso donde codificado no autorizado en caso de servicio de televisión por cable satelital. Igualmente existen aspectos del derecho nacional privado como son las reglas de competencia internacional, los exhortos internacionales y la extradición, todo ello con el fin de propender a la regulación sustantiva de los delitos y los aspectos procesales de cooperación judicial internacional como sería el caso de adecuar la materia a la convención sobre la ciberdelincuencia de Budapest.

CAPÍTULO VI

Referencias al tipo tradicional o básico estafa

y la estafa informática en España

I. Planteamiento

La estafa constituye hoy en día unos de los delitos de mayor ocurrencia, no existiendo un concepto único en la distintas legislaciones, puesto que las formas de la misma puede ser muy variadas, que van de la mano con la creatividad del delincuente, que usa para valerse de la víctima para después defraudar y que además debe existir siempre un mínimo de confianza entre sujeto activo y la víctima. Para tener una visión mucho más clara la materia, se aplicará en forma breve o en lo medular lo que concierne a la estafa tradicional o propiamente tal que rige en el Código Penal Español.

La palabra *estafa* proviene del italiano *staffa* que significa estribo. Originalmente, estafa o estafar significaba pedir algo prestado, si la intención de devolverlo. A su vez, antiguamente la estafa era el ardid que una persona utilizaba para pedir prestado su caballo. Entonces, ese ardid, servía como *estribo,* para subirse al caballo ajeno. Si bien la *staffa,* es estribo, de la raíz germánica *stap,* el sentido de estafa y estafar viene del verbo *staffare,* que propiamente era sacar el pie del estribo un jinete por ende al estafado se le deja económicamente falso como el jinete que queda en esa posición y sin apoyo, vinculándolo también a la raíz indoeuropea, *stebh,* que vendría siendo apoyar o aguantar. Se sostiene que cronológicamente, que

el precedente de la buena estafa en la figura delictiva crimen *stellionatus*, derivado de las voces *stellio* y *onis* con que se designaba el estelión o salamanquesa, a lo cual Carrara, propone explicar la cuando nota que teniendo este animal colores y definibles, por su variabilidad a los rayos solares, se aludía así a la multitud de hechos cometidos en daño de la propiedad que fluctúan entre la falsedad y el hurto, participando de las condiciones de la una y del otro, sin ser propiamente ni lo uno ni lo otro quizás, también creyéndolo una particular astucia del animal, correspondiendo entonces que la figura del estelionato, es una representación metafórica[393].

II. Tipo básico o tradicional de estafa

A) Antecedentes históricos

El primer cuerpo jurídico a mencionar, es la partida VII, del título XVI que reglamenta la figura delictual de la estafa bajo el epígrafe *engaños*, sin embargo el delito no es denominado estafa ni comprendido de modo genérico entre los que importan falsedades. Según las partidas los engaños, se pueden realizar distintas maneras como por ejemplo, cuando el engaño se hace por palabras mentirosas arteras, o cuando se pregunta algo a algún hombre sobre una respectiva cosa y él calla engañosamente, no respondiendo o si responde lo dice con palabras distintas son cubiertas. Con estas fórmulas se admite el engaño por omisión, asimismo se distinguía entre la simulación y la disimulación en los delitos de acción. Igualmente

[393] YUBERO CANEPA, Julio, *el engaño en el delito de estafa, doctrina y jurisprudencia*, 2 Edición, Editorial jurídica Cruz del Sur limitada, Chile 2010, págs. 21.

las partidas se referían a los engaños buenos y malos como ocurría en el derecho romano. Otra semejanza con el derecho romano que las partidas no consignar una definición general de engaño, incluyendo en sus distintas leyes sólo especies concretas a fin de *que los hombres puedan tomar apercibimiento para guardarse y los juzgadores puedan conocerlo y en escarmentarlos.*

Ahora bien dicha casuística de las partidas no era siempre completa porque la calificación del hecho específico quedaba entregada al criterio del juez, lo mismo ocurría con la consecuencia jurídica del delito, la pena. Carrara[394], sostiene que este sistema era el más plausible porque habría sido vano el afán de enclaustrar en inventario taxativo sus las diversas y múltiples especies de engaños, sin embargo, es de anotar que ya los tiempos de Carrara, las tendencias legislativas se dirigen a la formulación de un concepto de carácter general.

Haciendo un salto cronológico, hasta el Código Español de 1822, inspirado en el código francés vigente la época tradujo la *escroquerie*[395] por estafa, pero adicionó el epígrafe del capítulo perteneciente los engaños (Parte II, capítulo V del título III); la fórmula *de las estafas y engaños* que ha prevalecido los código posteriores con ligeras variantes. En la terminología de este código, los engaños son concebidos como una figura supletoria de otras infracciones, es decir cualquiera que con algún artificio engaños superchería hubiera sonsacado a otros dinero, efectos o escrituras o le hubiere perjudicado de otra manera en sus bienes, sin existe alguna

[394] Citado por YUBERO CANEPA, Julio, *el engaño en el delito de estafa, doctrina y jurisprudencia,* 2 Edición, Editorial, jurídica Cruz del Sur limitada, Chile 2010, págs. 25. Francesco Carrara "Programa del Corso delito informático Ditrito Penale". Parte especial Vol. IV N° 2336, 9° edición, Florencia, 1923.

[395] Escroquerie, traducido al español: estafa. También: calote, timo. Portal lingüístico bab.la en su plataforma online Oxford Dictionaries, en filial de Oxford University Press. Responsabilidad de contenido conforme a § 6 MDStV (ley alemana). [en línea] <https://www.es.bab.la/diccionario>.

circunstancia que le constituya verdadero ladrón, falsario o reo de otro delito especial[396].

Posteriormente se dictó el Código de 1848, donde se puede indicar como característica su sistema casuístico con una mecanización de la penalidad distinta a la anterior queda proporcionada la cuantía de la defraudación. En este orden, nace el Código de 1870, que no alteró el régimen en forma muy importante, sin embargo el Código de 1928, amplió el epígrafe del capítulo a *delito de estafa, chantajes y otros engaños* dicho código introdujo nuevas figuras y determinó forma muy prolija otras ya consagradas, mediante la inclusión de frases explicativas procedentes de la jurisprudencia.

En 1932, el Código dictado en dicho año del oso de la estafa y otros engaños el abuso de la impericia o pasiones de un menor a raíz de esta reforma esta figura fue insertada entre las correspondientes al delito de usura, distinguiendo también dicho Código entre falta y el delito, cediendo Código de 1932 el paso en la esfera normativa al de 1944, el cual en lo medular, agrava la pena correspondiente la cuantía superior; admite la conversión de la falta en delito por efecto de la reincidencia; forma sección aparte con la apropiación indebida que, en sistema anterior, estaba prevista entre las estafas, dedicando también sección aparte a las defraudaciones de fluido eléctrico y otras análogas. Siendo este último código el que perfecciona la reglamentación de las anteriores.

El concepto estafa, se acuña por primera vez en el Código de 1822, donde existía un catálogo de medios comisivos en su artículo 766[397]. Posteriormente las

[396] Citado por YUBERO CANEPA, Julio, *El engaño en el delito de estafa, doctrina y jurisprudencia,* 2ª Edición, Editorial jurídica Cruz del Sur limitada, Chile 2010, págs. 25

[397] Código Penal Español de 1822, artículo 766: cualquiera que con algún artificio, engaño, superchería, practica supersticiosa y otro embuste semejante, hubiese perjudicado de otra manera en

formas comisivas cambiaron a tres en el Código de 1848 y nueve en el artículo 548 del código de 1870, por último sólo a 529 en el código de 1944.

La definición de estafa fue incorporada en el artículo 528 del código de 1944 definición acuñada por Antonio Oneca[398], la cual indicaba *la conducta engañosa, con ánimo de lucro, propio o ajeno, que, determinando un error en una o varias personas, les induce a realizar un acto de disposición consecuencia del cual es un perjuicio en su patrimonio o en el de un tercero.* Con la ley de 1983, se obvia con la introducción, en una nueva configuración del artículo 528, de una definición esencial estafa, que pueda vender los diferentes supuestos planteados, el cual señala *cometen estafas los que con ánimo de lucro utilizan engaño bastante para producir error en otro, induciéndole a realizar un acto de posesión en perjuicio de sí mismo o de un tercero.* Ahora bien en el artículo 248 del código penal de 1995, creado por la ley orgánica 10/1995, de 23 de noviembre del mismo año, la cual trae un 2°, tomando la estafa mediante manipulaciones informáticas o artificio semejante, entregando algo de solución al problema que se tiene al momento de tener que calificar la estafa con engaños producidos a máquinas[399].

---

sus bienes, sin alguna circunstancia que el constituyere en verdadero ladrón, falsario o reo de otro delito especial.

[398] ANTÓN ONECA, José (1897-1981) Catedrático de Derecho Penal de la Universidad de Salamanca y, posteriormente, de la Universidad de Madrid. Perteneció a la escuela del Jiménez de Asúa al que consideró su mejor profesor, colaborando en la elaboración del Código Penal Español de 1932.

[399] STS, Sala 2ª de lo Penal, N° 328, de 5. V. 2015, (Ponente: José Ramón SORIANO SORIANO) / SAP de Madrid, Sección 2ª, N° 782 de 23 IX. 2015 (Ponente: María Del Rosario ESTEBAN MEILAN). Amas sentencias definen estafa como *un artificio creado por alguien con objeto de hacer pasar por cierta una situación que no lo es, como forma de inducir a error a otro que, en virtud de la aceptación de tal apariencia como real, dispone de algún bien a favor del primero, que se enriquece ilícitamente, con el consiguiente perjuicio patrimonial para el segundo.*

El Código actual, tratar la estafa de la sección primera, del capítulo VI, el cual trata sobre las defraudaciones del título XIII donde se hace cargo de los delitos contra el patrimonio y contra el orden socioeconómico del libro segundo; a su vez el capítulo queda integrado por tres secciones dedicadas a las estafas, la apropiación indebida y las defraudaciones de fluido eléctrico y análogas. La sección primera ha sufrido dos reformas, una por la Ley Orgánica 15/2003, de fecha 25 de noviembre de 2003 la cual vino a modificar los artículos 248 y 249, de esta manera trató la punición de la fabricación, introducción, posesión y facilitación de programas de ordenador destinados a la Comisión de estafas. Y la segunda ley que vino a modificar dicha sección fue la Ley Orgánica 5/20010, de 22 de junio de 2010 modificando los artículos 248 y 250, asimismo también incluyendo un nuevo artículo 256 bis el cual sanciona más enérgicamente la responsabilidad penal de las personas jurídicas que cometen delito de estafa, es creando el tipo penal también, de la mal utilización de tarjetas de crédito o débito o cheques de viaje, o sus datos, para la realización de operaciones fraudulenta. Por otro lado, existe un anteproyecto de octubre de 2012 el cual contempla la modificación de la Ley Orgánica, 10/de 23 de noviembre 1995, así las cosas se divisa la derogación del libro tercero relativo a las faltas modificando en consecuencia el artículo 249, es considerando la estafa como delito, con independencia de la cuantía de lo defraudado, aunque también toma un tipo atenuado o delito leve, en atención a las circunstancias que describe, el hecho fuera escasa gravedad, se impondrá la pena de multa de uno a tres meses sin que puedan considerarse de escasa gravedad los casos en los que el valor de la cantidad defraudada fuera superior a €1000. Es dable señalar las agravantes del artículo 250, incluyéndose un numeral nuevo 1 uno es uno. En 1.4° *cuando se cometa por un miembro de una organización constituida para la Comisión continuada del delito de falsedad estafa, por el autor actúe con profesionalidad. Existe profesionalidad cuando el autor actúe con el ánimo de proveerse de una fuente de ingresos no meramente ocasional,* Añadiéndose entonces otra agravante la cual tendría por fin o

se aplicaría cuando afecte a un elevado número de personas y por último una grabación más rigurosa cuando estamos en presencia de un valor de defraudación que supere los €250,000. Introduciendo por último un nuevo artículo 252 bis, el cual vendría a indicar que los condenados por la comisión de uno o más delitos comprendidos, en este capítulo se les podrá imponer además una medida de libertad vigilada.

B) Definición

El Código Penal, establece una serie de elementos para determinar si existe estafa o no, aunque como lo indicó anteriormente una de las definiciones más claras la entregó Antón Oneca, siendo similar a la que se encuentra hoy en la ley, de esta manera el artículo 248.1 del Código Penal Español, nos indica *que cometen estafa, lo que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno,* estableciendo una serie de requisitos para que se configure el tipo penal.

El artículo en comento, continúa indicando *también se consideran reos de estafa: a) los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) los que fabricaren, introducir, poseyeren o facilitaren programas informáticos especialmente destinados a la Comisión de las estafas previstas en este artículo. c) los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.*

Los elementos, que entrega el artículo recién indicado, o las pautas que el mismo establece también son establecidos por el Tribunal Supremo, en reiteradas oportunidades como ocurre con la sentencia número 187/2002, de 8 de febrero de 2002 de la segunda sala en lo Penal[400], en la cual se establecen los elementos del tipo, del cual se hace referencia, de igual manera en una sentencia más reciente se

[400] La sentencia indica lo siguiente: los elementos del delito de estafa hay que numerar: 1) un engaño procedente o concurrente, espina dorsal, factor nuclear, alma y sustancia de la estafa fruto de ingenio falaz y maquinador de los que tratan de aprovecharse del patrimonio ajeno. 2) dicho engaño ha de ser bastante, es decir, suficiente y proporcional para la consecución de los fines propuestos, cualquiera que sea su modalidad en la multiforme y cambiante operatividad en que se manifieste, habiendo de tener adecuada entidad para que en la convivencia social actúe como estímulo eficaz del traspaso patrimonial, debiendo valorarse aquella idoneidad tanto atendiendo a módulos objetivos como en función de las condiciones personales del sujeto afectado y de las circunstancias todas del caso en concreto; es la maniobra defraudador ya ha de revestir apariencia de seriedad y realidad suficiente: la idoneidad abstracta se complementa con la suficiencia en el específico supuesto contemplado, el doble módulo objetivo y subjetivo desempeñarán su función determinante. 3) orígenes acción o producción de un error esencial en el sujeto pasivo, desconocedor o con conocimiento deformado un exacto de la realidad, por causa de la insidia, mendacidad, fabulación o artificio de la gente, lo que lleva a actuar bajo una falsa presuposición de admitir una manifestación de voluntad partiendo de un motivo viciado, por cuya virtud se producen traspaso patrimonial. 4) acto de disposición patrimonial con el consiguiente correlativo perjuicio para el exponente, es decir, que la lesión del bien jurídico tutelado, el daño patrimonial, sea producto de una actuación directa del propio afectado, consecuencia del error experimentado y, en definitiva del engaño desencadenante de los diversos estadios del tipo; a tu disposición fundamental en la estructura típica de la estafa que ensambla o conecta la actividad engañosa y el perjuicio rogado, y que ha de ser entendido, genéricamente como cualquier comportamiento de la persona inducir a error, que arrastro conlleve de forma directa la producción de un daño patrimonial a sí misma un tercero, no siendo necesario que concurran en una misma persona la condición de engañado y de perjudicado. 5) ánimo de lucro como elementos subjetivos del injusto, exigido hoy de manera explícita por el artículo 248 del código penal entendido como propósito por parte del infractor de abstención de una ventaja patrimonial correlativa, aunque no necesariamente equivalente, al prejuicio típico ocasionado, eliminándose, pues, la incriminación a título de imprudencia. 6) nexo causal o relación de causalidad entre el engaño provocado y el perjuicio experimentado, ofreciéndose éste como resultante del primero, lo que implica que el dolo de la gente tiene que anteceder o ser concurrente en la dinámica recaudatoria, no valorándose penalmente, en cuanto el tipo de estafa se refiere, el "dolo subsequens", es decir, sobrevenido no anterior a la celebración del negocio de que se trate; aquel dolo característico de la estafa supone la representación por el sujeto activo, consciente de subordinación engañosa, de la consecuencia de su conducta, es decir, la inducción que alienta al desprendimiento patrimonial como correlato del dolor provocado, y el consiguiente perjuicio suscitado en el patrimonio del sujeto víctima, secundado de la correspondiente voluntad realizativa".

pueden extraer también las pautas que nos entrega dicho artículo así en la sentencia del Tribunal Supremo número 465/2012, de fecha 1 de junio de del mismo año[401].

Es dable, antes de dar una breve reseña sobre los elementos del tipo de estafa básico, entregar de manera general la diferencia entre el ilícito civil y el delito de estafa, diferencia que servirá para poder del entender y explicar la estafa informática, de esta manera para entender la línea divisoria entre el dolo Penal del dolo civil en los delitos contra el patrimonio, se sitúa la tipicidad, de esta manera si la conducta del agente se enmarca en el precepto penal tipificado del delito estafa, es punible la acción, no suponiendo que debe de vamos criminalizar todo incumplimiento contractual, tomando en consideración que el mismo ordenamiento jurídico prevé formas de restablecer el imperio del derecho cuando son vicios civiles. De esta manera, cuando estamos frente a contratos criminalizado, es decir cuando a mediados engaño que el causante del incumplimiento contractual, la jurisprudencia ha declarado que el incumplimiento contractual queda criminalizado bajo la denominada estafa, cuando con ocasión de la contratación de negocios jurídicos de carácter privado, ya sean civiles o mercantiles, uno de los contratantes el sujeto activo, simule desde el principio propósito de contratar con otra persona, cuando lo verdaderamente querido es aprovecharse del cumplimiento de la otra parte contratante, pero sin intención de cumplir la suya, por ello existe estafa en los casos en que el autor simula un propósito serie de contratar cuando en realidad sólo quiere

[401] Dicha sentencia dice lo siguiente: 1) la utilización de un engaño bastante, por parte del autor del delito, para generar un riesgo no permitido para el bien jurídico; esta suficiencia, idoneidad o adecuación del engaño al establecerse con arreglo a un baremo mixto objetivo-subjetivo, en el que se pondere tanto el nivel de perspicacia o intelección del ciudadano medio como las circunstancias específicas que individualizar la capacidad del sujeto pasivo en el caso en concreto. 2) el engaño ha de desencadenarse el error del sujeto pasivo de la acción. 3) debe darse también un acto de disposición patrimonial el sujeto pasivo, debido precisamente al error, en beneficio del autor de la defraudación o de un tercero. 4) la conducta engañosa ha de ser ejecutada con dolor y ánimo de lucro. 5) De ella tiene que derivarse un perjuicio para la víctima, perjuicio que ha de aparecer vinculado causalmente a la acción engañosa y materializarse en el mismo el riesgo implícito que para el patrimonio de la víctima supone la acción engañosa del sujeto activo.

aprovecharse del cumplimiento de la parte contraria y del propio incumplimiento. Descansando entonces la existencia de un engaño inicial y causante en uno de los contratantes que da lugar el incumplimiento contractual, pero tal cumplimiento queda criminalizado, dando paso a la existencia del dolo Penal propia del delito de estafa porque desde el principio existe una discordancia entre la voluntad interna de uno de los contratantes de no cumplir y enriquecerse, y la exteriorizada y engañosa que manifiesta un propósito de cumplimiento inexistente radicado aquí el engaño teniendo en consideración que los negocios jurídicos que se encuentran criminalizados se sabe en forma anterior, que no habrá cumplimiento por uno de los contratantes, y sí tan sólo aprovechamiento del cumplimiento del otro contratante.

Es dable indicar que se han entregado por los autores distintas definiciones de estafa, no olvidando lo recién indicado en cuanto a la dificultad que existe en la estructura misma de la figura, que lleva a llevado a las distintas legislaciones del mundo a conceptualizarla en forma genérica y no de manera casuística, al ver que los límites o las múltiples formas de Comisión hacen imposible indicar en el tipo penal la distintas formas de conductas podrían englobar el engaño, quedando por ende en conceptos amplios[402]. A modo ilustrativo diremos que para *Goldstein*, la estafa es "acción y efecto de estafar. Estafa que nace adoptar a otro, con ánimo de lucro, una disposición patrimonial que resulta perjudicial para sí o para terceros,

[402] De esta manera nos dice VON HENTIG "el delito de estafa presenta una serie de peculiaridades que lo separan de la masa de los restantes hechos punibles. Además de ser dogmáticamente complicado, está muy enmarañado psicológicamente. Los tránsitos de la estafa a la pequeña sin formalidades o truco comerciales son oscuros influyentes. La estafa proporciona, por término medio, el más alto botín de todos los delitos contra la propiedad. En ella la actuación del sujeto sobre la víctima es de índole psíquica, y por esto invisible, consintiendo en un determinar que mueve al estafado a perjudicarse asimismo o a perjudicar a otro, en su patrimonio. Como agente físico destaca no tanto el autor del delito como el lesionado". (VON HENTIG, Hans, *Estudios de psicología criminal, la estafa*, Volumen III, Traducción castellana y notas de José María RODRÍGUEZ DEVESA, 2ª edición, Editorial Espasa-Calpe, Madrid, 1964, págs. 17.), Citado por SILVA SILVA, Hernán, *Las estafas doctrina, jurisprudencia y derecho comparado*, Editorial jurídica de Chile, 2005, págs. 30.

mediante un despliegue de medios engañosos tendientes a provocar la víctima el error acerca de la conveniencia de su decisión[403]". A su vez para *Mezger, "*nos dice que con arreglo al §263, se castiga por estafa al que con la intención de procurar asimismo o un tercero una ventaja patrimonial antijurídica, perjudica el patrimonio de otro, haciendo surgir o manteniendo un error mediante simulación de hechos falsos o mediante deformación o supresión de hechos verdaderos en consecuencia estafa "es un perjuicio ocasionado mediante engaño al patrimonio, con intención de enriquecimiento"[404].

Por otro lado, para *Cuello Calón*, estafa es "el perjuicio patrimonial realizado con ánimo de lucro mediante engaño"[405]. Para *Quintano Ripollés,* nos dice "que en el derecho español una definición sintética de la estafa consiste en el lucro ilegítimo conseguido en perjuicio ajeno mediante el empleo de engaños reales o personales. Esquema que habría que rellenar con las adiciones normativas y culpables listas pertinentes, así como con las referencias típicas con misiva, si bien estas no son en absoluto requerirles, vista la amplitud que en esta materia se otorga a la analogía nuestro derecho. Sirve, por lo menos, como en otros sistemas doctrinarios para referencia ideal y contraste con los diversos supuestos que la ley y la vida presentan,

[403] GOLDSTEIN, Raúl, D*iccionario de derecho penal y criminología,* 2ª edición actualizada y ampliada, Editorial Astrea, Buenos Aires, Argentina 1978, págs. 312.

[404] MEZGER, Edmund, *Derecho penal, parte especial, libro de estudio,* Traducción de la 4ª Edición alemana de 1954, traducida por el Dr. Conrado A, Finzi, Traductor del Instituto de Derecho Penal de la facultad de derecho y ciencias sociales de Córdoba, Editorial bibliográfica Argentina, Buenos Aires, Argentina, 1959, págs. 239.

[405] CUELLO CALÓN, Eugenio, *Derecho Penal, parte especial*, tomo II, revisado puesta al día, por César Camargo Hernández, De la carrera fiscal, Dr. en derecho y profesor de la Universidad de Madrid, vol. 2, 14ª edición reimpresión, Editorial Boch, S.A., Barcelona, 1980, págs. 928.

permitiendo así perfilar mejor su contenido"[406]. A su vez, *Scelzsi*, indica que "la estafa es la acción es la defraudación y que fraude significa engaño abuso de confianza que crea o prepara un daño generalmente de naturaleza material"[407]. Para *Manzini*, "indica en relación con el artículo 640 del Código Penal Italiano que el delito estafa (truffa, escroquerie, bertug, false pretense), se configura cuando una persona induce a error a otra, por medio de artificios o engaño, obteniendo para sí mismo o para otro algún provecho injusto, con perjuicio ajeno"[408].

C) Bien jurídico protegido

En cuanto bien jurídico protegido, podemos decir que es el *patrimonio ajeno*, ya sea en sus distintos elementos que lo integran, como bienes muebles, inmuebles o derechos, etcétera. Además de ello se puede mencionar que también se ve afectada la buena fe, tomada como la que debe tener todo contratante o sujeto en el tráfico jurídico, puesto que se elimina o se cambia la esperanza que lo adquirido o lo supuestamente pactado no corresponde a la realidad. Teniendo la estafa un contenido patrimonial, que no permite castigar la frustración de expectativas derivadas del tráfico jurídico económico, pero que no perjudican económicamente

[406] QUINTANO RIPOLLÉS, Antonio, *Tratados de parte especial del derecho penal, infracciones patrimoniales de apoderamiento*, tomo II, 2ª edición puesta al día por Carlos García Valdés, profesor de Derecho Penal de la Universidad Salamanca, Editorial Revista de Derecho Privado, Madrid, España 1977, págs. 584.

[407] SCELZSI, José Licinio, *Defraudación por retención indebida*, Editorial DIN Editores, Buenos Aires, Argentina, 1992, págs. 10.

[408] MANZINI, Vicenzo, *Tratado de derecho penal, Parte Especial*, Editorial del foro, Buenos Aires, Argentina, 1996, págs. 122.

nadie en concreto, trascendiendo los derechos patrimoniales individuales a los derechos lesionados de los consumidores. Sin embargo es recomendable señalar que las tasas el delito patrimonial por excelencia, es el nombre siguiendo el tipo penal la protección de la propiedad, ni la posesión o título de crédito, sino que por el contrario patrimonio de una persona valores económicos, todo esto como expresión del desarrollo de la personalidad. Podemos decir entonces que los elementos esenciales del tipo penal en cuestión, son el *engaño, error, disposición patrimonial y perjuicio*[409].

[409] STS, Sala 2ª, de lo Penal, N° 187, de 08. II. 2002, (Ponente: José Ramón SORIANO SORIANO). Dicha sentencia, hace un análisis de los elementos del delito de estafa y señala: En lo pertinente, y en lo que respecta a sus fundamentos de derecho: Antes de examinar en sus detalles el primero de los motivos, conviene conocer los elementos constitutivos del delito de estafa, según doctrina de esta Sala. La Sentencia de 19/09/2001 nº 1.641/2001 los condensa en los siguientes términos: *"en los elementos configuradores del delito de estafa hay que enumerar: 1º) Un engaño precedente o concurrente, espina dorsal, factor nuclear, alma y sustancia de la estafa, fruto del ingenio falaz y maquinador de los que tratan de aprovecharse del patrimonio ajeno. 2º) Dicho engaño ha de ser «bastante», es decir, suficiente y proporcional para la consecución de los fines propuestos, cualquiera que sea su modalidad en la multiforme y cambiante operatividad en que se manifieste, habiendo de tener adecuada entidad para que en la convivencia social actúe como estímulo eficaz del traspaso patrimonial, debiendo valorarse aquella idoneidad tanto atendiendo a módulos objetivos como en función de las condiciones personales del sujeto afectado y de las circunstancias todas del caso concreto; la maniobra defraudatoria ha de revestir apariencia de seriedad y realidad suficientes; la idoneidad abstracta se complementa con la suficiencia en el específico supuesto contemplado, el doble módulo objetivo y subjetivo desempeñarán su función determinante. 3º) Originación o producción de un error esencial en el sujeto pasivo, desconocedor o con conocimiento deformado o inexacto de la realidad, por causa de la insidia, mendacidad, fabulación o artificio del agente, lo que lleva a actuar bajo una falsa presuposición, a emitir una manifestación de voluntad partiendo de un motivo viciado, por cuya virtud se produce el traspaso patrimonial. 4º) Acto de disposición patrimonial, con el consiguiente y correlativo perjuicio para el disponente, es decir, que la lesión del bien jurídico tutelado, el daño patrimonial, sea producto de una actuación directa del propio afectado, consecuencia del error experimentado y, en definitiva, del engaño desencadenante de los diversos estadios del tipo; acto de disposición fundamental en la estructura típica de la estafa que ensambla o cohonesta la actividad engañosa y el perjuicio irrogado, y que ha de ser entendido, genéricamente como cualquier comportamiento de la persona inducida a error, que arrastre o conlleve de forma directa la producción de un daño patrimonial a sí misma o a un tercero, no siendo necesario que concurran en una misma persona la condición de engañado y de perjudicado. 5º) Ánimo de lucro como elemento subjetivo del injusto, exigido hoy de manera explícita por el artículo 248 del C.P. entendido como propósito por parte del infractor de obtención de una ventaja patrimonial correlativa, aunque no necesariamente equivalente, al perjuicio típico ocasionado, eliminándose, pues, la incriminación a título de imprudencia. 6º) Nexo causal o relación de causalidad entre el engaño provocado y el perjuicio experimentado,*

D) Comentarios sólo respecto de sus elementos

1. Engaño[410]

El delito de estafa precisa de una determinada forma de conducta que dé inicio proceso causal, esto es el *engaño*[411], "falta de verdad en lo que se dice, hace,

---

ofreciéndose éste como resultancia del primero, lo que implica que el dolo del agente tiene que anteceder o ser concurrente en la dinámica defraudatoria, no valorándose penalmente, en cuanto al tipo de estafa se refiere, el «dolo subsequens», es decir, sobrevenido y no anterior a la celebración del negocio de que se trate; aquel dolo característico de la estafa supone la representación por el sujeto activo, consciente de su maquinación engañosa, de las consecuencias de su conducta, es decir, la inducción que alienta al desprendimiento patrimonial como correlato del error provocado, y el consiguiente perjuicio suscitado en el patrimonio del sujeto víctima, secundado de la correspondiente voluntad realizativa".

[410] Al respecto véase análisis dirigido por MIR PUIG, con PASTOR MUÑOZ, en el cual analiza, "[…] En realidad, el problema de los límites del engaño típico en el delito estafa pueden sintetizarse en una sola pregunta: ¿cuándo podemos hace responsable al autor por el acto de disposición perjudicial realizado formalmente por la víctima?", "[…] la doctrina lleva tiempo ocupándose de este problema y lo cierto que la cuestión de si existe un ámbito de responsabilidad de la víctima de la estafa. MIR PUIG, Santiago (director), PASTOR MUÑOZ, Nuria, *Comentarios a la jurisprudencia el Tribunal Supremo, Engaños punibles e mentiras impunes: un análisis de los límites del engaño típico en el delito estafa a la luz del caso de la sentencia del Tribunal Supremo de 18 de julio de 2003*, Anuario de Derecho penal y Ciencias penales, vol. LVI, 2003 Sección de jurisprudencia, Universidad Pompeu Fabra, Barcelona. pág 562.

[411] Para Bajo Fernández, el engaño es la falta de verdad en lo que se dice, o hace de modo bastante para producir error e inducir el acto de disposición patrimonial. "La presión engaño designa la acción y efecto de hacer creer a alguien, con palabras de cualquier otro modo, algo que no es verdad. Sin embargo no toda mentira constituye cumplimiento del primer requisito exigido por la ley para el delito estafa. "[…] el engaño que sea bastante para inducir a error, como entendió siempre la doctrina y jurisprudencia, y a la vez inductor del acto disposición patrimonial, pone de relieve la necesidad de que la simple mentira vaya acompañada de las características necesarias para que dichos resultados(error, actos de disposición en perjuicio), pueden serle a ella imputados objetivamente". BAJO FERNÁNDEZ, Miguel, / PÉREZ MANZANO, Mercedes / SUÁREZ GONZÁLEZ, Carlos, *Manual de derecho penal parte especial, Delitos patrimoniales y económicos*, 2ª Edición el centro estudios Ramón Areces, Madrid, 1993. pág. 274, y sigs.

cree, piensa o discurre[412]" De otro modo podemos decir que engaño, es la simulación o disimulación capaz de inducir a error a una o varias personas, puede consistir tanto en la afirmación de hechos falsos como la simulación o desfiguración de los verdaderos. Esta falta de verdad produce, que se forme una representación incierta de lo que el sujeto realmente pretende, se disfraza la realidad. La acción engañosa, que caracteriza a todos los tipos de fraude, tiene como denominador común que debe ser anterior o también puede ser concurrente. Como es el elemento nuclear de la estafa, dicho engaño debe ser suficiente y proporcional para lograr los fines propuestos, es decir debe ser adecuado eficaz para provocar el error esencial en el sujeto pasivo, todo ello con el fin que tenga la entidad suficiente para el traspaso patrimonial, con ello se cumple los fines propuestos por el estafador[413][414]. Para comprobar que el engaño es idóneo, es de vital importancia, indagar la capacidad ex

[412] Real Academia Española, [en línea], www.dle.rae.es.

[413] STS, Sala 2ª de lo Penal, N° 331, de 15. IV. 2014, (Ponente: Candido PUNPIDO TOURON). Dicha sentencia, se refiere al elemento engaño al indicar que el *engaño* ha de entenderse bastante cuando haya producido sus efectos defraudadores, logrando el engañador, mediante el engaño, engrosar su patrimonio de manera ilícita, o lo que es lo mismo, es difícil considerar que el engaño no es bastante cuando se ha consumado la estafa. Como excepción a esta regla sólo cabría exonerar de responsabilidad al sujeto activo de la acción cuando el engaño sea tan burdo, grosero o esperpéntico que no puede inducir a error a nadie de una mínima inteligencia o cuidado. STS, 2ª de lo Penal, N° 614, de 08. VII. 2016, (Ponente: Antonio del MORAL GARCÍA). Del mismo modo refiere que la necesidad de que el *engaño sea bastante*, no expulsa del ámbito de la estafa a cualquier supuesto en que se constate que la víctima pudiera haber sido más cautelosa o desconfiada. Solo los engaños burdos en que el error proviene más que del engaño de la absoluta desidia o indolencia del sujeto pasivo se desvanecerá la tipicidad del delito. Se desestima el recurso de casación.

[414] Al respecto se refiere QUINTANO RIPOLLÉS, "Y él lo culpa vista también, por cuanto que se engaño ha de ser requerido como tal por el culpable que lo usa, e ignorado por el destinatario, ya que, de otro modo, dejaría de ser engaño, siéndolo en rigor para una sola de las partes, la engañada perjudicada […] La entidad del engaño, su cantidad, ha de ser medida no exactamente en cómputos objetivamente cuantitativos, sino en relación con su eficacia operativa. Continua indicando, […] Que el engaño debe proyectarse la dimensión de persona a persona, aunque el destinatario concreto puede ser desconocido, o bien multitudinario, como cuando se dirige la maniobra fraudulenta el público en general, a través de anuncio propuesta impersonales. QUINTANO RIPOLLÉS, Antonio, *Tratado del parte especial del Derecho Penal*, *Infracciones Patrimoniales y Apoderamiento*, tomo II, 2ª Edición, , Editorial Revista de Derecho Privado, Madrid. 1977, pág 590 y 597.

ante del engaño para producir un error en la víctima, con ello resulta que dicho error ejercerá un papel limitador de las conductas típicamente relevantes.

1.1. Engaño omisivo[415]

Cuando hablamos de comisión por omisión en la estafa, se refiere al hecho de no declarar circunstancias en el momento de contratar, es decir cuando se calla el efecto o vicio de la cosa que se pretende entregar, en virtud de algún contrato u otro instrumento jurídico[416]. Al respecto PASTOR MUÑOZ, señala que "No todos los caos

[415] Sobre el particular y conforme a STS a propósito del delito de estafa CHOCLAN MONTALVO, realiza un examen acerca de los elementos del tipo, refiriéndose al *engaño por omisión,* en forma muy resumida refiere que "el engaño es el medio para la inducción a la disposición patrimonial, por ello se plantea la problemática sí dogmáticamente puede sostenerse la *inducción por omisión,* por ello se trata de terminación si un comportamiento inactivo del sujeto activo, tiene la virtualidad comunicante que requiere el engaño inductor, o si, en realidad, los caso que plantea la doctrina como engaño omisivo pueden ser reconocidos a la teoría de los comportamientos activos concluyentes admitidos por la teoría como medio para exteriorizar un engaño". El autor, igualmente se refiere a los delitos de resultado vinculados un determinado comportamiento donde surgen especiales problemas en la correspondencia con la acción, e indica que […] En este sentido Jakobs, advierte los problemas especiales que presenta los delitos que se cometen mediante la transmisión información, equivalente a la comisión cuando el autor omite reservación información que está saliendo de su ámbito de organización. Ejemplo: el jefe no impide que su secretaria envió una carta, concebida a un solo como proyecto, que contiene afirmaciones engañosas. Lo que ocurre es que, en este caso, la influencia psíquica en el sujeto pasivo no ha tenido lugar mediante un omisión sino a través de un comportamiento activo, la entrega de la carta que expresa, mediante su lectura, contenido engañoso. CHOCLAN MONTALVO, José, consideraciones particulares sobre el delito de estafa, (a propósito de la STS de 14 de marzo de 2003), Diario La Ley N° 5752, año XXIV, 02 de abril de 2003, referencia D-77. STS, Sal 2ª en lo Penal, N° 298, de 14. III. 2003, (Ponente: José Ramón SORIANO SORIANO).

[416] STS, Sala 2ª en lo Penal, N° 448, de 01. VI. 2007, (Ponente: Enrique BACIGALUPO ZAPATER). Dicha sentencia se refiere en lo principal, al delito de estafa, cuando existe una posición de garante y engaño omisivo, en indica "*La acción del que, consciente de su insolvencia y la imposibilidad de pago, omite informar al otro, con el que ha tenido relaciones mercantiles anteriores, circunstancias que son relevantes para decidir la celebración del contrato que se le ofrece, comete el engaño típico del art. 248.1º CP.*

silencio, son supuestos de estafa, por omisión. Por una parte, hay caso de silencio constituyen supuestos estafa mediante actos concluyentes, porque ese silencio es, en el contexto, un acto comunicación información, de esta manera así, no decir nada sobre el estado de un producto puede *comunicar*, en un determinado contexto, que aquél está en perfecto estado[417]. Por otra parte, hay otros casos de silencio que sí constituyen supuestos estafa por omisión, pues en ellos el autor no suministra el destinatario o información con la que este último podría haber alcanzado una representación correcta de la realidad[418].

1.2. Engaño implícito

Cuando existe la obligación de informar, y se incumple conduce a una reticencia con valor concluyente. Es decir, el sujeto activo no debe callarse, de acuerdo a los deberes, tanto de usos y costumbres como también jurídico, por ello se dice que el silencio permite que el sujeto pasivo del delito interprete, siendo amparado por el derecho, de un modo determinado, es decir el sujeto pasivo entiende que no hay nada que informar. También se han denominad formas omisivas

[417] Algunos autores (BAJO FERNÁNDEZ / PÉREZ MANZANO), admite la estafa por omisión cuando se fundamenta que el autor que omitió que tenía una posición de garante consistente en el deber de eliminar el error de la víctima. En cambio, otros (VIVES ANTÓN, RODRÍGUEZ RAMOS) rechaza la estafa por omisión con el argumento del óbice cronológico: la estafa, el engaño debe causar el error, y ello no es así en los casos de estafa por omisión, en los que el error existe antes de que se produzca el engaño. PASTOR MUÑOZ, Nuria, *Lecciones de Derecho penal, Parte especial*, en SILVA SÁNCHEZ, Jesús, (dir.) RAGUEZ VALLÉS (coord.), *Delito contra el patrimonio*, Editorial Atelier, Barcelona, 2006. pág. 215.

[418] PASTOR MUÑOZ, Nuria, *Lecciones de Derecho penal, Parte especial*, en SILVA SÁNCHEZ, Jesús, (dir.) RAGUEZ VALLÉS (coord.), *Delito contra el patrimonio*, Editorial Atelier, Barcelona, 2006, pág. 215.

impropias de acción concluyente[419]. Se ha discutido, con respecto a si existe propósito no defraude previo[420].

2. Error[421]

Existe una falsa representación o equivocada de la realidad, que nace producto del engaño provocado, y que sitúa a la voluntad del sujeto pasivo en una posición viciada, y consecuentemente también el acto lo es. Esta conducta que tiene

[419] SAP, de Valencia, Sección 3ª, N° 363, de 21. V. 2010, (Ponente: Lamberto RODRÍGUEZ MARTÍNEZ). Refiere dicha sentencia [….] En definitiva, en estas figuras de estafa impropia del art. 251 CP el engaño aparece implícito en cada una de ellas, como ocurre en estos casos de doble venta, en los cuales ese engaño se encuentra en la segunda operación al ocultar que antes había realizado ya otra, mediante la cual se había despojado de su titularidad, aunque, como aquí ocurrió, esa titularidad constase formalmente en el Registro de la Propiedad al que no pudo tener acceso el documento privado con el que se realizó la primera compraventa.

[420] El engaño puede ser explicito (efectuando aseveraciones falsas) o implícito (ocultando, aun sin afirmar falsamente, el propósito de incumplir los términos de la relación contractual en la que halla inmerso, cual sucede en los contratos o negocios jurídicos criminalizados). SUAREZ, Carlos / JUDEL, Ángel / PIÑOL, José, *Delincuencia informática, tiempos de cautela y amparo*, Capitulo 10, *Las estafas*, 1ª Edición, Editorial Aranzadi, Pamplona, 2012. pág. 223.

[421] PASTOR MUÑOZ, Nuria señala que algunos autores han defendido la tesis de que el art. 248 CP no exige la concurrencia de error como estado psicológico del engañado, sino que el error es solamente la *medida normativa para fijar la idoneidad del engaño;* es decir, en su opinión, la capacidad para producir error es un criterio para saber si el engaño es idóneo o no. Esta definición de error es útil para el juicio de imputación objetiva del comportamiento (definición del riesgo *ex ante)*, en el que el error es un criterio normativo para definir el engaño; en cambio, en el juicio de imputación objetiva del resultado (realización del riesgo en el resultado), parece que debe existir un error real (psicológico), que demuestre que el riesgo típico creado por el autor con el engaño se ha realizado en el resultado. PASTOR MUÑOZ, Nuria, *Lecciones de Derecho penal, Parte especial*, en SILVA SÁNCHEZ, Jesús, (dir.) RAGUEZ VALLÉS (coord.), *Delito contra el patrimonio*, Editorial Atelier, Barcelona, 2006, pág. 216.

ser anterior al engaño debe ser *bastante*[422], o tener la fuerza suficiente para producir un error en otra persona. Dicho comportamiento anterior, también debe haber una relación de causalidad y además se debe tomar en cuenta las características personales del sujeto, rango etario, su capacidad intelectual, y también qué tipo de relaciones tiene con el sujeto activo, entre otras. Este error sobre la víctima, bajo su influencia de actuar sin sospechar que sus actos traerán consecuencia negativa sobre su patrimonio. El engaño y error se vinculan por una difícil relación de causalidad. En definitiva, el engaño como tal, produce en la víctima error y ha de permitir obtener algo con el consentimiento de la víctima, hace que se verifique la disposición o el acto de disposición con el desplazamiento de sus bienes, lo que obviamente no aparece en el delito de hurto, donde no hay entrega voluntaria, y algo similar con la apropiación indebida donde no hay engaño en la entrega de lo luego apropiado[423]. Se argumenta que la estafa el error, es una libre derivación esencial del engaño que usa el autor del delito para influir, que la voluntad sujeto pasivo ya su vez, produce una alteración de la verdad. De esta manera se consuma el acto dispositivo de la víctima, que deja en manos del sujeto activo del delito, o del tercero al que se dirige lucro, el objeto de la estafa. El acto disposición se observa desde un punto de vista amplio, no iusprivatista. Aunque siempre habrá de mostrar contenido patrimonial, entendemos que basta la simple transferencia de la cosa o

[422] STS, Sala 2ª en lo Penal, N° 614, de 08. VII. 2016 (Ponente: Antonio DEL MORAL GARCÍA). Se estima en dicho fallo en lo medular, que la necesidad de que el engaño sea *bastante*, no expulsa del ámbito de la estafa a cualquier supuesto en que se constate que la víctima pudiera haber sido más cautelosa o desconfiada. Solo los engaños burdos en que el error proviene más que del engaño de la absoluta desidia o indolencia del sujeto pasivo se desvanecerá la tipicidad del delito. Se desestima el recurso de casación.

[423] STS, Sala 2ª en lo Penal, N° 358, de 10 VI. 2015, (Ponente: Francisco MONTERDE FERRER). Dicha sentencia estima que, el *engaño ha de ser idóneo*. Es preciso que exista una relación de causalidad entre el engaño que provoca el error y el acto de disposición que da lugar al perjuicio, de donde se obtiene que aquél ha de ser precedente o, al menos, concurrente, al momento en que tal acto tiene lugar. El engaño debe ser la causa del error; el error debe dar lugar al acto de disposición y éste ha de ser la causa del perjuicio patrimonial. Se estima parcialmente la casación.

desplazamientos un valor económico de las ferias sujeto pasivo al sujeto activo. La entrega no tiene que ser un acto jurídico, ni le disposición un negocio jurídico. Por último conviene indicar que no es preciso que la víctima sepa de la naturaleza del acto que realiza por engaño, pero el acto de disposición del sujeto pasivo ha sido siempre una expresión muy discutida. Si se suprimiera evitaríamos impunidad muchos casos con independencia de que el daño provenga, generalmente un acto dispositivo del propio perjudicado, y que sin engaño no hubiera realizado[424]. A mayor abundamiento, el delito de estafa tradicional, discurre en un error de la realidad que sufre la víctima, puesto que dicho error, y como consecuencia directa del mismo se realizó un acto de disposición, que trae un perjuicio para el sujeto pasivo. Este error ha sido preparado por la otra persona, que recibe ganancia o que es beneficiado por dicho error, a pesar de ello vale aclarar que el núcleo de la estafa es un engaño antecedente, causante y bastante, toda vez que el error es consecuencia del engaño, y debe existir relación de causalidad entre ambos, es decir, el engaño trae como consecuencia el error del sujeto pasivo de la acción, y con la fuerza necesaria para poder culminar el acto de disposición, acto que va en directo beneficio del autor de la defraudación o también en beneficio de un tercero. A raíz de lo anterior es que se exige por el artículo 248 del Código Penal Español, que sea o que tenga lugar mediante un engaño *bastante*, porque para que se configure el delito de estafa, no es suficiente con realizar el tipo objetivo, un engaño que causalmente produzca un perjuicio patrimonial, además se exige que dicho perjuicio patrimonial sea imputable objetivamente a la acción engañosa. Es dable se presente, el caso en que el sujeto activo conoce la debilidad de la víctima, o el nivel de

[424] SAP, de Madrid, Sección 15, N° 293, de 15. IV. 2015, (Ponente: Carlos FRANCISCO FRAILE), Dicha sentencia se Refiere, a los elementos de la estafa, señalando que por último, […] De ella tiene que derivarse un perjuicio para la víctima, perjuicio que ha de aparecer vinculado causalmente a la acción engañosa (nexo causal o naturalístico) y materializarse en el mismo el riesgo ilícito que para el patrimonio de la víctima supone la acción engañosa del sujeto activo (relación de riesgo o segundo juicio de imputación objetiva).

instrucción, puesto que en estos casos la normalidad aparecen como objetivamente idóneas como para producir un engaño, sin embargo esto no puede ser excluido, utilizándose la fórmula del criterio de inadecuación del engaño, usando un juicio de prognosis, tomando en consideración la normalidad del suceder social, y de acuerdo a ello adecuar la situación a la normalidad y de acuerdo al tipo penal, para que éste resulte idóneo, se refirió de esta forma el TS, al indicar "que el engaño ha de ser examinada conforme un baremo objetivo y otro subjetivo. El baremo objetivo va referido un hombre medio a ciertas exigencias de seriedad y entidad suficiente para afirmarlo. El criterio subjetivo tiene presente las concretas circunstancias del sujeto pasivo. En otras palabras, la cualificación del engaño como bastante pasa por un doble examen, el primero desde la perspectiva de un tercero ajeno a la relación creada y, el segundo, desde la óptica del sujeto pasivo, sus concretas circunstancias y situaciones, con observancia siempre, de la necesaria exigencia de autodefensa, de manera que se exigirá en el examen del criterio subjetivo una cierta objetivación de la que resulta una seriedad y entidad de la conducta engañosa"[425].

3. Acto de disposición patrimonial

Cuando nos referimos al acto disposición patrimonial podemos indicar que estamos frente a una variedad de formas de comportamiento de la persona inducida a error, que lleva de forma directa a la producción de un daño en su patrimonio, el daño que puede ser tanto si misma, como generarse también el patrimonio de un tercero, teniendo en cuenta además que no es necesario que concurran en una misma

[425] STS, 2ª de lo Penal, N° 452, de 31. V. 2011, (Ponente: Juan Ramón BERDUGO GOMEZ DE LA TORRE).

persona el estado de engañado y de perjudicado. *Bajo Fernández*, explica respecto de dicho elemento, "Inducido por el engaño y a consecuencia del error ha de darse un acto de disposición patrimonial, de este modo la relación con el engaño, exigirá la ley, pone de relieve la identidad del sujeto engañado y del imponente, identidad que no tiene por qué darse necesariamente con el perjudicado. La doctrina entiende que la expresión *acto* deben incluirse tanto las acciones positivas como las acciones que provoca el perjuicio señalado en la ley. Del mismo modo nos ilustra al referirse que entiende que "Perjuicio es la disminución del patrimonio del engañado o de un tercero. No es necesario que engañado perjudicado sean la misma persona. Son, sin embargo la misma persona el sujeto pasivo del delito y el perjudicado. El engaño aparece exclusivamente sujeto pasivo de la acción, pero no necesariamente como sujeto pasivo del delito con las implicaciones que ello supone a nivel procesal. Indica además, que el perjuicio se determina con la disminución de patrimonio tras una comparación de su situación antes y después del acto disposición determinado por el error"[426]. La conducta típica puede ser realizada por cualquier sujeto, es decir la persona que utiliza el engaño idóneo, del cual nace la disposición patrimonial lesiva[427][428]. Por otro lado, no es necesario que el sujeto pasivo sea consciente estar

[426] BAJO FERNÁNDEZ, Miguel, / PÉREZ MANZANO, Mercedes / SUÁREZ GONZÁLEZ, Carlos, Manual de derecho penal parte especial, Delitos patrimoniales y económicos, 2ª Edición el centro estudios Ramón Areces, Madrid, 1993. pág. 283, y sigs.

[427] STS, Sala 2ª en lo Penal, N° 660, de 14. X. 2014 (Ponente: Ana María FERRER GARCÍA). Al resumir lo resuelto por dicha sentencia nos dice…"Cuando en un contrato una de las partes disimula su verdadera intención, su genuino propósito de no cumplir las prestaciones a las que contractualmente se obligó y como consecuencia de ello la parte contraria desconocedora de tal propósito, cumple lo pactado y realiza un acto de disposición del que se lucra y beneficia al otro, nos hallamos en presencia de la estafa conocida como negocio o contrato criminalizado".

[428] BALMACEDA HOYOS, Gustavo, *El delito de estafa, una necesaria normativizados y de sus elementos típicos,* Revista estudios socio-jurídicos, 13, U. de los Andes, Chile, 2011. pág. 163-219.

realizando un acto de disposición, puesto que sólo se exige que exista un acto voluntario.

Vale considerar que el acto de disposición nace cuando se refiere a alguna acción positiva, como por ejemplo entregar una cosa, prestar un servicio por el cual se obtiene contraprestación, y asimismo también puede consistir en una omisión respecto de la cual produce un perjuicio señalado en la ley.

Es importante señalar, que el Tribunal Supremo ha planteado otro tema en cuanto si la exclusión de la imputación a la víctima desaparece por la coetánea concurrencia de elementos subjetivos en el comportamiento de la misma, como el afán de lucro con desprecio de la eventual ilegalidad del propósito de enriquecimiento. Esta cuestión radica en si el tipo penal de la estafa puede tutelar pérdidas patrimoniales que tienen lugar en un contexto de un negocio con causa ilícita, o expresado de otra manera en ciertos casos de disposición por obtener un fin con propósito ilícito, que incluso llene el tipo subjetivo de un tipo penal, toda vez que no es irrelevante la conducta de la víctima en cuanto el fin de protección de la norma en la estafa, toda vez que permitiría dejar al margen del tipo determinados perjuicios causalmente producido por comportamientos engañosos pero que puedan no hallarse comprendidos en dicho ámbito de protección según su sentido y las finalidades político criminales perseguidas por el legislador. Respecto lo mismo es importante, desde un punto de vista criminológico, que el fin de protección de la norma en el delito estafa no puede sólo consistir en el entregar tutela penal a quien sufre un menoscabo patrimonial, como producto de un incumplimiento de una promesa ilícita, incluso constitutiva de delito o cuando la disposición del patrimonio pretende conseguir determinados efectos contrarios a derecho, infringiendo incluso la norma penal, existiendo casos, que inclusive se pudiera exigir de responsabilidad penal a propia víctima, siempre y cuando el comportamiento de ella puede ser calificado al menos como tentativa punible, perdiendo la protección penal de aquel

patrimonio, esto a base que se puede extraer de la norma penal, como razón de existencia de la misma en que la protección que la norma imparte no puede alcanzar la tutela frente a pérdidas patrimoniales que han nacido o existido en el marco negocio ilícito perdiendo con ello el derecho de recuperar su patrimonio perdido[429]. CORCOY, concluye que lo normal será que le engañado sea el exponente y, a su vez, el eventual perjudicado de esto deriva que cité supuesto de estafa triangular, donde el engañado predisponentes la misma persona, pero no se corresponde con el perjudicado. En estos casos es preciso que el imponente tenga algún poder disposición, jurídicamente relevante, son el objeto material: la estafa implica engañar a quien pueda jurídicamente disponer de un patrimonio que resulte lesionado, en todo caso el imponente que ser el engañado. Continúe indicando el autor, que el delito de auto perjuicio patrimonial inconsciente vinculado a la estructura de la autoría mediata, lo que sirve para imitarlo del hurto en la presión indebida resulta: en la estafa es el eventualmente perjudicado que nace entrega de la cosa a sujeto activo, sin que sepa que esa entrega es perjudicial; el engaño previo al acto desplazamiento patrimonial diferencie la estafa de la apropiación indebida[430].

4. Perjuicio. Animo de lucro

[429] STS, 2ª Sala de Lo Penal, N° 733, de 09. VII. 2009, (Ponente: Juan Ramón BERDUGO GOMEZ DE LA TORRE). Sobre el tema dicha sentencia refiere, […] "la hipótesis que pudiera calificarse de autopuesta en peligro. Es decir cuando la víctima no es ajena con su comportamiento a la producción del resultado. Supuesto en que surge la necesidad de decidir si la víctima pierde la protección del Derecho Penal, bajo criterios de autorresponsabilidad, o si, por el contrario, debe mantenerse la atribución de responsabilidad al autor que creó el riesgo. Lo determinante sería la existencia de ámbitos de responsabilidad diferenciados, con determinación normativa previa a la imputación".

[430] CORCOY BIDASOLO, Mirentxu, *Manual Práctico de Derecho penal, Parte especial*, 2ª Edición, Editorial Tirant lo Blanch, Valencia, 2004, pág. 570.

Al hablar de perjuicio, podemos entender que existe una lesión de elementos indeterminados del patrimonio, de la víctima que es engañada o de un tercero, puesto que si no existe perjuicio no hay estafa consumada y el perjuicio ha de ser consecuencia del acto de disposición, indicando la vez que no tiene importancia o es indiferente que el perjuicio recaiga en el que dispone de su patrimonio o de un tercero, no necesario entonces que el exponente y perjudicado coincidan. Al respecto se refiere el autor VIVES ANTÓN, "toda acción y omisión que implique un desplazamiento patrimonial. Ese desplazamiento puede tener lugar en forma de entrega, cesión o prestación de la cosa, derecho servicio de que se trate (pues el delito de estafa puede recaer sobre cualquier elemento del patrimonio, incluida la expectativa legítimas y económicas valuables)"[431].

Citando a BUSTOS RAMÍREZ, refiere "que para determinar el perjuicio se tiene que partir de alguna cosa estimable económicamente que puede ser incluido en el patrimonio y si recibe protección jurídica, por ello la expectativa solo futuros, así la venta de un negocio la estimación económica de la clientela (que se asegura mediante datos falsos de ser de gran consideración), o bien, mediante información falsa asegura que futuro del negocio será excelente, cuando éste está de antemano

[431] Vives Antón, entrega un ejemplo, referido por la doctrina en varias oportunidades, y la vez explica respecto del mismo, "del sirviente que entrega una cosa de su principal que se le pide por el autor fingiéndose enviado de éste, hay estafa y no hurto, pues no concurre la conducta de sustracción exigida por el delito y sí todos y cada uno de los requisitos exigidos por el de estafa. Pero, en cualquier caso, ha de haber una atribución de bienes, derechos, servicios, etcétera. En la hipótesis del matrimonio engañoso, en que se fingen cualidades intenciones para mejorar la posición económica tras la boda, no hay estafa, porque el matrimonio no puede calificarse de acto disposición. Para que un determinado acto disposición llegué tener relevancia típica, ha de ser inducido por el error causado mediante engaño bastante. Por lo tanto, el acto de disposición ha de realizarse por el engañado. Pero, quien realiza el acto de disposición, puede no coincidir con el sujeto pasivo del delito". VIVES ANTÓN, Tomás, Derecho penal, Parte especial, Editorial Tirant lo blanch, Valencia, 2004, pág. 485.

condenado al fracaso"[432]. en cuanto ha habido una contraprestación estimada equivalente que implique una disminución del patrimonio de la víctima perjudicado, haciendo hincapié que es algo totalmente distinto o diferente cuando existe una estimación subjetiva de la víctima, puesto que al perjudicar el patrimonio, no puede entenderse que son simples expectativas, que no pueden valorarse económicamente.

En este sentido entonces, cuando hablamos de patrimonio, y con la idea que ha sido perjudicado, el daño en el mismo debemos entender que tiene que ser valorable económicamente, y no tomando estándares morales que sólo pueden ser valorados en todo caso en forma civil. Ahora bien una vez que ha ocurrido este perjuicio la posterior reparación del mismo no hace que desaparezca el delito, porque en este caso solo estaríamos de alguna manera entrando a sede civil.

Anteriormente en esta breve relación, con respecto a lo elementos objetivos de la estafa nos referimos al engaño, error, disposición patrimonial y perjuicio, ahora bien en cuanto al ánimo de lucro, se puede indicar que es un elemento subjetivo del injusto exigible manera explícita por el artículo 248 del Código Penal Español, y que ha sido entendido como un propósito por parte del infractor de obtener algún tipo de ventaja patrimonial, aunque no necesariamente debe ser equivalente, al prejuicio típico ocasionado[433]. Este tipo subjetivo o dolo de la estafa[434], se refiere al

[432] BUSTOS RAMÍREZ, Juan, *Manual de Derecho penal, Parte especial*, 2ª edición, Editorial Ariel, Barcelona, 1991. pág. 194.

[433] SUAREZ, Carlos / JUDEL, Ángel / PIÑOL, José, *Delincuencia informática, tiempos de cautela y amparo, Las estafas*, Capitulo X, 1ª Edición, Editorial Aranzadi, Pamplona, 2012. pág. 224.

[434] Refiere el Dr. POLAINO NAVARRETE, "cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndole a realizar un acto de disposición en perjuicio propio o de tercero (artículo 248 del Código Penal): el delito de estafa constituye un delito subjetivamente configurado por partida doble pues exige una doble intencionalidad en el agente: el ánimo de lucro y el ánimo de perjuicio. POLAINO NAVARRETE, Miguel, *Derecho penal, Parte genera,* Tomo II, Vol. I, Editorial Bosch, Barcelona, 2000, pág. 537.

conocimiento que se está engañando y perjudicando a otro, es decir querer obtener una ventaja o provecho, un ánimo de lucro[435].

En cuanto el lucro y el perjuicio, ambos son conceptos correlativos, que no es indispensable que el primero tenga una coincidencia con el segundo, puesto que el perjuicio puede tener un carácter económico ya la ves el lucro su contenido puede ser de afección o moral, aunque el lucro deviene del acto de disposición, y consecuentemente con eso el perjuicio no es necesario que sea querido por el sujeto activo que realiza la estafa, por el fin que quieren alcanzar, cuando se realiza dicho acto ilícito. BAJO FERNÁNDEZ, "indica que problema el lucro cesante ganancia futura está mal planteado, por supuesto que no pertenece el patrimonio las futuras esperanzas y los proyectos, pero sí los lucros o ganancias correspondientes a la entrega de una cosa prestación de un servicio. Si tales lucros o ganancias se frustran se produce un perjuicio desaparecer tal valor económico del patrimonio. La mera lesión de un derecho cuando no hay perjuicio económico, debe ser cuestión exclusivamente civil. En efecto, no constituyen delito de estafa la defraudación de un derecho sin contenido económico"[436].

Vale señalar, que algunos autores indican que cuando estamos hablando del elemento subjetivo del injusto, ánimo de lucro parece excluir la eventualidad del

[435] SAP de Cádiz, Sección 1ª N° 181, de 08. VI. 2015, (Ponente: Francisco Javier GRACIA SANZ), respecto de dicha elemento, explica la sentencia, "El *ánimo de lucro*, verdadero elemento subjetivo del injusto, constituye la característica determinante del dolo específico con que se procedió por el agente, como deseo, meta, logro o intención para obtener un lucro, un beneficio patrimonial, una ganancia evaluable económicamente, precisada de manera cierta, exacta y conocida. Este ánimo de lucro va embebido en ese dolo intencional que se desenvuelve con conciencia y voluntad de engañar, naturalmente que coetáneo a la propia mentira. Se absuelve a los acusados".

[436] BAJO FERNÁNDEZ, Miguel, / PÉREZ MANZANO, Mercedes / SUÁREZ GONZÁLEZ, Carlos, *Manual de Derecho penal, Parte especial, delitos patrimoniales y económicos*, 2ª Edición, Editorial Centro estudios Ramón Areces, Madrid, 1993. pág. 287.

dolo, y por supuesto formas imprudentes, toda vez que en algunos casos de jurisprudencia admitido que elemento subjetivo del injusto pueda ser eventual, sin embargo ello, otros autores niegan la hipótesis, porque precisamente se requiere ánimo de lucro.

Razonando de acuerdo a ello el elemento subjetivo del tipo se eliminaría cuando el sujeto activo no crea que engaña, por el contrario estima de un modo invencible lo que manifiesta su víctima, consecuentemente con ello, si falta el elemento subjetivo del injusto, las condiciones exigidas en el tipo estarían incompletas, por ende también se excluiría la tentativa imposible y hace atípica la conducta[437]

5. Relación de causalidad

La doctrina desde siempre y también la jurisprudencia exigido, entre los distintos elementos típicos del delito de estafa, una relación de causalidad de modo que el error sea consecuencia del engaño, el acto disposición patrimonial consecuencia del error y el perjuicio consecuencia del acto disposición. El artículo 248 expresamente definir el engaño como aquél bastante para producir error y como aquel que induce a realizar un acto disposición patrimonial[438].

[437] CONDE PUMPIDO, Cándido, *Estafas*, Editorial Tirant lo blanch, Valencia, 1997. pág. 97 y sigs.

[438] BAJO FERNÁNDEZ, Miguel, *Los delitos de estafa del Código penal*, Editorial Universitaria Ramón Areces, Madrid, 2004, pág. 57.

El Tribunal Supremo, ha dicho que el engaño ha de ser idóneo. Es preciso que exista una relación de causalidad entre el engaño que provoca el error y el acto de disposición que da lugar al perjuicio, de donde se obtiene que aquel de ser precedente o al menos concurrente, al momento en que tal acto tiene lugar. El engaño debe ser la causa del error; el error debe dar lugar al acto de disposición y este ha de ser la causa del perjuicio patrimonial[439]. El mismo tribunal también lo explica como *Nexo causal o relación de causalidad* "entre el engaño provocado y el perjuicio experimentado, ofreciéndose éste como resultancia del primero, lo que implica que el dolo del agente tiene que anteceder o ser concurrente en la dinámica defraudatoria, no valorándose penalmente, en cuanto al tipo de estafa se refiere, el dolo subsequens, es decir, sobrevenido y no anterior a la celebración del negocio de que se trate; aquel dolo característico de la estafa supone la representación por el sujeto activo, consciente de su maquinación engañosa, de las consecuencias de su conducta, es decir, la inducción que alienta al desprendimiento patrimonial como correlato del error provocado, y el consiguiente perjuicio suscitado en el patrimonio del sujeto víctima, secundado de la correspondiente voluntad realizativa[440].

III. Orígenes y evolución de la estafa informática en el Código Penal Español

[439] STS, 2ª Sala en lo Penal, N° 358, de 10. VI. 2015, (Ponente: Sr. Francisco MONTERDE FERRER).

[440] STS, 2ª Sala de lo Penal, N° 1768, de 28. X. 2002, (Ponente: Sr. D. Julián SÁNCHEZ MELGAR), (considerando quinto).

El derecho penal, ha debido adaptarse a las novedades sociales que trae los riesgos de la delincuencia informática, puesto que la nueva forma de criminalidad conlleva como consecuencia cierta incertidumbre, teniendo entonces la necesidad de control en la red para prevenir los daños posibles. De esta manera distintos gobiernos que pertenecen a la Unión Europea, han debido trabajar en la Convención del Consejo de Europa sobre delincuencia informática de 23 de noviembre de 2003 en Budapest, con el fin de unificar legislaciones. Antes del Código Penal de 1995 este tipo de delitos resultaban atípicos y los tribunales no estaban de acuerdo con aplicarlos o adecuarlos a la normativa existente.

El actual Código Penal, como se dijo anteriormente trata este tipo de delitos al referirse, a casos de transferencia electrónica de fondos, puesto que el aumento progresivo, resultaba dificultoso e ineficaz para la normativa existente, por lo mismo debía ser tratado. Falsificaciones antiguas tenían que ver con que sólo podían alcanzar valores o bienes jurídicos que tenían relación, con objetos físicos, visibles, que se percibían con los sentidos, siendo un problema toda vez que eran situaciones donde no existía dinero transable, por el contrario asientos contables como por ejemplo. En el código de 1995 no sólo se preocupa de los objetos físicos, también de bienes intangibles como son los datos, descubrimiento de secreto[441], y espionaje industrial[442].

[441] CPE Artículo 197. 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. 3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con

Ahora bien, como los activos patrimoniales son considerados susceptibles de apropiación, conduce a hablar de prevención, por lo mismo se produjo un cambio importante para dar cabida a las nuevas situaciones, de esta manera con el transcurso del tiempo, era más imprescindibles regular el fraude informático, adecuarlo a la nueva realidad puesto que al utilizar máquinas destinadas a realizar las acciones bancarias o de cualquier otro tipo era imposible aplicar el tipo básico de estafa,

las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior. 4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando: a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior. 5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior. 6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años. 7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

[442] Código Penal Español artículo 278.1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses. 2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos. 3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

siendo uno de los mayores problemas el *elemento engaño*, al hablar de ordenadores, programas, toda vez que las máquinas no se pueden engañar sino, que manipular[443].

Es dable hacer presente, que la reforma al Código Penal Español, no tenía por fin regular los delitos informáticos sino que las conductas de tipo fraudulentas que tenían que ver con entidades bancarias, donde algún tercero podía operar terminales de pago, realizar transferencias o inclusive los mismos funcionarios o empleados de la entidad financiera[444]. En definitiva el Código Penal, habla de hurto, de apropiación indebida u otros imposibles enjuiciar en relación al tipo de delitos informáticos, legislando y agregando en definitiva el apartado del artículo 248.2 del Código Penal Español, con el fin de hacer frente a esta nueva forma de criminalidad.

El legislador en el caso de la estafa puntualizó, sobre la base de la conducta típica del delito, abarcando los casos de estafa informática, utilizando un método destinado a complementar los tipos legales existentes, tomando en consideración las nuevas tecnologías y su rápido avance y la gran cantidad de formas de comisión o su constante transformación a medida que la tecnología avanza.

A pesar de los cambios en la legislación la rapidez de la red hace que las normas que van adoptando los países se muestren lentas, estamos ante un delito de

[443] De esta manera, se puede hacer mención a la STS, de 19 de abril de 1991 donde los juzgadores indican que el tipo de estafa básico, no puede contener los supuestos de un fraude informático indicando "mal puede concluirse la perpetración de un delito de estafa por parte el procesado, al impedirlo la concepción legal y jurisprudencial del engaño, al que se produce e incide por y sobre personas. La inducción a un acto de disposición patrimonial sólo es realizable frente a una persona y no frente a una máquina. Con razón se ha destacado que a las máquinas no se les puede engañar, a los ordenadores tampoco, por lo que los casos en que el perjuicio se produce directamente por medio del sistema de informático, con el que se realizan las operaciones de desplazamiento patrimonial, no se produce ni el engaño, ni el error necesario para el delito de estafa".

[444] FERNÁNDEZ TERUELO, Javier, *Crimen en los delitos cometidos a través de internet*, Editorial Constitutio Criminalis Carolina, Oviedo, 2007, pág. 46.

trascendencia de fronteras con el consiguiente problema que ello trae consigo, tomando en consideración que hay personas que indican que la red debe ser intervenida penalmente, ya que hoy se está viviendo una expansión del Derecho Penal[445], tal expansión se concreta en el derecho penal simbólico, aunque frente a esta posición amplia está la que aboga, por un derecho penal mínimo.

Podemos decir entonces, que actualmente se está viviendo una expansión del derecho penal, concretándose en tipologías cuyos bienes jurídicos, afectan a las personas de aquellos otros que afectan al patrimonio, esta categoría penal autónoma es coincidente con el objeto de protección actual de estos tipos penales, debiendo adaptarse las nuevas formas de comisión, es decir a la división que trae este tipo de criminalidad, como lo son los atentados patrimoniales, contra elementos informáticos y atentados patrimoniales realizados por medio de sistemas informáticos, siendo aquí donde se encontraría entonces, el fraude informático siendo su diferenciación principal, el modus operandi de este tipo de fraude.

Como se indicó anteriormente, al mismo paso que se han ido agregando tipos penales que requieren, para que se configure el uso de tecnología, se ha ido legislando y estudiando este tipo de fenómeno, siendo las nuevas conductas fraudulentas las cuales están unidas al uso de la nueva tecnología informática, las cuales han sido objeto de controversia jurídica, en relación a los tipos básicos o tradicionales en relación al mismo tipo penal. Así las cosas, el tipo básico que se tipifica en el artículo 248 del Código Penal, recoge varias conductas, que si no fuera porque el legislador indica al inicio de cada numeral una referencia a su inclusión dentro del tipo, nada haría sospechar que forman parte del mismo concepto de estafa, de esta manera la reforma operada por la LO 5/2010, de 22 de junio, llevó un

[445]ÁLVAREZ VIZCAYA, Maite, *Consideraciones político criminales sobre la delincuencia informática, el papel del derecho penal en la red, en internet y derecho penal*, Cuadernos de Derecho Judicial, (2001), pág. 260 y 261.

importante cambio en este ámbito encontrándonos en este momento con una extensión, entre el delito tradicional de estafa, que se regula en el artículo 248.1 del código penal español y los diferentes ilícitos cuya comisión, nos entrega como un enunciado el legislador en el número segundo, al indicar *también se consideran… Estafa*, las conductas que allí se señalan.

Además de ello nos entrega o introduce una modalidad de estafa impropia en el apartado 248.2 letra c), en el cual regula las operaciones fraudulentas que se cometan con las tarjetas de crédito o débito o con los cheques de viaje, o los datos obrantes en cualquiera de ellos. El nuevo tipo penal de estafa informática que regula el artículo 248.2, del código penal español de 1995, que regula una modalidad de la estafa, teniendo conceptos relativos a la penalidad de la misma forma ya grabaciones, si bien es cierto tiene semejanzas con la estafa genérica del artículo 248.1 estas no son de relevancia, puesto que se considera por los variados autores que lo adecuado, debiera creado haberse creado una figura distinta e independiente de la estafa[446]. En definitiva la nueva regulación eliminó de alguna manera la laguna legal existente, introduciéndose este nuevo tipo penal por razones político criminal, toda vez que al no existir un tipo penal que regulara la manipulación informática, las figuras tradicionales de estafa y también del hurto o la apropiación indebida, no daban el ancho para sostener este ilícito moderno, por ello dicha manipulación quedaba impune, y así debió regular legislador, incluso hasta cuando se habla o se trata el fraude informático de actos preparatorios.

Hasta el momento se ha hablado o referido indistintamente tanto a fraude como estafa, por ello se hace necesario, explicar las diferencias entre ambos vocablos, ya sea para asimilarlos o derechamente para encontrar alguna diferencia

[446] SUÁREZ GONZÁLEZ, Carlos, en RODRÍGUEZ MOURULLO (dir.)/ BARREIRO (coord.), Comentarios al Código Penal, Editorial Civitas, Madrid, 1997.

entre ello, puesto que al parecer tanto en la jurisprudencia como en los textos legales se usan de forma variada, por ello el titulo siguiente se abordará un estudio breve acerca del fraude, estafa y por supuesto el fraude informático.

IV. Antecedentes de la estafa informática

El Código penal de 1973 no contemplaba la estafa informática, utilizándose el delito de estafa genérico en su artículo 528[447], sin embargo fue modificado por la Ley 8/1983. Posteriormente cuando comenzó a regir el Código penal de 1995, se incluyó la calificación jurídica del delito estafa informática, añadiendo en el apartado segundo del artículo 248, "también se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la trasferencia no consentida de cualquier activo patrimonial en perjuicio de tercero".

Nuevamente con la Ley Orgánica, 15/2003, a pesar de no alterar la redacción del apartado anteriormente indicado, se introduce un apartado tercero en el artículo, indicando que se sanciona como estafa informática no sólo al que comete la defraudación patrimonial, sino también al que utiliza los medios tecnológicos para ello, adelantando el legislador y castigos timando como autor de la conducta penalmente reprochable, no solamente a la persona que ejecuta desplazamiento

[447] Artículo 528 (hasta 1983): "Cometen estafa los que con ánimo de lucro utilizan engaño bastante para producir error en otro, induciéndole a realizar un acto de disposición en perjuicio de sí mismo o de tercero. El reo de estafa será castigado con la pena de arresto mayor, si la cuantía de lo defraudado excede de 30.000 pesetas. Si concurrieren dos o más circunstancias de las expresadas en el artículo siguiente o una muy cualificada, la pena será de prisión menor. Si concurrieren las circunstancias primera o séptima con la octava, la pena será de prisión mayor. Si concurriere sólo alguna de las circunstancias del artículo siguiente, la pena se impondrá en su grado máximo".

patrimonial, sino también quien que desarrolla de alguna forma los artificios necesarios para llevar a cabo el delito patrimonial, indicando "la misma pena se aplicará a los que fabricaren, introducir en, poseyeren o facilitaren programas de ordenador específicamente destinados a la Comisión de las estafas previstas en este artículo".

Finalmente en el año 2010, el legislador añade algo más en cuanto la estafa informática se trata, agregando como forma de estafa informática tres modalidades diferentes en tres apartados distintos, dentro del apartado segundo del artículo 248 del Código penal, es decir las letras a y b son las modalidades que ya existía, incluyéndose una tercera letra c), a saber *"los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero"*[448].

El tipo básico de estafa o tradicional, con anterioridad a la entrada en vigor del Código penal de 1995[449], producía discusión acerca de las conductas en las cuales el interlocutor del sujeto activo era una máquina, puesto que un sector de la doctrina entendía el error como elemento independiente del delito estafa, cuya misión principal era la de delimitar el ámbito del engaño típicamente relevante y en

[448] Artículo modificado por la Ley Orgánica 5 del /2010, de 22 de junio.

[449] Al respecto refiere MATA Y MARTÍN, "la lucha frente la criminalidad informática desborda naturalmente el campo exclusivo del Derecho penal, pues se trata de un fenómeno cuyo control reclama además otros instrumentos más amplios y complejos (del tipo jurídico no Penal, de tipo técnico, formativo, así como educativo). Sin embargo es preciso bordar con seriedad y estudio profundo las implicancias penales de las tecnologías informáticas y de la comunicación. El legislador Penal antes de tomar decisiones apresuradas en este campo deberá contar con estudios informes previos de personas e instituciones especializadas en su análisis. Una política criminal racional es imprescindible en este terreno tan abonado al alarmismo, alejada de la conmoción producida por determinados hechos, por importantes que sin duda resulten, si se quiere obtener una respuesta legal adecuada y de largo alcance. MATA Y MARTÍN, Ricardo, *Criminalidad informática: una introducción al cibercrimen*, En revista de actualidad Penal número 37, (trabajo que forma parte del desarrollo del proyecto de investigación de la junta de Castilla y León sobre Protección penal del consumidor en el comercio electrónico), 2003, pág., 936.

función del cual debían medirse los parámetros de imputación objetiva del resultado. Entonces existía consenso en que la máquina no puede ser engañada, puesto que es imposible inducir a error al ordenador, porque se le induce actuar correcta o incorrectamente de acuerdo a las órdenes o comandos que se introducen en el sistema.

A finales de los años 80, comenzó la llamada revolución informática, llegando a influir en la jurisprudencia, donde ya existía negación para calificar el delito de estafa, cuando existían supuestos donde se provocaban transferencia de suma de dinero determinada de cuentas corrientes de clientes de algún banco, puesto que se manipulaba el ordenador calificándolo a través del tipo penal de apropiación indebida, al unir al sujeto activo con las cuentas corrientes[450]. Otra parte de la doctrina entendía que el engaño típico no debe conllevar necesariamente un tipo de relación inter-subjetiva con un tercero, lo que se suma a la configuración del error como elemento dependiente del engaño típico[451]. Por otro lado, debe entenderse que en el delito estafa ante de la reforma, se mantenían las opiniones de lo que ha dado en llamarse interpretación clásica de elementos típicos. Desde el punto de vista del

[450] De esta manera en la sentencia de 19 de abril de 1991 donde resuelve el recurso de casación presentado contra la sentencia referida de la audiencia Provincial de Granada el Tribunal Supremo admite un concepto material de documento, en un sentido idéntico a la audiencia Granada, pero rechaza la calificación de estafa, no considerando aquí posible una interpretación teleológica, del tipo de la estafa, estimándolo contraria al principio de legalidad, por lo mismo argumento definidos en la doctrina. La conducta no quedan obstante, impune, pues, ávidos efectuado por un empleado de la entidad bancaria en cuyo sistema informáticos ejecutaron las anotaciones ficticias, entren del tribunal que cabe aplicar el delito de apropiación indebida. GUTIÉRREZ FRANCÉS, María luz, *Los fraudes informáticos en el nuevo código penal*, Departamento de justicia al centro de estudios jurídicos y formación especializada, Cataluña, 1996, pág. 215 y sigs.

[451] XALABARDER PLANTADA, Raquel, *Derecho y nuevas tecnologías*, PEGUERA POCH, Miguel (coordinador), Capítulo IX, Editorial UOC, Barcelona, 2005, pág. 413 y sigs.

delito de estafa informática, este cambio no sólo aclaró un problema de seguridad jurídica, sino que más aún, subsanó una laguna de punición[452].

El artículo 248. 2 a) contempla, la *estafa informática*, la cual se asienta dentro del concepto más general de los fraudes informáticos, recordando entonces los cuatro elementos de la estafa, es decir engaño con una presentación falsaria de una determinada realidad; error que se sufre a consecuencia del engaño; ánimo de lucro en el sujeto activo; disposición patrimonial de sujeto pasivo. Sin embargo ello, y según lo anteriormente analizado respecto del tipo básico de estafa, la estafa informática no se ajusta, con la anteriormente descrita o con la dinámica comitiva de la estafa tradicional, puesto que en este tipo distinto, donde se le agrega al estafa tradicional el apellido *informática*, no existe realmente engaño o error, toda vez que estamos en presencia como se dijo de una máquina, la cual no tiene o por lo menos por ahora una psicología que puede ser objeto de un posible engaño. Este tipo de estafa, descansa sobre ciertos elementos diferentes a la clásica estafa, puesto que el legislador en su estructura, contempló la expresión *manipulación informática o empleo de artificio semejante,* que viene a equivaler al engaño de la estafa tradicional, no olvidando que en ambos tipos de estafa, debe existir un perjuicio

[452] La técnica de formulación normativo utilizar el Código penal de 1995 puede calificarse muy peculiar, considerando que en lugar de crear tipos delictivos autónomos, (Alemania e Italia), se prefirió modificar y extender el ámbito de aplicación de los delitos tradicionales. Por una parte, se introdujo dentro de los delitos tradicionales subtipos autónomos para castigar las nuevas modalidades ilícitas. Y por la otra, se amplió el ámbito de los objetos materiales de aquellos delitos que presentaban analogías con los nuevos hechos delictivos. Un ejemplo paradigmático de la adopción de la primera técnica de formulación normativa es el delito de fraude informático (artículo 248.2 del Código Penal). Con respecto al delito tradicional de estafa (artículo 248.1 del Código Penal) el fraude informático, se realiza por parte del que obtiene un acto disposición patrimonial mediante una conducta de tipo *lógico*, es decir, a través de una manipulación informática u otro artificio semejante, que ocupa el lugar del engaño que induce un tercero a error. SALVADORÍ, Iván, *Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5 /2010.* Perspectiva de derecho comparado, ADPCP, Vol. LXIV, 2011, pág., 226.

económico, que va a sufrir el sujeto pasivo a raíz de las consecuencias del ataque informático patrimonial.

Antes de analizar el tipo en todo su ámbito, vale indicar que en cuanto a la modalidad de acción, se puede actuar sobre el sistema, esto es directamente sobre la máquina que realiza el acto, acto que va ser erróneo de disposición patrimonial o también se puede actuar sobre el programa, ya sea manipulándolo en forma previa a que se concrete su instalación o en forma posterior una vez que ya está en funcionamiento.

A modo de aclaración previa, en los casos que se utiliza internet, como por ejemplo son en los casos de subasta en la red, que no entrega el producto que ha sido anunciado por ese medio y pagado, lo cual vendría a ser una prestación de servicios, pudiendo llamarlos *fantasmas*, (en los cuales se les atribuye algún poder milagroso o por el contrario tienen costos altísimos, que no producen los efectos que prometen en dichos anuncios), constituirían *estafas tradicional* y no una estafa informática. Por esta razón cuando estamos en presencia, del artículo 248.2 del Código penal, ingresan los tipos de estafas donde el engaño, se realiza al sistema informático propiamente tal, como son por ejemplo el apoderamiento de contraseñas para acceder a distintas cuentas o como en el uso de tarjetas de terceros, por lo mismo el tipo penal requiere de manipulación y emplear distintos artificios contra o directamente sobre las máquinas, con el fin de perjudicar a terceros. Como existe norma legal expresa, aún que los conceptos entregados por el legislador como son manipulación informática y artificio semejante no son muy precisos, podemos hablar de estafa construyéndose el delito a base de la manipulación informática y

posteriormente con un resultado de transferencia de activos que no es consentida por el sujeto pasivo[453].

Ahora bien, si las empresas utilizan algún modo para no ser engañadas, como sería por ejemplo comprobar identidad junto con el producto bancario, nos trae como consecuencia, que dichos métodos son independientes de la acción delictiva toda vez que la consumación del tipo o su tentativa no requiere que el vendedor del bien o servicio se encuentre obligado a desplegar una batería de distintas formas de defensa[454]. Asimismo, es recomendable hacer la distinción, con otro tipo de delitos como sería por ejemplo el delito de falsificación de moneda cometido con el llamado dinero plástico, al copiar el contenido de las bandas magnéticas[455], toda vez

[453] STS N° 807, Sala 2ª de lo Penal, de 03. III. 2003 (Ponente: Excmo. Sr. D. Andrés MARTÍNEZ ARRIETA), la sentencia examina un caso de estafa informática, la cual se trata el interesante tema del engaño, ya que en el delito de estafa, al tratarse un delito relacional, entre personas, es claro que el engaño no debe producir el agente a la víctima. Sin embargo cuando la conducta se realiza frente a una máquina, mediante la forma con misiva del artículo 248.2 del C.P. nos encontramos con la denominada estafa informática. En el presente caso, si bien no es posible engañar a una máquina, hay una apariencia de titularidad de una persona hacia otra, a la que se engañen, usando una tarjeta electrónica que corresponde a otra persona.

[454] STS N° 1476, Sala 2ª de lo Penal, de 21. XI. 2004 (Ponente: Excmo. D. Enrique BACIGALUPO ZAPATER). Esta sentencia se hace cargo del delito de estafa informática del artículo 248.2 del Código Penal, en la cual los hechos en forma medular son: el hijo de los propietarios del establecimiento de deporte, irrumpe de madrugada del mismo, acompañado de una joven, manipulando el terminal punto de venta, fingiendo ventas que cargaban en la tarjeta visa de la joven, a la cual, en forma de supuestas devoluciones, se le ingresaron unos 52 millones de pesetas. La sentencia considera que estamos ante un delito de estafa informática del artículo 248.2 del C.P., ya que el autor se ha válido de *alguna manipulación informática*, como requiere el subtipo. Indicando o examinando también, quien sea el sujeto pasivo de este delito, concluyéndose que lo es el titular del patrimonio perjudicado, el banco, aunque finalmente sean los padres de uno de los condenados, lo que hubieron de responder civilmente.

[455] STS N° 948, Sala 2ª de lo Penal, de 08. VII. 2002 (Ponente: Excmo. Sr. D. José Manuel MAZA MARTÍN), dicha sentencia trata del delito de falsificación de moneda, cometido mediante el llamado *dinero plástico*, al copiar el contenido de las bandas magnéticas de tarjetas de crédito de sus titulares, y realizar nuevas tarjetas, a nombre del acusado. Para, a continuación realizar diversos pagos, en diferentes establecimientos comerciales. La referida sentencia, indica que se trata de un delito de falsificación/fabricación de moneda, del artículo 386.1 del C.P. al haber confeccionado tarjetas mediante la sustitución de los datos auténticos contenidos en la banda magnética de las

que por un lado no estamos ante un delito del artículo 248.2 del Código penal, toda vez que cosa distinta es que se manipulen sistemas informáticos para defraudar, y otra, que se confeccione una tarjeta mediante la incorporación falsaria de datos de origen o producción informática para, con ella, posteriormente, llevar a cabo actos con contenido fraudulento.

Vale señalar, que la forma en que legislador español, reguló la estafa informática, fue a través de la tipificación *amplia o general* de este delito, no tomando como referencia otros modelos donde se entrega un catálogo de conductas comisivas. Ahora bien, como indica CORCOY BIDASOLO, al referirse la estafa cometida por medios informáticos, indica que "se diferencia de la estafa común en que no existe alteridad entre sujeto activo sujeto pasivo del engaño, no hay relación interpersonal entre ambos. Eso es lo que hacía que no pudiese estimarse estafa en los casos de engaño una máquina. Agregan mismo autor, "las estafas comunes cometidas en la red, sino las estafas cometidas con manipulaciones informáticas. Ejemplo de una posible estafa común (artículo 248.1) cometida la red: en algunas páginas web de subastas se realizaba el siguiente operativo: se mostraron imagen del producto a subastar, acabada la puja se enviaban mejor postor lo subastado dos. Imagen, la fotografía, no el objeto representado en ellas"[456]. Se debe entender, que lo que se regula, no son las estafas cometidas en la red, sino que los *supuestos de estafa cometida con manipulación informática,* es decir, aquellas manipulaciones del proceso de elaboración electrónica de cualquier clase y en cualquier momento de

mismas. Por ende, fabricar equivale a confeccionar ex novo, por lo que el verbo nuclear del delito encaja perfectamente en el artículo mencionado según el acuerdo del pleno de la sala segunda del Tribunal Supremo, de fecha 28 de junio de 2002.

[456] CORCOY BIDASOLO, Mirentxu, *Manual práctico de Derecho penal, Parte especial*, Doctrina y jurisprudencia, con casos solucionados, 2ª edición, Editorial Tirant lo Blanch, Valencia, 2004, pág., 588.

éste, con la intención de obtener un beneficio económico, causando un tercero un perjuicio patrimonial[457].

A) Ubicación del tipo en el Código Penal

El 27 de noviembre de 2009 se presentó el proyecto de reforma de la Ley Orgánica 10/1995, de 23 de noviembre, esto es, al Código penal vigente, que tenía por objeto principal dar ejecución a los mandatos internacionales y lograr de alguna manera cubrir, los delitos respecto de los cuales existía imposibilidad de perseguir.

La técnica que se utilizó en el código penal de 1995 ha sido criticada y calificada de peculiar, como sucede con la técnica utilizada para la formulación normativa del delito de fraude informático, toda vez que aunque existió un esfuerzo de legislador de integrar de adaptar los nuevos delitos informáticos a los tipo ya existentes, se dice que trato de responder a la idea de que la llegada de las nuevas tecnologías hubiese comportado un cambio de las modalidades de agresión a los bienes jurídicos clásico, recurriendo a la creación de artificiosas y poco apropiadas formulaciones legislativas ya una discutible ubicación sistemática de los nuevos delitos informáticos dentro del Código penal. De esta manera se dice que la técnica utilizada, posicionó a los nuevos tipos penales (protección de información, integridad y disponibilidad de los datos y sistemas informáticos), junto a los tipos delictivos tradicionales que representan respecto de ellos algún tipo, desemejanza o analogía[458].

---

[457] BALMACEDA HOYOS, Gustavo, *Revista de derecho y ciencias penales…*Op. Cit., pág, 135.

[458] SALVADORÍ, Iván, *Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5 /2010*. Perspectiva de derecho comparado, ADPCP, Vol. LXIV, 2011, pág., 225 y sigs.

El fraude informático debería estar ubicado dos secciones más adelante en el mismo capítulo, esto es, en la sección tercera que trata de las defraudaciones de fluido eléctrico y análogas, ya que como dice *Bueno Arús*, le informáticos se refiere, no ya al objeto de protección sino lo medio utilizado para la comisión del delito. De hecho, la defraudación informática es análoga a la realizada al fluido eléctrico[459], e incluso, el artículo 256, dedicado a estas defraudaciones análogas, castiga al que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento del titular, ocasionando a este un perjuicio[460].

El tipo penal del artículo 248.2 como el del artículo 256 el bien jurídico protegido es el mismo hacer similar un equipo terminal de telecomunicaciones en equipo informático o artificio semejante refiere a mayor abundamiento aquel tipo, y que en ambos casos se trata de un uso no consentido, corroborando así, no sólo la misma naturaleza delictiva sino también el mismo medio comisivos.

Por último, refiere GONZÁLEZ EXTREMERA, que "la inclusión del fraude informático junto a la estafa o mejor dicho, formando parte de ella ha pesado más *elemento perjudicial patrimonial* que el de *engaño bastante a otro*, sin embargo la doctrina jurisprudencial, establece el elemento nuclear de la estafa es el engaño y que es éste el que a su vez permite diferenciar aquella de otras figuras delictivas,

[459] En relación al elemento lógico, y puesto que su importancia económica parece fuera de toda duda, la cuestión a determinar es, pues, si se corresponden con esta noción de cosa. En este sentido, debe recordarse que el elemento lógico (software, ficheros) no son, sin un conjunto de información, ideas instrucciones que se recogen en un medio al que se accede eléctricamente. Lo elemento lógico pueden ser considerados, por tanto, como una especie de *flujo electromagnético*, lo que permite que su consideración Penal pueda plantearse de forma semejante a la de la energía eléctrica. GONZÁLEZ RUS, Juan, *Nueva forma de delincuencia, Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos*, Número especial IX, Consejo General del Poder Judicial, Madrid, 1988, pág., 43.

[460] GONZÁLEZ EXTREMERA, Josep, *La estafa mediante título mercantil abstracto*, Editorial Metropolitana, Santiago de Chile, 2008, pág. 213.

como la apropiación indebida el hurto o el alzamiento de bienes. Por otro lado el perjuicio patrimonial es el elemento característico de los delitos económicos, mientras que el concepto de engaño bastante otro lo es como diferenciador de la estafa de los demás delitos que integran el más amplio grupo que tienen común aquel desplazamiento"[461].

B) Concepto de estafa informática

La estafa propiamente tal, es un delito clásico patrimonial que se encuentra tipificado nuevamente jurídico español como la perpetración de un desfalco a una tercera persona, utilizando para ello un ardid o argucia, de tal magnitud o elaborada que permite engañar a esa persona de manera suficiente bastante, como para que se ejecute un desplazamiento patrimonial que de otro modo nunca hubiera realizado.

Ahora bien, las llamadas *estafas por ordenador* pueden definirse como toda manipulación o alteración del proceso de elaboración electrónica de cualquier clase en cualquier momento de éste, realizada con ánimo de lucro y causando un perjuicio económico de un tercero. Es decir cuando ya se tiene la definición del delito de estafa tradicional, la estafa por medios informáticos es una modalidad de realizar la conducta delictiva de la estafa básica, pero debe agregarse que lo empleado para poder realizarlo, es un medio o sistema informático[462]. En este caso la manipulación informática, viene siendo trascendente para la alteración o modificación de los datos que pueden consistir en su supresión, en la introducción de nuevos datos falsos, en su modificación dentro del programa, en colocar datos en distinto momento lugar, o

[461] GONZÁLEZ EXTREMERA, Josep, *La estafa…*op. cit., pág. 214.

[462] FLORES PRADA, Ignacio, *Criminalidad informática, aspectos sustantivos y procesales*, Editorial Tirant lo blanch, Valencia, 2012, pág. 202.

en valorar las instrucciones de elaboración. Según lo anterior, cuando toman presencia de estafa tradicional o básica, no constituiría estafa informática, cuando existe una conducta que se inicia por engaño real, físico o directo con el fin de obtener datos o algún tipo de información o soporte, para que posteriormente éstos mismos puedan ser utilizados a través de artificios informáticos[463].

[463] STS, Sala 2ª en lo Penal, N° 662, de 14. X. 2008. (Ponente: Sr. Joaquín GIMÉNEZ GARCÍA), dicha sentencia, se refiere "que por la vía del error iuris se denuncia la indebida aplicación del artículo 248.1 estafa básica, y se postula la figura de la estafa informática del artículo 248.2 del Código penal, resulta sorprendente esta tesis porque la estafa informática es igualmente delito sancionado con igual pena que la estafa básica, de la que se separa el modus operandi, ya que constituyen una manipulación o artificio informático, no existe engaño porque no puede ser engañado una máquina un sistema informático, por ello nada afecta a la punición ni tendría relevancia penal desde la perspectiva del recurrente. Sin embargo la figura informática no concurren este caso porque la actividad de las cajas concernidas al acceder a la apertura de una cuenta corriente facilitando al recurrente un TPV era precisa e indispensable para el modus operandi del recurrente, y para conseguirlo, éste aparentó ante aquellas una solvencia y seriedad suficientes como para que aquéllas creyeran, erróneamente, su aparente intención. No hubo una exclusiva manipulación informática o científica semejante a la que se refiere el párrafo 2° del artículo 248 del Código penal".

CAPÍTULO VI

Imputación típica del delito de estafa informática

I. Imputación típica en el ámbito del tipo objetivo

Para que una acción humana alcance significación en el ordenamiento jurídico, debe reunir los elementos normativos correspondientes, es decir al acreditarse las características de la tipicidad, con ello se indica la subsumibilidad o adecuación de la conducta un precepto legal incriminado[464]. La tipicidad es un elemento esencial del concepto de delito, los conceptos de tipo y tipicidad se exigen mutuamente aunque son dos nociones diferentes, puesto que el tipo es un instrumento legal para determinar y describir las acciones penalmente relevantes, apartando las de las que no lo son, vendría siendo entonces un elemento externo al delito, una técnica legislativa del Derecho penal. En cambio la tipicidad no es un instrumento legal, sino un elemento del delito y por ello algo interno, pertenece la esencia del mismo[465].

Vale se presente o aclarar cómo lo que se analizará a continuación no serán las estafas comunes cometidas en la red, sino aquellas estafa cometida con manipulación informática, las cuales son cometidas con manipulaciones del proceso de elaboración electrónica, con la intención de obtener un beneficio causando a un tercero un perjuicio patrimonial, con ello se persigue que manipulaciones de esta clase no queden impunes, siendo castigados como delitos de peligro que y como

[464] POLAINO NAVARRETE, Miguel, *Derecho Penal*, *Parte general*, tomo II, Teoría jurídica del delito, Editorial Bosch S.A., Barcelona, 2000, pág. 20 y sigs.

[465] POLAINO NAVARRETE, Miguel, *Derecho Penal*, *Parte general*…op. cit., pág. 125.

delitos consumado, conductas en fase tentativa[466]. De acuerdo lo anterior las estafas cometidas con manipulación informática también pueden cometerse a través de Internet o de la red[467]. Galán Muñoz estima que la conducta típica del delito de estafa informática, responde a dos posibles modalidades delictivas alternativas en este delito, considerando entonces, que su estructura típica correspondería a la de los denominados tipos mixtos alternativos, puesto que la acumulación real de sus posibles de alternativa modalidades con misiva, sólo daría lugar a un único delito.

El mismo autor aclara en este sentido indicando por ejemplo si para obtener una transferencia patrimonial el autor de este delito realizase una manipulación informática ya además una conducta análoga, como sería el caso de la utilización de un artificio a ella semejante, no estaríamos en presencia de la Comisión de los delitos diferentes de estafa informática en concurso, sino tan sólo uno[468].

A) Sujeto activo y pasivo

En relación con el sujeto activo no se presentan particularidades relevantes, pudiendo cometer el delito tanto las personas legitimadas para acceder al sistema, como terceros no autorizados, siempre que para conseguir el fraude recurran a alguna manipulación informática. Mayores dificultades presenta la delimitación del sujeto pasivo, toda vez que la particular dinámica comisiva de esta infracción hace que muchas veces, además del titular del patrimonio defraudado, se vea implicada alguna entidad bancaria, puesto que éstas asumen en ocasiones los perjuicios

[466] CORCOY, Mirentxu / JOSHI, Ujala, *Delitos contra el patrimonio cometidos por medios informáticos*, En revista jurídica Catalunya, vol. 87 N° 3, 1988, pág. 141.

[467] HERRERA MORENO, Mirian, *El fraude informático en el derecho penal español*, Revista de Actualidad Penal, número 39, Sevilla, 2001, pág. 954 y sigs.

[468] GALÁN MUÑOZ, Alfonso, El fraude y la estafa mediante sistemas informáticos, análisis del artículo 248.2 Código penal, Editorial Tirant Lo Blanch, Valencia, 2005, pág. 559.

causados a sus clientes cuando la defraudación tiene lugar, a través del sistema informático de la propia entidad. Con todo, como es común en los delitos patrimoniales, debe reputarse sujeto pasivo al titular del patrimonio afectado por la acción delictiva, sin perjuicio de que el banco pueda ser perjudicado civil si abonare a su cliente la cantidad estafada, subrogándose en su lugar frente al responsable civil. A diferencia de lo que ocurría anteriormente, que se decía que la criminalidad económica, se vinculaba a un tipo delincuente de cuello blanco, hoy en día cualquier persona puede serlo, y cometer una estafa informática. Por ello, pueden ser sujetos activos tanto las personas legítimamente autorizada para acceder y operar en el sistema, como tercero no autorizado que exceden a las terminales públicas o privadas o intercepte líneas[469].

En cuanto sujeto pasivo, la doctrina señala que vendría siendo la víctima sobre la que recae la acción, cuando es propiedad es estrictamente el portador del bien jurídico lesionado, puesta en peligro debido y que no debe ser confundido, aunque puede coincidir, con la persona o cosa sobre la que recae la conducta delictiva, es decir el objeto material del acción. Por ello se dice, el artículo 248.2, es estrictamente patrimonial de una perspectiva microsocial individual, entonces sujeto pasivo del mismo será única y exclusivamente el titular del derecho patrimonial que sufre el detrimento del mismo. Es dable señalar que el objeto material sobre el que recae la acción son los datos, los programas o la información sí misma, y el equipo sistema informático, tanto físico como lógico, y son también el medio aunque no lo único de comisión directiva[470]. Por último, la condición de perjudicado casi siempre coincide con quien tiene la condición de sujeto pasivo, pero sí lo fueron tercero,

[469] ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Editorial Comares, Granada, 2002, pág. 565 y sigs.

[470] ROVIRA DEL CANTO, Enrique, *Delincuencia informática…*op. cit., pág. 657 y sigs.

además del titular del sistema informático como directamente por dedicado su patrimonio, el que lo resultará indirectamente, se podría hablar de un tercero perjudicado.

B) Conducta típica (acción y omisión)

Esta conducta típica[471], viene a llenar una importante laguna de punibilidad que existían el rodamiento jurídico español puesto que como se dijo anteriormente el tipo básico no cumplía con los estándares necesarios para los delitos de la nueva tecnología[472]. El artículo 248.2 a) del Código penal, expresa que "*también se consideran reos de estafa: a) Los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la trasferencia no consentida de cualquier activo patrimonial en perjuicio de otro"*[473].

1. Comisión del delito de estafa informática

La acción positiva opción activa, constituye aquella forma de conducta que infringe una norma prohibitiva, a través de la ejecución de un determinado comportamiento positivo por parte sujeto[474]. Resulta del todo indiscutible que la

[471] Artículo 10 Código Penal español: Son delitos las acciones y omisiones dolosas o imprudentes penadas por la ley.

[472] Refiere el TS, "Es bien conocido que el tipo penal del artículo 248.2 del Código Penal (hoy 248.2. a) advino al Código Penal de 1995 como remedio para la atipicidad persistente tras la reforma de 1983, de comportamientos defraudatorios caracterizados por la utilización de medios informáticos". STS, 2ª de lo Penal, N° 622, de 09. VII. 2013, (Ponente: Sr. Luciano VARELA CASTRO)

[473] El TS indica "También hemos dicho que cuando la conducta que desapodera a otro de forma no consentida de su patrimonio se realiza mediante manipulaciones del sistema informático, bien del equipo, bien del programa, se incurre en la tipicidad del art. 248.2 del Código penal". STS, 2ª de lo Penal, N° 368, de 09. V. 2007, (Ponente: Sr. Juan Ramón BERDUGO GOMEZ DE LA TORRO)

[474] POLAINO NAVARRETE, Miguel, *Derecho Penal, Parte general*, tomo II, Teoría jurídica del delito, Editorial Bosch S.A., Barcelona, 2000, pág. 268.

forma de cometer el delito estafa informática consiste en nacer positivo, y que la modalidad con misiva básica del delito, será la manipulación informática, elemento del tipo objetivo de tal delito, sobre el cual no existe una definición unánimemente aceptada por la doctrina[475]. La comisión este delito es activa, toda vez que legislador incluyó la conducta que puede ser llevada a cabo por el sujeto activo.

2. Comisión por omisión en el delito de estafa informática

Del mismo modo que la comisión, es decir el modo el hacer activo, puede la omisión integral una forma de conducta típicamente relevante, siempre que no se trate de un no actuar absoluto, un no actuar genérico, sino de un no hacer algo concreto y determinado cuya positiva ejecución es ordenada por una ley penal preceptiva respecto de determinados sujetos en determinadas situaciones jurídicas[476]. El Dr. POLAINO NAVARRETE, indica que respecto de la Comisión por omisión, dicha conducta humana con relevancia típica participa, en cierto sentido, de la estructura jurídica de las dos modalidades anteriores de comportamiento (la acción positiva y la omisión pura), en ella por un lado se infringe una norma penal prohibitiva de la realización del resultado antijurídico (como ocurre en los supuestos acción activa) y, por otro, el resultado típico se produce mediante un no hacer que infringen la norma preceptiva o de mandato (como en las hipótesis de omisión pura o propia)[477]. Ahora bien, el delito estafa informática el legislador lo tipifica como un delito con una extensión de la conducta típica conscientemente indeterminada, se establece una clara restricción de los comportamientos que para el mismo legislador son relevantes mediante una exigencia que deben ser idóneos, para que se genere una transferencia

[475] GALÁN MUÑOZ, Alfonso, *El fraude…op. Espacio…op. cit.,* pág. 560.

[476] POLAINO NAVARRETE, Miguel, Derecho Penal, Parte general, tomo II, Teoría jurídica del delito, Editorial Bosch S.A., Barcelona, 2000, pág. 268.

[477] POLAINO NAVARRETE, Miguel, *Derecho Penal*…op. cit., pág. 269.

no consentida de cualquier activo patrimonial[478]. Algunos autores han señalado que lo importante no es definir qué clase manipulación informática se trata, sino que por el contrario lo importante o relevante en la capacidad para lesionar el patrimonio ajeno, siendo la estafa informática aquella que manipulaciones adecuadas para transferir activos en forma no consentida[479].

Existe desacuerdo en la doctrina respecto de la comisión por omisión en el delito de estafa informática del artículo 248.2 a Código penal, sin embargo HERRERA MORENO, nos plantea una posibilidad de la Comisión por omisión en este delito, al analizar la admisibilidad de la ocultación de datos en cuanto a manipulación informática, toda vez que la ocultación de datos, cómo conducta activa, es decir cuando opera a partir de una red de positivo, no ofrece perfiles espinosos, sin embargo maniobras de ocultación serán por ejemplo, la presión de una tecla que impide positivamente que datos que han de ser conocidos accedan al ordenador, sin embargo, puede cuestionarse si es aceptable como manipulación la simple *ocultación omisiva*, en el sentido si equivaldría acción, conforme a la

[478] GALÁN MUÑOZ, Alfonso, El fraude…op. Espacio…op. cit., pág. 649. La conducta de la estafa informática no siempre se caracteriza por la alteración del funcionamiento del sistema informático; y mucho menos del resultado que se derivaría de un proceso de datos, ya que en ocasiones la comisión de este delito, ni siquiera requerirá que tales sistemas lleguen a efectuar proceso de tratamiento alguno con respecto a los datos que contienen o que se le introducen, limitándose los mismos a servir de soporte de la representación o anotación de la transferencia producida. La única exigencia de ineludible cumplimiento de la conducta realizada sobre un sistema informático, para que pudiese ser calificada como constitutiva de una estafa informática propiamente dicha, vendrá constituida por el hecho de que fuese adecuada para determinar una transferencia patrimonial real, efectiva y no consentida.

[479] Con cita a ROMEO CASABONA, también MAGLIONA MARKOVICTH y LÓPEZ MEDEL incluyen dentro de los ejemplos de manipulación del "input" a la "omisión de registro de datos. MAGLIONA MARKOVICTH, Claudio, *Análisis de la normativa sobre delincuencia informática en Chile, Derecho y Tecnologías de la Información*, Fundación Fernando FUEYO LANERI y Escuela de Derecho Universidad Diego Portales, Chile, 2002, pág. 55.

exigencia del artículo 11 del Código penal[480], regulador de la omisión impropia, por ello indica la autora, que la conducta ocultación consistente en una mera omisión de datos que han de ser exteriorizados, conformó la posición de garante que ostenta el autor[481]. MATA Y MARTÍN, también está de acuerdo con ello indicando que se admitimos como manipulación, como se hace muy habitualmente, el supuesto de no inclusión de los datos reales que deberían ser objeto de procesamiento, estamos ya abarcando la omisión y rechazar estos casos omisiva os habríamos de adoptar un concepto muy restrictivo de manipulación informática que generalmente no se toman consideración[482].

C) Descripción legal de la conducta típica[483]

[480] Artículo 11 Código Penal español: Los delitos que consistan en la producción de un resultado sólo se entenderán cometidos por omisión cuando la no evitación del mismo, al infringir un especial deber jurídico del autor, equivalga, según el sentido del texto de la Ley, a su causación. A tal efecto se equiparará la omisión a la acción: a. Cuando exista una específica obligación legal o contractual de actuar. b. Cuando el omitente haya creado una ocasión de riesgo para el bien jurídicamente protegido mediante una acción u omisión precedente."

[481] HERRERA MORENO, Mirian, *El fraude informático en el derecho penal español*, Revista de Actualidad Penal, número 39, Sevilla, 2001, pág. 954 y sigs.

[482] Es dable agregar que sin negar las dificultades para admitir la estafa por omisión y haciéndose cargo de que, en muchos casos, los que aparecen como supuestos omisivos son realmente comportamientos activos en sentido estricto, apunta que si admitimos como manipulación el supuesto de no inclusión de datos reales que deberían ser objeto de procesamiento (lo que se llama manipulación previa). MATA Y MARTÍN, Ricardo es, *Delincuencia informática y Derecho penal*, Editorial Edisofer, Madrid, 2001, pág. 54.

[483] Sin embargo, sin ser una estafa propiamente dicha, presenta importantes similitudes con la estafa (de ahí que se inserte en el art. 248 CP). Así, el bien jurídico protegido es el patrimonio (la referencia a cualquier activo patrimonial como objeto material sobre el que deba recaer la acción típica así lo avala). Además, la modalidad comisiva a través de manipulaciones informáticas tiende a conseguir una transferencia no consentida de activos patrimoniales. En suma, podemos decir que la criminalización de la denominada estafa informática, viene a colmar una laguna legal derivada de la inadecuación del tipo de estafa tradicional para hacer frente a determinados ataques al patrimonio mediante la alteración o manipulación de datos informáticos. REY HUIDOBRO, Luis Fernando, *La estafa informática: relevancia penal del phishing y el pharming, En La ley Penal*, En revista de Derecho penal, procesal y penitenciario, número 101, 2013, pág. 6.

En cuanto al tema y tomando en consideración la modalidad con misiva básica del delito estafa informática, a saber la manipulación informática, la definición entregada por Romeo Casabona, es una de las que ha tenido mayor acogida en Derecho Penal Español, el cual indica "que habría de entenderse por manipulación aquella, incorrecta modificación del resultado de un procesamiento automático de datos, mediante la alteración de los datos que se introducen o están ya contenidos en el ordenador en cualquiera de sus fases de procesamiento o tratamiento, siempre que sea con ánimo de lucro y perjuicio de terceros"[484].

1. Manipulación informática

Antes que todo, es necesario referirse al a la definición que entrega la Real Academia Española, la cual indica, que manipulación es *intervenir con medios hábiles y, a veces, arteros, en la política, en el mercado en la información…etc. Con distorsión de la verdad o la justicia, ya servicio de intereses particulares. Manejar alguien los negocios a su modo, o mezclarse los ajenos*[485]. El concepto descrito, no se acomoda a lo señalado por el legislador, teniendo que ampliarse según los términos referidos en la norma penal estudiar.

Ahora bien, en todo delito al cual hacemos referencia a informática, se tiene que distinguir el medio y el fin, con el objetivo que se puede encuadrar la acción dolosa 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

[484] ROMEO CASANOVA, Carlos, Poder informático y seguridad jurídica, La función tutelar del derecho penal ante las nuevas tecnologías de información, Editorial Fundesco, Madrid, 1988, pág. 47.

[485] Diccionario de la Real Academia Española, [accesible en]: <www.dle.rae.es>.

informática, y el fin que se persiga debe ser la producción de un beneficio al sujeto autor del ilícito, una finalidad deseada que causa un perjuicio a otro o un tercero[486].

El carácter informático, se planteado que puede deducirse acudiendo a la interpretación sistemática, tomando en cuenta lo que legislador plantea cuando existen conductas de criminalidad informática en el plano de la previsión de intimidad, como es en el delito descubrimiento revelación de secretos de carácter informático[487], entonces, lo indicado en dicho artículo es válido también para la manipulación de datos, y al tratar de manipulación de funciones, el referente que confiere a la acción su carácter informático será la afectación a un programa informático[488].

En forma general la doctrina se ha referido que el ordenador en cuanto a la materia se trata, debe entenderse como una instalación del proceso de datos, es decir una máquina en la cual se introducen los datos para ser procesados (input), en la forma en que el usuario necesite y con los programas adecuados para ello, después de esta operación se obtendrá un resultado (output), por ello, se debe distinguir entre supuestos de manipulación[489]. En cuanto la manipulación se refiere, distintos autores

[486] DAVARA RODRÍGUEZ, Miguel, *Manual de Derecho informático*, Editorial Thomson Aranzadi, 7ª Edición, Navarra, 2008, pág, 358.

[487] Artículo 197. 2 del Código Penal: "Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos ya que los altere o utilice en perjuicio del titular de los datos o de un tercero".

[488] HERRERA MORENO Myriam, *El fraude informático en el derecho penal español*, Revista de Actualidad Penal, número 39, Sevilla, 2001, pág. 953.

[489] La actual redacción del art. 248.2 del Código penal permite incluir en la tipicidad de la estafa aquellos casos que mediante una manipulación informática o artificio semejante se efectúa una transferencia no consentida de activos en perjuicio de un tercero admitiendo diversas modalidades, bien mediante la creación de órdenes de pago o de transferencias, bien a través de

indican, que se debe distinguir distintas formas en que opera la manipulación informática fraudulenta[490], con distintos supuestos: manipulación que pueda afectar tanto suministro o alimentación de datos[491], o también llamado *input*; manipulación que afecta a la salida de datos o también llamado *output*; manipulación en el

---

manipulaciones de entrada o salida de datos, en virtud de los que la máquina actúa en su función mecánica propia. En realidad, el engaño mediante un artificio como el utilizado por los acusados es equivalente al consistente en la "manipulación informática" que contempla el tipo delictivo, pues el precepto admite diversas modalidades, bien a través de manipulaciones de entrada o salida de datos, en virtud de los que la máquina actúa en su función mecánica propia. También se comete estafa del art. 248.2 a) C. P. cuando se emplea un artificio semejante. STS, 2ª DE LO PENAL, N° 364, DE 11. V. 2011, (Ponente: Sr. Diego Antonio RAMOS GANCEDO)

[490] PÉREZ MANZANO, propone circunscribir las manipulaciones informáticas a las alteraciones del software. Ciertamente, eso dejaría fuera del concepto de "alguna manipulación informática" a otras comúnmente aceptadas como estafas informáticas, en que la alteración afecta a los datos sobre los que opera el sistema e incluso sobre los elementos materiales del mismo -sin perjuicio de que pudiera calificarse de "otro artificio semejante", para lo que no cabe una respuesta dada de antemano por la semejanza general del proceso planteado, sino que hay que estar a circunstancias concretas de ese proceso. ANARTE BORRALLO, Enrique, *Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información, Derecho y conocimiento,* Vol. 1, Facultad de derecho, de la Universidad de Huelva, España, 2001, pág. 235.

[491] *Dato:* Representación simbólica (numérica, alfabética, etc.) de un atributo de una entidad. Un dato no tiene valor semántico (sentido) en sí mismo, pero al ser procesado puede servir para realizar cálculos o tomar decisiones. Los datos son susceptibles de ser comprimidos, encriptados, transmitidos y almacenados. Unidad mínima de información, sin sentido en sí misma, pero que adquiere significado en conjunción con otras precedentes de la aplicación que las creó, por ello en su conjunto de símbolos que unidos de cierta forma dan un significado lógico. Todo el software se divide en dos categorías: datos y programas. Los programas o aplicaciones son colecciones de instrucciones que manipulan datos, que pueden presentarse en variedad de formas, como números, texto, bits o bytes almacenados en memoria, etc. Ahora bien, técnicamente, los datos son hechos y cifras en bruto, tales como órdenes y pagos, los cuales se procesan para obtener información, por ejemplo el saldo deudor y el monto disponible. Sin embargo, en el uso común, los términos datos e información se toman como sinónimos. La cantidad de datos versus información que se guarda en el computador constituye una compensación. Los datos pueden procesarse en diferentes formas de información, pero toma tiempo clasificar y sumar transacciones. La información actualizada puede proporcionar respuestas inmediatas. Vale indicar que un error frecuente es creer que el software es también datos. El ordenador ejecuta o corre un software. Los datos se *procesan*, mientras que el software se *ejecuta*. [accesible en] <http://www.lawebdelprogramador.com>.

2. Cualquier forma de información, ya sea en forma electrónica o sobre papel. En forma electrónica, "datos" se refiere a archivos, bases de datos, documentos de texto, imágenes y, voz y video codificados en forma digital.

programa o en la consola[492]. Respecto el anterior y en cuanto a la manipulación se trata, hay que distinguir, tanto si se trata de una *manipulación propiamente tal*, una *manipulación de datos*, y de una *manipulación del bit* [493].

La manipulación propiamente tal, tiene por fin alterar la conducta de un sistema operativo, modificando su código, para cambiar la forma en que se ejecuta un programa. En cuanto la manipulación de datos, tiene lugar en el procesamiento de los mismos, es decir cuando se instalan programas informáticos con comando determinados, con ello se pueden manejar los datos existentes de distinta manera, entregando órdenes distintas al *hardware* para que realice los datos. Y al hablar de manipulación de *bites*, la acción dirigida a cambiar sólo uno o varios bites individuales dentro de un byte[494], nos referimos a la manipulación de bites operaciones bit a bit, que son algo común en los programas de micro-controladores, puesto que permiten configurar los registros para usar el *hardware* incluido, también

[492] ROVIRA DEL CANTO, Enrique, *Hacia una expansión doctrinal y táctica del fraude informático*, En revista de derecho y nuevas tecnologías, Número 3, Editorial Thomson Aranzadi, 2003, pág. 133.

[493] El *Bit*: (Binary Digit o Dígito binario). Es la unidad digital más pequeña que puede manejar una computadora. Se maneja a través del sistema binario, es decir, puede tener dos estados: 1 ó 0. Con la combinación de ocho bits (ej: 00110010) se forma un *byte*. [accesible en] <www.alegsa.com>.

[494] El *byte*: es la unidad de información digital formada usualmente por ocho bits (serie de ceros y unos). Según cómo estén combinados esos ocho *bits*, formarán un byte que representa un carácter de texto determinado en un ordenador, es decir, el *byte* es la unidad que la mayoría de los ordenadores actuales utilizan para representar un carácter como una letra, un número y otros símbolos. El tamaño del byte depende del *hardware* empleado en el ordenador, pero históricamente el más popular ha sido el de 8 *bits* (llamado octeto). Estos 8 *bits* permiten 256 combinaciones y, por lo tanto, representar 256 caracteres diferentes. El *byte* es la menor unidad de memoria accesible en la mayoría de las arquitecturas de ordenadores. En otras palabras, es la unidad de datos más pequeña con significado, siempre hablando de ordenadores típicos. Por último, dependiendo de la cantidad de *bytes*, formarán *kilobytes*, *megabytes*, *gigabytes*, *terabytes*, etc. [accesible en] <www.alegsa.com>.

permiten acceder a los puertos de entrada y salida, hacer cálculos rápido, y verificar la autenticidad de datos enviados y recibidos[495].

Según indica su CHOCLAN MONTALVO, Y BALMACEDA HOYOS, las manipulaciones informáticas más comunes se generan normalmente por medio de las modalidades de la *introducción de datos falsos y mediante alteración de programas.* De esta manera CHOCLAN MONTALVO, reflexiona "indicando que la defraudación acometida través del sistema informático en virtud de las cual el autor consigue a su favor movimiento contables representativos de la transferencia de fondos, una cancelación de deuda o reconocimiento de un crédito puente tener lugar, fundamentalmente por las siguientes vías, todas las cuales suponen casos de operaciones realizadas autónomamente por la máquina sin necesidad de la contribución de persona que realiza un desplazamiento patrimonial voluntario"[496].

1.1 manipulación de input o manipulación de datos de entrada

En este caso, se conoce también como sustracción de datos, en este tipo de ilícitos, podemos encontrar aquellos que afectan tanto suministro o limitación de datos. Representa el delito informático más común puesto que es de fácil acción, y difícil de descubrir, puesto que no requiere tanto conocimientos técnicos de informática pudiendo realizarlo cualquier usuario con acceso a funciones básicas y normales de procesamiento de datos en la fase de adquisición de los mismos.

[495] BALMACEDA HOYOS, Gustavo, Estafa informática…op. cit., pág. 110.

[496]CHOCLÁN MONTALVO, José, *Delincuencia Informática, Problemas de responsabilidad, Infracciones patrimoniales en los procesos de transferencia de datos*, (director) MORALES GARCÍA, Oscar, Cuadernos de Derecho Judicial IX-2002, Consejo General del Poder Judicial, Madrid, 2002, pág. 251.

Cuando me referí en forma breve a la estafa común, y sus elementos, al encontrarnos con la estafa informática, además del hecho que los elementos de engaño y error no se encuentran presentes en esta última, tiene como distintivo, que la disposición patrimonial se consigue por parte del sujeto activo, *por alguna manipulación informática o artificio semejante.* En este tipo penal, se ha planteado que si bien en la estafa tradicional, tipificada como delito de resultado con ciertas modalidades especiales de acción queda abierta, en el tipo penal de estafa informática esta situación se exacerba, puesto que da cabida para múltiples interpretaciones y además se suma a ello, que la segunda parte del enunciado *u otro artificio semejante*, puede abrir el tipo penal hasta el punto que, puede afirmarse que son delitos de resultado que en cuanto a la acción literalmente sólo exige que se realice algún artificio, necesariamente informático[497]. Se plantea que manipular tiene demasiada amplitud, considerándose que sería una expresión que atentaría contra el principio de legalidad, englobando la acción típica, toda intervención autorizada o no en el sistema informático[498].

ROMEO CASANOVA, indica "*que la manipulación de datos informáticos consiste en la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o*

[497] CABANA FARALDO, Patricia, los concepto de manipulación informática y artificio semejante en el delito estafa informática, En cuaderno del Instituto vasco de criminología, San Sebastián, (jornadas "retos en la securización los territorios digitales: delitos informáticos"), número 21, 2007, pág. 41.

[498] GARCÍA SERVIGÓN, Josefina, *El fraude informático en España e Italia. Tratamiento jurídico penal y criminológicos,* En revista cuatrimestral de las facultades de derecho y ciencias económicas y empresariales, Número 74, España, 2008, pág. 294.

tratamiento informático, con ánimo de lucro y en perjuicio de tercero"[499]. Por otro lado, MATA Y MARTÍN, refiere "*que la manipulación a que hace referencia el precepto parece que implica la actuación del sujeto activo sobre un sistema informático de manera que altere este altere, de modo muy diversos, el resultado a que habría de conducir el normal procesamiento automatizado de datos.* Ahora bien, igualmente el autor reflexiona que el concepto de manipulación, puede verse de otro punto de vista, es decir como alteración de software, sin embargo si lo entendemos de manera estricta, tiene un efecto muy restrictivo a la hora de señalar las conductas abarcadas, pues solamente se incluiría la manipulación del programa y no otras, generalmente aceptadas, que suponga la alteración de los datos sobre los que opera el sistema incluso sobre elementos materiales del mismo. Del mismo modo, se refiere CHOCLAN MONTALVO, el cual dice *"toda acción que suponga intervenir el sistema informático alterando, modificando u ocultando los datos que deban ser tratados automáticamente modificando la instrucciones del programa, con el fin de alterar el resultado debido y tratamiento informático y con el ánimo de obtener una ventaja patrimonial*"[500].

Estas manipulaciones, pueden ser entendidas como aquellas intervenciones que inciden en la fase de tratamiento, y por lo mismo tienen por fin adulterar originarias instrucciones del programa de configuración, todo lo cual se realiza para que el mismo se desconfigure alterando los datos correctos. Anteriormente al tratar el tema de los fraudes en la red y sus distintas modalidades, pudimos ver las formas

[499] ROMEO CASANOVA, Carlos, Poder informático y seguridad jurídica, La función tutelar del derecho penal ante las nuevas tecnologías de información, Editorial Fundesco, Madrid, 1988, pág, 47.

[500] CHOCLAN MONTALVO, José, *Fraude informático y estafa por computación*, Cuadernos de Derecho Judicial-internet y Derecho penal, Escuela judicial, Consejo General del Poder Judicial, Madrid, X-2001, pág. 328.

de intervención de los ordenadores, entre ellos los spyware, o los Keyloggers, los cuales son usados para alterar el programa.

1.2. Manipulaciones en el programa

Se realizan durante la creación del programa, esto consiste en alteración información, la cual se lleva a cabo insertando datos, eliminando los ya sea en una parte o todo o posicionando los en un distinto lugar, es decir el *input*, manipulados. Existen múltiples posibilidades para manipular los programas, sobre todo con los spyware, o los troyanos que sólo más típicos donde un programa malicioso accede al ordenador aparentemente inofensivo y seguro.

1.3. Manipulación en el sistema de salida de datos u output

En este caso se manipula sistema de salida de datos como puede ser al momento de intervenir un cable telefónico o modificar una impresión final, el engaño posterior, existe la posibilidad de discutir si se presenta especificidad, al modificar un documento en forma posterior como se indicó, y ver la posibilidad estar en un caso de artificio semejante más. Vale se presente, que algunos autores indican que con esta manipulación, no podrían encuadrarlo comportamientos constitutivos de los delitos que conforma la criminalidad informática, no resultando posible su adecuación al artículo 248.2 Código Penal español. Por ello se dice, que está actividades no tienen las peculiaridades propias de la criminalidad por ordenador[501]. En conclusión, se estima que legislador tuvo una visión futura entregando una amplia expresión de lo que se entiende por alguna manipulación o

[501] CORCOY, Mirentxu / JOSHI, Ujala, *Delitos contra el patrimonio cometidos por medios informáticos*, En revista jurídica Catalunya, vol. 87 N° 3, 1988, pág. 136.

valerse de con el fin que las acciones tengan cabida en los posibles causas de ejecución[502].

La manipulación informática, tomada en forma general puede entrar en concurso con el delito de daños del artículo 264.2[503] Código Penal español[504], en el caso que exista destrucción o alteración de los datos contenidos en el sistema informático. Y también en el caso de falsedad documental, puede entrar en concurso

[502] Hay quien afirma que el *scammer* o manipulador informático no realiza ninguna manipulación ni alteración, sino que lo que se produce es una suplantación respecto al verdadero titular, ya que el que introduce determinadas claves afirma con ese acto ser determinada persona, pues son claves personales que identifican únicamente al sujeto titular de las mismas. No hay alteración alguna del sistema o software que lo soporta; aunque dicha conducta eventualmente pudiera ser reconducida a formas falsarias, quedaría totalmente desprotegido el aspecto lesivo patrimonial. Sin embargo, la mayoría de la doctrina y la jurisprudencia, están de acuerdo (acertadamente a mi modo de ver), en que con tales actuaciones se comete un delito claramente insertable en la estafa informática del art. 248. 2-a), ya que se utiliza un artificio informático mendaz para engañar al dueño de la cuenta bancaria defraudada a través de mensajes en los que, haciéndose pasar por una entidad bancaria o financiera (o sus servicios de seguridad), le pide que le recuerde sus claves y contraseñas secretas, utilizándolas posteriormente una vez obtenidas para realizar la disposición no consentida del dinero de la cuenta corriente, ingresándolo en otras cuentas, suplantando la identidad del titular de la misma. REY HUIDOBRO, Luis Fernando, La estafa informática: relevancia penal del phishing y el pharming, En La ley Penal, En revista de Derecho penal, procesal y penitenciario, número 101, 2013, pág. 8 y sigs.

[503] Artículo 264.2 Código Penal español: 2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.

[504] Los casos en los que el acceso ilícito se realiza para llevar a cabo un perjuicio patrimonial ajeno (estafa informática) se tratarán dentro de los delitos producidos por medio del sistema informático. Aquéllos que supongan la utilización ilegítima de terminales de comunicación (art. 256), que puede ser una modalidad delictiva apta para castigar determinadas formas de acceso ilegítimo a sistemas informáticos ajenos, se tratarán también de forma autónoma. En todo caso, en la medida en que el acceso resulte punible en sí, las figuras eventualmente aplicables podrán concurrir en concurso de delitos con las que sancionen otros resultados punibles causados con el mismo (daños y descubrimiento de un secreto de empresa, estafa informática y utilización ilegítima de un terminal de comunicación, etc.). GONZÁLEZ RUS, Juan, *Protección penal de sistemas, elementos, datos, documentos y programas informáticos*, En revista electrónica de ciencia penal y criminología, número 1-14, Córdoba, 1999, pág. 7.

real con el fraude informático pues el artículo 26 del Código Penal español[505], equipara soporte material que incorpora datos y documentos[506].

2. Artificio semejante[507]

Dicho término se incorporó con el Código penal de 1995, con el fin de abarcar supuestos donde no se manipulaba un sistema informático, sino la manipulación de otro tipo de máquinas automáticas, como por ejemplo las monedas falsas usadas en máquinas automáticas o de servicios. Esta fórmula, recaló el legislador artificio semejante se considera como una fórmula de cierre, con el fin de cubrir toda la posibilidad de fraude informático, sin embargo se caracteriza por su indeterminación. Otros estiman que ante la dificultad de delimitación de ambas modalidades típica, se llegaba incluso considerar factible una doble interpretación, decir como *artificio semejante a la manipulación.* Como se observa, la fórmula legal es muy amplia, aunque tal vez inevitable en este campo, en el desarrollo tecnológico

[505] Artículo 26 Código Penal español: A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

[506] GARCÍA SERVIGÓN, Josefina, *El fraude informático en España e Italia. Tratamiento jurídico penal y criminológicos*, En revista cuatrimestral de las facultades de derecho y ciencias económicas y empresariales, Número 74, España, 2008, pág. 295.

[507] Cuando la conducta que desapodera a otro de forma no consentida de su patrimonio se realiza mediante manipulaciones del sistema informático, bien del equipo, bien del programa, se incurre en la tipicidad del art. 248.2 del Código penal. También cuando se emplea un artificio semejante. Una de las acepciones del término artificio hace que este signifique artimaña, doblez, enredo o truco. La conducta de quien aparenta ser titular de una tarjeta de crédito cuya posesión detenta de forma ilegítima y actúa en connivencia con quien introduce los datos en una máquina posibilitando que ésta actúe mecánicamente está empleando un artificio para aparecer como su titular ante el terminal bancario a quien suministra los datos requeridos para la obtención de fondos de forma no consentida por el perjudicado. En primera instancia se absuelve al acusado. Se estima la casación. STS, Sala 2ª de lo Penal, Nº 364, de 11. V. 2011, (Ponente: Sr. Diego Antonio RAMOS GANCEDO).

es continuo en el peligro de que una prosa más estricta dejara pronto obsoleto el precepto, el *artificio semejante* podría hacer pensar que se incluyen también otra maniobra naturaleza no informática, sin embargo, el sentido del apartado obliga a entender que todo él, va referido estos supuestos, por lo que la mención legal debe ser interpretada también desde esa perspectiva[508].

Podemos decir entonces, que al incluir en la normo concepto amplio evita el *casuismo,* tomando en consideración la seguridad jurídica y el principio de legalidad, con ello da la posibilidad al sentenciador de poder incluir dentro de dicho tipo legal conductas efectuadas por medios indebidos de los sistemas ya indicado. González Rus, explica que el precepto castiga sólo transferencia electrónica de fondos, sin comprender la conducta que no provoque una operación este tipo, es decir nos incluyen manipulaciones que se dirigen encubrir apoderamiento disposición efectuada por medios, toda vez que transferir es trasladar, cambiar de lugar a otro[509].

3. Resultado típico, transferencia no consentida de un activo patrimonial

[508] GONZÁLEZ RUS, Juan, *Protección penal de sistemas, elementos, datos, documentos y programas informáticos*, En revista electrónica de ciencia penal y criminología, número 1-14, Córdoba, 1999, pág. 17.

[509] En relación a la interpretación de los elementos típicos "manipulación informática u otro artificio semejante", destaca el hecho de que la acción típica, perfectamente delimitada en la estafa común, que es un delito de resultado con modalidades determinadas de acción, queda abierta, se puede decir que en exceso, en la estafa informática: no sólo el concepto de "manipulación informática" es susceptible de múltiples interpretaciones sino que la coletilla, *u otro artificio semejante*, sin duda introducida para no dejar al margen ningún posible desarrollo tecnológico en el futuro, abre el tipo hasta el punto de que se puede afirmar que es un delito de resultado que en cuanto a la acción literalmente sólo exige que se realice algún artificio, necesariamente informático. Por tanto, no puede hablarse de que la estafa informática sea un tipo mixto alternativo, pues no se describen modalidades concretas de acción. FARALDO CABANA, Patricia, *Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática*, En Eguzkilore Cuaderno del Instituto Vasco de Criminología, número 21, 2007, pág. 41.

A diferencia del redactado ofrecido por el Código Penal para el delito de estafa en el apartado primero del artículo 248, en este apartado no se utiliza el sustantivo disposición sino transferencia, debiendo entender por tal la obtención por el sujeto activo de la disponibilidad de los bienes con los cuales se obtiene la ventaja patrimonial, evitando de ese modo que tenga que ser la víctima la engañada y por tanto la que ejecute el desplazamiento patrimonial, puesto que aquí a quien se engaña es a la máquina. Esa transferencia ha de ser sin consentimiento. La ausencia de consentimiento refuerza el hecho de que el engaño en forma de manipulación informática o artificio semejante recae sobre la máquina, puesto que la persona física no quiere realizar ese desplazamiento patrimonial y por lo tanto no da su consentimiento para ello, sino que se ejecuta al margen del mismo, sin su conocimiento. La persona física a la que nos estamos refirieron es lógicamente la titular del patrimonio que está siendo objeto de saqueo. Finalmente la transferencia no consentida ha de ser de activos patrimoniales, es decir, dinero contable o escritural, valores patrimoniales sin correspondencia con un objeto material. El Magistrado Choclán Montalvo entiende que incluso dentro de este concepto tienen cabida los servicios así como la eliminación de pasivo en cuanto que ello implica siempre un activo patrimonial[510].

Por acto disposición patrimonial, Mata y Martín, refiere "que sería en la entrega de una cosa material o dineraria, en la realización del acto documental con transferencia económica, ya sea un gravamen de un bien o en la presentación de cualquier tipo servicio, todo ello siempre cuantificable económicamente". A que se presente, que se hace referencia transferencia y no a disposición, es decir actividad humana puesto que es perfecto la mente realizable por una máquina sin intervención

[510] CHOCLÁN MONTALVO, José, *Delincuencia Informática, Problemas de responsabilidad, Infracciones patrimoniales en los procesos de transferencia de datos*, (director) MORALES GARCÍA, Oscar, Cuadernos de Derecho Judicial IX-2002, Consejo General del Poder Judicial, Madrid, 2002, pág. 255.

humana. A su vez el concepto patrimoniales amplio pues admiten tanto bien inmueble como inmuebles[511].

Podemos señalar entonces, que la transferencia no consentida de activos patrimoniales, que debe ser un efecto inmediato de la manipulación informática, equivale al acto disposición de la estafa común, exigiendo el tipo penal cumplir la función de resultado intermedio la estafa informática, caracterizándolo, al igual que la estafa básica, como un hecho punible con un proceso causal que se encuentra típicamente configurado. Se presenta como un elemento de criterio objetivo del injusto de la estafa informática, que parece cumplir la función de resultado intermedio necesario en tal delito, de este modo no cualquier perjuicio patrimonial podría determinar la consumación del delito estafa informática, sino sólo aquel que hubiese sido causado mediante una conducta constitutiva de una manipulación informática generadora una transferencia activos patrimoniales[512]. Refiere Herrera Moreno, que sin duda la demarcación de este resultado abona la postulación de una concepción subjetiva del engaño, o, más rectamente, ardid manipulador, puesto que a través de ésta referencias introduce la conexión con el bien jurídico protegido, por cuanto importante no será discernir, sobre un catálogo de las posibles manipulaciones, tanto como restringir al alcance típico el precepto, identificando como objeto de la acción las que supongan un riesgo tolerable para el patrimonio tutelado[513].

[511]GARCÍA SERVIGÓN, Josefina, *El fraude informático en España e Italia. Tratamiento jurídico penal y criminológicos*, En revista cuatrimestral de las facultades de derecho y ciencias económicas y empresariales, Número 74, España, 2008, pág. 296.

[512] GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos, análisis del artículo 248.2 Código penal*, Editorial Tirant Lo Blanch, Valencia, 2005, pág. 591.

[513] HERRERA MORENO, Myriam, *El fraude informático en el derecho penal español*, Revista de Actualidad Penal, número 39, Sevilla, 2001, pág. 958.

4. Perjuicio

Este tercer elemento del tipo penal implica la necesidad de que como consecuencia de los actos acometidos por el sujeto activo del delito, se cause un perjuicio a una tercera persona, entendiendo por tal un daño cuantificable desde un punto de vista económico**.** De esta manera, el efecto propio del engaño es el acto disposición patrimonial, con su consecuente perjuicio causado a la víctima, que puede ser el mismo sujeto un tercero, por ello se dice que el perjuicio puede ser propio ajeno, sin embargo debe ser cuantificable de manera económica[514].

II. Imputación en el ámbito del tipo subjetivo

A) Títulos de imputación de responsabilidad penal

El perjuicio debe afectar a un tercero, ya que no es la propia víctima la que realiza la transferencia económica, sino que es el propio autor del delito el que la lleva a cabo. En este delito no cabe la comisión culposa, el sujeto activo actúa dolosamente, es decir, actúa conociendo y queriendo realizar la acción delictiva. El concepto de *manipulación informática* implica por sí mismo, la intencionalidad del sujeto activo, es difícil que alguien lleve a cabo actos de alteración, modificación de datos o programas informáticos por error y que además le reportan un beneficio económico, ya que estas acciones requieren conocer los datos o instrucciones correctas y cambiarlos por otros, el sujeto sabe que su actuación constituye una acción contraria a derecho y aun así la lleva a cabo.

[514] El engaño ha de ser idóneo. Es preciso que exista una relación de causalidad entre el engaño que provoca el error y el acto de disposición que da lugar al perjuicio, de donde se obtiene que aquél ha de ser precedente o, al menos, concurrente, al momento en que tal acto tiene lugar. El engaño debe ser la causa del error; el error debe dar lugar al acto de disposición y éste ha de ser la causa del perjuicio patrimonial. STS, 2ª Sala de Lo Penal, N° 358, de 10. VI. 2015, (Ponente: Sr. Francisco MONTERDE FERRER)

El tipo subjetivo, de la estafa informática en forma preliminar debería estudiarse los mismos términos que el delito estafa tradicional. La teoría de los elementos subjetivos del injusto reconoció que el tipo de justo existen algunos elementos de carácter subjetivo, que presuponen el dolo pero trascienden del y que son imprescindibles para fundamentar lo injusto[515]. La doctrina estima que el tipo subjetivo del delito estafa informática, al igual que como se dijo el de la estafa tradicional, está integrado por dos elementos, a saber se exige que el autor actúe con dolo a todos los elementos que delimitan su tipo objetivo, incluido resultado consumación del mismo, es decir el perjuicio patrimonial; se suma a lo anterior que el autor debe actuar con un ánimo o intención, y el legislador la describe como ánimo de lucro. En este sentido, el ánimo de lucro deberá ser considerado como un elemento subjetivo del injusto, distinto del dolo general de dicho delito, el cual vendría a delimitar o colorear de forma significativa el concreto contenido de su justo, introduciendo, en el mismo la voluntad característica es decir el autor actúa con intención de apoderarse del patrimonio ajeno, y que es el bien jurídico protegido por este delito[516]. Ahora bien, las conductas dolosas se diferencian de las imprudentes por ser manifestaciones, de una decisión de su autor contra el orden jurídico protegidos, dicha decisión se adopta sobre la base de una previa y como incorrecta prevención de la situación en general, es decir el autor previamente analiza este, estudia o se representa la realidad con sus distintas variables, ya sea en los hechos, como las normas, e igualmente se representaría el resultado consultivo[517]. En todo caso, no necesario un dolo específico o directo, sino que basta

[515] POLAINO NAVARRETE, Miguel, *Derecho Penal, Parte general*, tomo II, Teoría jurídica del delito, Editorial Bosch S.A., Barcelona, 2000, pág. 264.

[516] GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos, análisis del artículo 248.2 Código penal*, Editorial Tirant Lo Blanch, Valencia, 2005, pág. 796.

[517] GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos, análisis del artículo 248.2 Código penal*, Editorial Tirant Lo Blanch, Valencia, 2005, pág. 730.

con un dolo genérico, siendo factibles todas las modalidades de dolo, incluso el dolo eventual, no resultando sancionables las conductas imprudentes o negligentes, o aquellas por mera utilización, de una manipulación informática, puesto que se exige un elemento subjetivo del injusto, cual es el resultado de toda la acción es decir el ánimo de lucro.

B) Ánimo de lucro

Aunque el texto legal no incluye elemento subjetivo alguno de manera expresa, como sucede en todo delito patrimonial, salvo exclusión expresa del legislador, es necesaria la concurrencia del ánimo de lucro, como intencionalidad de obtener un beneficio patrimonial con su actuar. Ello significa que la persona que comete el verbo típico y por lo tanto fábrica, introduce, posee o facilita el programa informático, tiene que hacerlo para poder obtener un beneficio económico derivado de su conducta, lo cual es evidente atendiendo al elemento finalístico anteriormente mentado que sí se encuentra expresamente incluido en el texto legal[518].

El ánimo de lucro requerido en el tipo encarna un elemento subjetivo del injusto que puede definirse en general como intención de enriquecimiento a costa del empobrecimiento de la víctima cuya virtualidad reside, esencialmente, en la exigencia implícita de dolo directo en el ámbito de la culpabilidad. Por consiguiente, aun cuando resultan difíciles de imaginar, deben excluirse aquellas hipótesis en las que el objetivo del autor no sea conseguir la cantidad *estafada*, obtenida en el desarrollo de operaciones informáticas realizadas con otro propósito. La configuración típica de la manipulación informática obliga a que el autor realice dicha acción, pretendiendo obtener ventaja económica o patrimonial, que ingresan a su acervo producto de dicha manipulación informática. La afectación del patrimonio

[518] PILLADO QUINTAS, Víctor, *Estafas Cometidas por medios informáticos y mediante el uso de tarjetas bancarias,* Aranzadi – Westlaw" - Base de Datos, pág.

ajeno, se constituye en una delimitación restrictiva del ámbito de afectación o de incidencia de la manipulación informática al área económica patrimonio individual, en su sentido microsocial individualista, de manera tal que una manipulación informática defrauda Torio patrimonial será aquella que supone no sólo un perjuicio o grave puesta en peligro del bien jurídico informático protegido en, sino también el patrimonio individual de un tercero, no sólo en cuanto los objetos de la acción tengan un contenido valor económico patrimonial, sino que además sea susceptible de causar un perjuicio patrimonial ajeno correlativo enriquecimiento ilícito del autor[519].

III. Iter crimnis

Para que un delito se encuentre consumado, requiere un acto perfecto o acabado, como indica el Dr. POLAINO NAVARRETE, que el sujeto no solo infringen la norma sino que produce todos los actos con un resultado de además este mismo se produce[520].

La consumación de la estafa informática se produce en el momento en que el sujeto consigue la transferencia no consentida. Consecuentemente, se precisa la efectiva producción del desplazamiento patrimonial con el perjuicio y enriquecimiento consiguientes, lo que no impide apreciar la infracción en grado de tentativa si una vez realizada o comenzada la manipulación no llega a producirse el resultado señalado. En materia concursal, como hemos visto, los Tribunales aprecian

[519] ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Editorial Comares, Granada, 2002, pág. 270 y sigs. El mismo autor, conceptualiza *Manipulación Informática Defraudatoria Patrimonial:* como cualquier acción de intervenir o afectar de forma subrepticia la información informatizada, los datos o los programas que la representan, o las funciones propias de un sistema de procesamiento, de tratamiento o transferencia de los mismos, realizada con ánimo de lucro y en perjuicio patrimonial de un tercero.

[520] POLAINO NAVARRETE, Miguel, Derecho Penal, Parte general…op.cit., pág. 222.

a veces un concurso entre el presente delito y el de falsedad documental, cuando el sujeto falsifica la firma correspondiente al titular de una tarjeta de crédito sustraída, para conseguir así una transferencia patrimonial no consentida.

El artículo 248.2 Código penal, recoge un tipo de resultado material que exige para su consumación un efectivo perjuicio cono mico en el patrimonio ajeno, a través de la transferencia no consentida un determinado activo patrimonial, por ello se aprecia que momento la consumación delictual se produce al verificarse, al materializarse, al conseguir tal transferencia patrimonial siempre que la misma suponga el perjuicio de esta índole a personas ajenas sujeto activo. PÉREZ MANZANO, señala "que si bien al ser el perjuicio resultado material, en la consumación no se va producir hasta que éste no se materialice, matiza que la tentativa exigirá la ejecución de la manipulación informática y que difícilmente se podrá diferenciar de la tentativa acabada y la inacabada dado que la transferencia de activo patrimonial producirá automáticamente perjuicio, aunque no implique paralelamente la obtención del beneficio económico. Asimismo indica ORTS Y ROIG, al señalar que la consumación de la estafa informática se produce el momento en que sujeto consigue la transferencia no consentida, por ello se precisa o necesita la efectiva producción del desplazamiento patrimonial con el perjuicio y enriquecimiento consiguiente, pero a pesar de ello esto no obstaculiza la tentativa si es que una vez realizada comenzada manipulación no llega a producirse resultado señalado[521]. REY HUIDOBRO, señala que la forma imperfecta de ejecución caben a la estafa informática como es la tentativa inacabada, como la tentativa acabada, y además refiere que transferir supone trasladar, cambiar algo de un lugar a otro, constituye un proceso meramente contable que supone cargar débitos, del contractivo ordenar ingresos con la correlativa notación a favor del sujeto, al que

[521] ORTS BERENGUER, Enrique / ROIG TORRES, Margarita, *Delitos informáticos y delitos comunes cometidos a través de la informática*, Editorial Tirant lo blanch, Valencia, 2001, pág. 70.

esta forma se realice una determinada prestación o servicio, de esta manera la consumación se alcanza o no se produce perjuicio, y que no es necesario que coincida con la realización del asiento contable fraudulento, toda vez que por ejemplo una entidad bancaria o financiera que sido suplantada para llevar a cabo el fraude, se aperciba a tiempo de la operación y anule la misma, impidiendo así la atracción del dinero, con ello existe esta posibilidad de delito pero no se ha consumado, siendo estos casos frecuentes y debiendo calificarse como tentativa delictivas[522].

IV. Problemas concursales

Esta primera modalidad de estafa informática prevista en el apartado a) del artículo 248 del Código Penal puede entrar en relación de concurso con el delito de daños informáticos previsto en el artículo 264 del Código Penal, habida cuenta de que el sujeto activo de la defraudación patrimonial, a la hora de acometer la manipulación informática o artificio semejante, puede provocar un borrado de datos del sistema informático atacado o incluso una interrupción del sistema. La relación

[522] En relación a la controvertida estafa informática denominada "fishing Pues bien, de la estafa informática del artículo 248.2 del Código Penal, en la modalidad conocida por fishing por la que viene condenado el apelante, se ocupó este Tribunal en la sentencia de 29 de Julio de 2011 en la que se describía tal clase de práctica y se ocupaba del papel desempeñado por el conocido en estos casos como intermediario o mulero, que es el que le cabe al apelante en los hechos objeto de la presente causa Recordando el debate doctrinal sobre la tipología penal de esta clase de práctica, desde la postura del colaborador, destacaba dicha resolución cómo una parte de nuestros tribunales englobaba la conducta del intermediario en la estafa informática y ponía como un ejemplo de dicha posición Se afirmaba en tal sentido que siempre que no exista acuerdo expreso o tácito con los scammers, (que son los sujetos que transfieren el dinero inconsentidamente apropiado) y que los muleros ignoren que están inmersos en un delito de estafa informática, es decir, que no sepan que el dinero proviene de la sustracción a un tercero, ha de señalarse que no tienen responsabilidad penal por ese delito de estafa informática y terminaba absolviendo en el caso enjuiciado a la acusada por considerar que no estaba probado que hubiera participado en la manipulación informática, base de dicha defraudación, ni que conociera que la transferencia hecha a su cuenta se hubiera realizado de forma fraudulenta, elemento preciso en tanto que estamos hablando de conductas eminentemente dolosas. STS, 2ª De Lo Penal, N° 524, de 15. X. 2014, (Ponente: Sr. Miguel Ángel AMEZ MARTÍNEZ).

de ambas conductas delitctivas entiendo que ha de ser en concurso real, por afectar cada una de ellas a bienes jurídicos diferentes y por lo tanto merecer castigo independiente, pero siempre y cuando los daños informáticos causados para perpetrar la estafa sean más de los imprescindibles y necesarios para cometer el acto defraudatorio, puesto que en ese caso el daño podría ser valorado a efectos de responsabilidad civil pero no castigado penalmente de manera independiente al delito de estafa.

CAPÍTULO VII

Imputación objetiva en el delito de estafa informática

I. Planteamiento

Internet ha posibilitado el procesamiento de datos electrónicos, almacenamiento y traspaso de grandes cantidades de información, entregando una herramienta eficiente, tanto para la economía en general, como para gobiernos y personas. Sin embargo ello, las tecnologías relacionadas con la información han obligado el Derecho, a tener que dar respuesta a los nuevos delitos y en especial a los transnacionales, tomando en consideración el objetivo fundamental del Derecho penal de la globalización que es eminentemente práctico, proporcionando una respuesta uniforme o, al menos, armónica a la delincuencia relacionada con este tipo de delitos, evitando que se formen paraísos jurídico penales[523][524]. Dichos fenómenos

[523] Respecto de ello, SILVA SÁNCHEZ, apunta, "en todo caso, la homogeneización de las reglas legales de la parte general y de los propios criterios dogmáticos de imputación en un plano global podría, por lo demás, pugnar en teoría con la naturaleza cultural de la dogmática. En efecto, por mi parte, comparto la convicción, profundamente arraigada entre los penalistas, del carácter supranacional de la ciencia del derecho penal". Agrega, "ello determinaría que nuestra ciencia fuera no solo transnacional, sino, más bien aún, global, universal, desvinculada de referencias espacio temporales, independiente de culturas y sistemas de valores. Modernamente, en cambio, se rechaza por mucho la posibilidad construir de modo completo el sistema dogmático del derecho penal sobre la única base de las verdaderas supuestamente permanentes e inmutables, inherentes a las estructuras lógico objetivas. SILVA SÁNCHEZ, Jesús María, *La expansión del Derecho penal, aspectos de la política criminal en las sociedades postindustriales*, 3ª Edición, Editorial Edisofer, España, 2011, pág. 96.

[524] Estima Silva Sánchez, sinónimo de exhaustividad alguna, puede mencionarse las siguientes cuestiones como característica de la dogmática de la globalización, en la que las cuestiones probatorias adquieren por otro lado una trascendencia excepcional. La imputación objetiva tiende a perder ya los derechos nacionales su vinculación con relaciones de necesidad con arreglo a las leyes físico naturales. En su lugar, se plantea la suficiencia de relaciones de probabilidad o, incluso, directamente depurar relaciones (normativas), de sentido. Esta tendencia, quien sí puede adquirir sin embargo un importante sesgo anti garantía está en la medida en que se asiente la propuesta de algunos autores de proceder a una inversión de la carga de la prueba en este punto. También el autor, entregar razones, respecto de la superación entre la diferencia entre el dolo

económicos de la globalización y de la integración económica da lugar a la conformación de modalidades nuevas de delitos clásicos, así como la aparición de nuevas formas delictivas generando una delincuencia contra los intereses financieros de la comunidad producto del integración, como el fraude, emergiendo una nueva concepción de lo que se entiende por delictivo, apartándose de la idea marginal de delincuencia[525].

Cuando se habla de delito informático eminentemente entendemos, que la acción delictiva se comete con tecnología informática, por ende para poder hacer frente a esta nueva forma de criminalidad, como se comentó, las legislaciones en el mundo han tenido que actualizar sus políticas criminales creando nuevos tipos penales o derechamente leyes especiales que regulan la materia. En estos ámbitos, el comportamiento delictivo requiere la intervención de la informática, para luego acomodar al delito informático específico, es necesario el conocimiento de la tecnología informática para concretar estos tipos de delitos, e igualmente se requiere dicha expertís para su investigación por parte del ente persecutor, y los conocimientos ampliados en dicho ámbito para el posterior juzgamiento. Por ello, de manera general en cuanto los delitos informáticos se tratan, existen modalidades básicas, a saber, sabotaje informático; acceso no autorizado a datos o sistemas computarizados; y manipulación informática, caracterizándose ésta última cuando el

---

eventual y culpa consciente. Igualmente se disminuye la brecha entre autoría y participación fórmulas ya no de distinción de las mismas, a lo que ya se advierten el plano de la pura tipificación si se examinan los tipos de delito en materia de tráfico de estupefacientes o de blanqueo de capitales. Igualmente tendería a desaparecer la diferenciación entre causas de justificación y causas de exculpación. SILVA SÁNCHEZ, Jesús María, *La expansión del Derecho penal*…op. cit., pág. 104, y sigs.

[525] Al respecto confrontar, SILVA SÁNCHEZ, Jesús María, *La expansión del Derecho penal, aspectos de la política criminal en las sociedades postindustriales*, 3ª Edición, Editorial Edisofer, España, 2011, pág. 90 y sigs.

autor influencia sobre procesamiento de datos para modificar su resultado y obtener una ventaja personal.

Durante la historia dogmática penal, los sistemas de atribución de responsabilidad han variado de acuerdo a los modelos de imputación, según sea el momento histórico predominante, por ello, la forma y disposición de la teoría del imputación objetiva, tiene como bases originales, los escritos de Dissertation de Karl LARENZ, del año 1927; el artículo sobre causalidad e imputación objetiva de Richard HONIG, de 1930 y las reflexiones de Claus ROXIN sobre la problemática de la imputación en Derecho penal, del año 1970[526][527].

Respecto del origen, refiere el Dr. POLAINO NAVARRETE, "que para superar las insuficiencias de causalismo clásico y finalismo, a partir de los años 60 y 70 del siglo XX un grupo de autores, entre ellos ROXIN y JAKOBS comenzaron a desarrollar una doctrina llamada *teoría del imputación objetiva*, siendo discutible que sea una única teoría, puesto que son varias formulaciones diferentes y es cuestionable también que sea puramente objetiva, porque realmente tanto objetiva como

[526] ROJAS AGUIRRE, Luis, *Lo subjetivo en el juicio de imputación objetiva: ¿aporía teórica?,* En revista de derecho U. A. de Chile, Vol. XXIII número 1°, 2010, pág. 243.

[527] El autor en su valoración final indica a modo de resumen indica: "el origen de la teoría de la imputación objetiva en LARENZ, se vincula a una concepción del hecho como unidad de acción y consecuencia, dominada por la voluntad, que en esa medida superar la relación de causalidad. La versión propuesta por HONIG, se construye básicamente sobre el concepto de evitar habilidad del resultado, que fundamenta la responsabilidad tanto la acción como en la omisión. Para ambas versiones, resulta determinante la medida en que la conducta está, por su relación con la voluntad, inclinada hacia la realización del resultado. Metodológicamente, ambas versiones de la teoría se comprenden en términos objetivos y, al menos en el caso del LARENZ, como una categoría previa a la valoración jurídica. El ROXIN concibe también esta teoría en términos exclusivamente objetivos, pero al mismo tiempo construida sobre la base criterios normativos. Esta versión de la teoría, a diferencia de las dos originales, se inclina menos en inclusión de aspectos subjetivos en el juicio de imputación objetiva. Para BUSTOS, O FRISCH, la consideración de aspectos subjetivos resulta menos problemática, en la medida en que ambos acuñan un filtro previo a la pregunta estricta por la imputación del resultado, concebido en términos altamente normativos. ROJAS AGUIRRE, Luis, *Lo subjetivo en el juicio de imputación objetiva*… Op. cit., pág. 235.

subjetiva, debiendo ser mejor llamada doctrina, y mejor qué de la imputación objetiva sería llamarla de la imputación jurídica o del imputación penal, eminentemente desarrollada por el sistema de funcionalismo normativo de JAKOBS".

El autor también indica "que la primera diferencia que presenta esta teoría frente a las formulaciones anteriores es que se trata de una doctrina puramente normativa, esto es, para determinar que interesa al Derecho penal no acude a un elemento extra jurídico (como la causalidad o la finalidad), sino a un elemento propio del Derecho penal como es la *imputación*, se trata de la primera doctrina que abandona el ontologismo (la ciencia del ser) y resuelve el problema jurídico mediante criterios normativos (la ciencia del deber ser). Además el mismo catedrático agrega, el sistema funcionalista normativo ha comportado una normativización de todos los conceptos jurídico-penales, desde la acción hasta la imputación penal. Para ello, el funcionalismo parte de la teoría de los roles sociales"[528].

La dogmática penal, tiene como una de sus misiones fundamentales, determinar cuándo un hecho jurídico penalmente relevante, puede ser atribuido a un sujeto, y ha sido obra del mismo. De acuerdo ello, si la conducta se mira como mero movimiento corporal que causa un efecto externo perceptible por los sentidos, las modificaciones del mundo exterior pasan a ser determinante. Sin embargo, se miran de forma distinta cuando el comportamiento como actividad del mismo hombre, se dirige de acuerdo con sus facultades intelectuales y volitivas, pero no toma en cuenta, la repercusión o efecto de la misma.

[528] POLAINO NAVARRETE, Miguel, *Lecciones de Derecho penal*, *Parte general*, tomo II, Editorial Tecnos en Madrid, 2013, pág. 83 y sigs. En el mismo sentido, MIR PUIG, Santiago, *Derecho pena*, *Parte general*, 9ª edición, Editorial Reppertor, Barcelona, 2011, pág. 535 y sigs.

De esta manera, la base del delito cambia y también sobre elementos, siendo el hecho que no toda conducta humana tenga la respuesta penal, nos lleva a seleccionar aquella que interesa para los efectos del mismo, es decir según lo que se determine por el Derecho penal. De esta manera, como explica el Dr. POLAINO NAVARRETE, la noción de norma jurídico-penal influirá a la hora de establecer cuál es esa conducta valorada, (positiva o negativamente) por ella, al realizar las diversas imputaciones. Así, mientras el comportamiento humano apunta al *ser*, el derecho se refiere al *deber ser*, lo correcto o adecuado según el objeto valorado y la clase de valoración desde el punto de vista penal[529].

MIR PUIG[530], refiere que el hecho antijurídico ha de poder ser imputado a su autor, por ende la imputación objetiva supone la atribución de un sentido jurídico-penal específico en los términos legales que expresa la conducta típica, y no sólo la descripción del verdadero sentido de dichos términos. Sobre lo mismo, el Dr. POLAINO NAVARRETE, nos vuelve a ilustrar, y dice "ejercer el rol significa compilar la expectativa social y respetar la norma. Por el contrario, apartarse del rol significa defraudar la expectativa social, esto es: *infringir la norma*. Desde este punto de vista, la imputación penal puede definirse muy sencillamente como la desviación respecto de aquella expectativa que comete al portador de un rol o, más escuetamente: como la desviación de un rol"[531].

En definitiva, en forma muy general la teoría de la imputación objetiva, plantea que para que un resultado pueda ser atribuido a un sujeto, es necesario que

[529] Confr. VARGAS PINTO, Tatiana, *Manual Derecho penal práctico, teoría del delito con casos*, Editorial Abeledo-Perrot, 1ª edición, Santiago de Chile, 2010, pág. 17.

[530] MIR PUIG, Santiago, *Derecho penal, Parte general*, 9ª edición, Editorial Reppertor, Barcelona, 2011, pág. 534.

[531] POLAINO NAVARRETE, Miguel, *Lecciones de Derecho penal, Parte general*, tomo II, Editorial Tecnos en Madrid, 2013, pág. 87.

en el plano objetivo, que el resultado a imputar constituya la realización de un riesgo jurídicamente relevante y que precisamente la finalidad de la norma infringida por el sujeto es la evitación de ese riesgo. Entonces delimita la responsabilidad penal por un resultado ya en el tipo objetivo, siguiendo la fórmula básica que utiliza la imputación objetiva, al tomar un resultado y afirmando que es objetivamente imputable, cuando el autor ha creado un riesgo no permitido, el cual se realiza en el resultado típico, en su configuración concreta y se encuentra dentro del ámbito de protección de la norma. El principio de causalidad, según el cual toda causa le sigue un resultado y el nexo, para poder atribuirlo ese resultado a una determinada conducta, debemos establecer la relación de causalidad, con perspectiva natural, siendo esto relevante para el derecho penal, formulando un juicio normativo, es decir juicio de imputación objetiva.

Según MIR PUIG, "la imputación objetiva, imputación subjetiva y la imputación individual o personal, son tres niveles necesarios para que sea posible la completa imputación a un autor culpable. Imputar el delito en su totalidad significa *culpar*, a alguien como su autor (se imputar es atribuir algo a alguien, cuando lo que se imputa es algo ético jurídicamente disvalioso, imputar es culpar de ello). Los tres niveles indicados de imputación (objetiva, subjetiva y personal) constituyen exigencias del principio de culpabilidad, entendido en el sentido amplio que permite y aconseja este término para servir de fundamento a toda la exigencias que entraña la prohibición de castigar a un inocente (no culpable), en un Estado social y democrático de derecho respetuoso de la dignidad humana: el principio de personalidad de la pena, que impide hacer responsable a un sujeto por delitos ajenos (y que se corresponde con la exigencia procesal de necesidad de rebatir la presunción de inocencia mediante la prueba de que el sujeto ha realizado materialmente el hecho); el principio de responsabilidad por el hecho que proscribe

la culpabilidad por el carácter llamado el derecho penal del autor; el principio de dolo o culpa y el principio de imputación personal"[532].

Por último por último, como señala FEIJOO SÁNCHEZ, no cabe duda que la teoría de la tipicidad del ámbito del Derecho penal, está sufriendo una auténtica revolución a través de la denominada teoría del imputación objetiva, que fruto de una línea metodológica opuesta a la del finalismo; a la fundamentación y sistematización ontológica que caracterizaba al finalismo, se ha opuesto una fundamentación y sistematización teleológica-funcional. Evidentemente un cambio radical esta naturaleza respecto la teoría jurídica del delito, supone una reformulación de sus distintas partes[533].

II. Imputación objetiva en los delitos informáticos en general

Ahora bien, en esta parte de esta investigación se busca realizar una relación somera, respecto a la dogmática jurídico-penal en relación a los delitos informáticos, comenzando desde un punto de vista normativo, para la construcción de los tipos penales, de manera tal que de acuerdo al delito informático en general se pueda determinar qué conducta es la que se pretende imputar, tomando como base la imputación en virtud de competencia, según la concepción del funcionalismo normativista. Las múltiples formas posibles que existen para vincular a un ordenador y con ello realizar un delito son ilimitadas, tomando en consideración que puede lograrse ejecutar una conducta delictiva, que tenga por fin transferencia de un activo

[532] MIR PUIG, Santiago, *Significado y alcance del imputación objetiva en el derecho penal, En nuevas formulaciones en las ciencias penales,* Homenaje profesor Claus ROXIN, Editorial Córdoba Marco Lerner, Argentina, pág, 61, Citado por LAMAS PUCCIO, Luis, *Una aproximación a la teoría de la imputación objetiva, En cuestiones actuales de Derecho penal y Procesal penal,* 1ª edición, Editorial E&J Graff, Perú, 2013, pág., 157.

[533] FEIJOO SÁNCHEZ, Bernardo, *Imputación objetiva en Derecho penal,* Publicación del Instituto peruano de ciencias penales, Editorial Grijley, Lima, 2002, pág., 25.

no consentido o alterar información que se mantenga en alguna base de datos. La facilidad que existe hoy en día para cometer cualquier tipo de delito, a través de los medios informáticos como es la violación de secretos, la obtención de datos, dan pie para entender que las formas delictivas, solamente con la capacidad de cualquier usuario de poder manejar un ordenador, hoy en día se multiplican, puesto que las reglas que ante existían que se aplicaban a los delitos tradicionales, se alteran en este espacio virtual, ante ello tanto legislador como la doctrina han tenido que solucionar este tipo de conflictos. Además se suma que al hablar de imputación frente a lo que se entiende como delito informático, frena de alguna manera al Derecho penal, toda vez que tampoco se tiene un concepto definido de delito informático, negando parte de la doctrina la existencia de un concepto único, toda vez que se entiende que viene a unificar una pluralidad de delitos que tendrían común solamente la vinculación con ordenadores[534].

La doctrina indica que los delitos de peligro abstracto son aquellos delitos donde la consecuencia jurídica del mismo, para ser aplicadas se toman cuenta la peligrosidad general de la acción típica para determinar el jurídicos. Esta clase de delitos no hay lesión efectiva sino probabilidad de lesión del bien jurídico, repitió tipo penal singulariza una determinada situación de peligro o de riesgo que suficiente para su consumación, basta con el peligro real (riesgo) imputable a la

[534] El autor, plantea en cuanto el concepto de delincuencia informática patrimonial, y en cuanto su utilidad e intento de definición que "las descripciones realizadas en el epígrafe anterior sobre delincuencia informática de carácter patrimonial obligan ya a no posponer una aproximación a su definición, es decir, a lo que debe entenderse por ella, ya los hechos vinculados con esta forma de delincuencia susceptible de incriminación, ya sean subsumible serotipo penales existentes o merezcan dicha incriminación. El sólo objetivo de querer presentar o describir la fenomenología de la delincuencia informática en general y poder valorarla con exactitud ha planteado inconvenientes, aparte de los mencionados, de la no existencia de un significado general predicable a esta delincuencia o al delito o abuso informático. ROMEO CASANOVA, Carlos, *Poder informático y seguridad jurídica, La función tutelar del derecho penal ante las nuevas tecnologías de información*, Editorial Fundesco, Madrid, 1988, pág., 40 y sigs.

realización típica[535]. De acuerdo lo anterior, el tipo penal se satisface con la mera realización de comportamiento o descrito, no necesario entonces que se afecte un bien jurídico protegido, con ello no necesario comprobar en el caso en concreto si se ha producido un peligro o no, toda vez que sólo necesario acreditar la realización del comportamiento típico. Por otro lado cuando se habla de peligro, éste debe ser concebido normativamente, es decir tomando en consideración un juicio normativo respecto de la posibilidad de existencia de un bien.

En el ámbito de la criminalidad informática[536], en cuanto este tipo de delitos de peligro extracto, se ha desarrollado en cuanto los delitos de difusión de material pornográfico, y también en los delitos de agitación xenófoba. Es posible analizar a base de la estructura estos delitos, en materia informática tomando en consideración la perturbación de los sistemas o programas informáticos, como por ejemplo en el acceso indebido al correo electrónico. Con estos delitos de peligro abstracto en cuanto la imputación objetiva es suficiente la imputación del comportamiento. Ahora bien, en cuanto los delitos informáticos que se refieren al acceso no autorizado a una base de datos, se puede señalar que ésta constituye una conducta de

[535] BUSTOS RAMÍREZ, Juan / HORMAZÁBAL MALARÉE, Hernán, Lecciones de Derecho penal, Parte general, Editorial Trotta, Madrid, 2006, pág. 192.

[536]Aquí lo que interesa más bien es poner de relieve hasta qué punto la técnica de tipificación no ha acentuado injustificadamente los problemas hermenéuticos, en comparación con la modalidad común de la estafa 248. En el caso del artículo 248.2 la indeterminación es general, aunque se centra en el modo tan abierto en que ha quedado delimitada la acción típica, lo que podría llevar a plantear que habríamos pasado de un delito característico de medios comisivos determinados a uno cuasi-resultativo, con lo que, por cierto, según el criterio dominante, se acentúan la necesidad y posibilidades de recurrir a la teoría de la imputación objetiva. En particular, aquella indefinición se advierte en la expresión "u otro artificio semejante", que, aparte de otras funciones, parece, en principio, configurada con el propósito de dominar con el tipo lo que se ha llamado desarrollo tecnológico vertiginoso, aunque alcanza, como se verá inmediatamente, a otros elementos del tipo. ANARTE BORRALLO, Enrique, *Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información, Derecho y conocimiento,* Vol. 1, facultad de derecho, de la Universidad de Huelva, España, 2001, pág. 214.

mera actividad, puesto que sólo se exige el acceso indebido sin ninguna otra condición.

En cuanto la teoría del imputación objetiva, en forma como se relaciona a la explicación de la vinculación entre una conducta y sus consecuencias en los delitos de resultado, no obstante ello es posible articular esta doctrina en los llamados delitos de mera actividad, como en el caso ya indicado de acceso no autorizado, siguiendo al Dr. JAKOBS, puesto que indica que la imputación objetiva desarrollada a partir de los delitos de resultado sirve de patrón para todos los otros delitos[537].

III. Riesgo permitido

Se debe señalar, que la doctrina española dominante, entiende que el punto central de tensión es el del juicio de imputación objetiva del resultado[538], tanto desde un punto de vista general como en relación al delito de estafa en particular, partiendo el siguiente supuesto: asegurada relación de causalidad conforme con la teoría de la equivalencia de condiciones, deben agregarse criterios correctores de índole normativo que exige la ejecución un peligro por parte del autor y, que el mismo, no se encuentre cubierto por un riesgo permitido dentro del alcance del

[537] JAKOBS, Günther, *Derecho penal, Parte general. Fundamentos y teoría de la imputación,* (trad. Joaquín CUELLO CONTRERAS y José LUIS SERRANO GONZÁLEZ DE MURILLO). Madrid, Ediciones Jurídicas Marcial Pons, 1997, pág. 226.

[538] Se han diferenciado dos planos o niveles de análisis, a saber, la imputación objetiva del comportamiento imputación objetiva del resultado. Un primer nivel hace referencia a lo que se ha denominado conducta típica o imputación del comportamiento: la definición de las conductas que están prohibidas de modo objetivo-general o dicho con otras palabras, que rebasan el límite de lo penalmente neutral. Un segundo nivel es el de la imputación objetiva del resultado, que se configura como vínculo entre la conducta típica-el comportamiento objetivamente imputado-y el resultado. Así como tradicionalmente esta teoría se ha dedicado al análisis de la imputación del resultado, ésta es la perspectiva que todavía hoy adopta la doctrina dominante. PASTOR MUÑOZ, Nuria, *La determinación del engaño típico en el delito estafa*, Editorial Marcial Pons, Madrid, 2004, pág. 152.

tipo[539]. De acuerdo a lo que indica el autor antes citado, la estafa tradicional, como delitos de resultado es dable analizarla conforme la teoría de la imputación objetiva, tal como indica PÉREZ MANZANO, "la estafa, como delitos de resultado, es susceptible de ser analizada conforme propugna la tesis de la imputación objetiva. Si la teoría de la adecuación y la relevancia han sido criticadas en cuanto teorías de causalidad, admitiendo que sólo la teoría de la equivalencia es una tesis satisfactoria desde el plano de la causalidad, si se sostiene que la constatación de la causalidad terminó de equivalencia o de conditio sine qua non, no es suficiente para afirmar la tipicidad de la conducta, sino que es necesario además analizar la imputación objetiva del resultado, no parece existir ninguna razón para reducir este tipo de análisis a la producción de resultados decisivos para la vida o la integridad física y excluir la lesiones patrimoniales"[540].

La noción riesgo permitido implica que se esta conducta que significaron peligro de lesión para bien jurídico penales, no obstante, se encuentra autorizada con tal de que no se rebase cierto grado de riesgo, por haberse tomado las medidas que mantengan dentro de cierto perímetros que son social y jurídicamente admisibles. En la sociedad modernas *sociedades de riesgo,* todas lo han sido, pero los modernos avances tecnológicos (investigaciones genéticas, Internet etcétera) también han incrementado los focos sociales de riesgo (manipulaciones genéticas, delitos cibernéticos como la difusión de pornografía través Internet etcétera)[541].

[539] BALMACEDA HOYOS, Gustavo, *El delito estafa*…op. cit. pág. 185. Puta la web

[540] PÉREZ MANZANO, Mercedes, *Acerca del imputación objetiva de la estafa, En hacia un Derecho penal económico europeo,* Jornadas en honor del profesor Klaus TIEDEMANN, Estudios Jurídicos Serie Derecho Público, Boletín Oficial Del Estado, Madrid, 1995, pág, 285.

[541] POLAINO NAVARRETE, Miguel, *Lecciones de Derecho penal. Parte general.,* t. II, Editorial Tecnos S.A., Madrid, 2013, pág. 88.

La sociedad es consciente la existencia de una multa tipo de riesgoso peligros de diversa procedencia, existiendo ruego naturales son inevitables riegos humanos, que su vez pueden ser incontrolables o perfectamente controlable, voluntario imputables. El derecho penal de la sociedad. Trial tiene que guiarse, es lo que se refiere a la constatación de la antijuricidad de la conducta, esencialmente por fundamento de peligrosidad de la misma para los bienes jurídico-penales, así cualquier otra perspectiva debe quedar, por ello, sometido esta[542].

A) Riesgo permitido y estafa informática

En cuanto al riesgo permitido, ámbito que se tratará respecto de la imputación estafa informática, en este tipo de delitos, la superación del mismo permite acotar los parámetros de incumbencia o atribución de una consecuencia a una persona, juicio que ha de tomarse en cuenta al momento de verificarse el comportamiento típico, al entenderse el riesgo permitido como una conducta que crea un riesgo jurídicamente relevante, pero que generalmente es permitida y, por ello, a diferencia de las causas de justificación, excluye ya la imputación al tipo objetivo.[543]

Vale indicar que en los delitos informáticos, la determinación del conjunto de conductas socialmente aceptables o, más bien, la línea divisoria constituida por el riesgo permitido, no parecen claras. En el caso por ejemplo de la conducta del acceso indebido como una conducta sancionable por el ordenamiento jurídico penal, se puede identificar un deseo de resguardo e inviolabilidad del soporte lógico del sistema informático; la confidencialidad del mismo, y; otros intereses jurídicamente

[542] CORCOY BIDASOLO, Mirentxu, *Manual práctico de Derecho penal, Parte especial, Doctrina y jurisprudencia, con casos solucionados*, 2ª edición, Editorial Tirant lo Blanch, Valencia, 2004, pág. 369 y sigs.

[543] ROXIN, Claus, *La imputación objetiva en el Derecho penal*, (trad. y edit. Manuel ABANTO VÁSQUEZ), Editorial Idemsa, Lima, 1997, pág. 106.

relevantes como el derecho a la intimidad. La conducta delictiva pretende la protección de intrusos que potencialmente pudieren hacer inoperante e inútil la mantención del soporte lógico del sistema informático; perdiendo la funcionalidad asignada para la custodia de información.

Adentrándonos en el tema, se hace necesario determinar en primer lugar las intensidades de los riesgos. En efecto, para excluir la imputación objetiva en supuestos de riesgo permitido en el delito informático en el supuesto del hecho de acceso no autorizado, se debe atender a factores como la irreprochabilidad de conductas inocuas en contra del bien jurídico, o derechamente garantizadoras del mismo y el abuso de confianza. Que el tipo penal exija un elemento subjetivo de tendencia interna trascendente, implica que el cambio en el mundo exterior no puede identificarse con el cumplimiento del objetivo, dado que no exige la obtención de la intencionalidad, por lo que habría que identificarlo con la propia conducta y en la propia vulneración al soporte lógico del sistema. Y es claro que constituye una situación de riesgo el hecho de que un sistema presente vulnerabilidades; ello sin desconocer que no exige la norma que la información procesada se encuentre protegida con barreras de seguridad informática, aunque se trate de información valiosa o relevante. De manera que para brindar protección penal por una conducta de acceso no autorizado, no es necesario que existan determinadas barreras de seguridad que protejan el soporte lógico, en términos cualitativos o cuantitativos.

En el caso no existe obligación de quien posee un conocimiento especial de advertir a la víctima de las vulnerabilidades del sistema automatizado de información, por mucho que para el sujeto con conocimientos especiales le sea extremadamente probable y/o le sea más que evidente que esa vulnerabilidad pueda ser utilizada en detrimento de aquél. Luego no puede entonces pretender en palabras de JAKOBS que a causa de un saber especial superior del autor, se puede pronosticar un riesgo incrementado o la seguridad de un resultado. De modo que no le es

imputable objetivamente responsabilidad al que, sabiendo de la vulnerabilidad, no la alerta al administrador del sistema, por mucho que tenga certeza del aprovechamiento ilícito de terceros; no hay creación de un riesgo no permitido nuevo, ni tampoco la superación del riesgo permitido, pues por muy especiales que sean los conocimientos no se transforma en autor, ni tampoco en cómplice quien no da aviso, ya que nadie tiene por qué controlar las vulnerabilidades de un sistema ajeno. Si la conducta precedente se estudiara bajo la óptica de la teoría de la equivalencia de las condiciones, quien no alerta del riesgo cae en una conducta omisiva que es condición para que un tercero destroce, utilice o tome ventajas ilícitas de la información obtenida a través de la vulnerabilidad. Este supuesto objetivo se puede dar con el ánimo de conocer o usar la información, cuando se trata de un experto que se inmiscuye en redes, con una motivación de curiosidad, conocimiento y práctica de su técnica. Aquí el experto, al menos, tendrá el ánimo de usar datos funcionales del sistema de tratamiento de información, para investigar las fallas en las barreras de seguridad o puertas lógicas.

Especial atención surge frente al *hacking* ético que corresponde al que accede sin tener derecho, a través de una falla del sistema; analizando un caso específico en que el acceso se logró por medio de la búsqueda de códigos y vulnerabilidades, para luego dar aviso al administrador de dichas debilidades, pidiendo recompensa o beneficio alguno por tal acción. Algunos insisten en que esta situación es, y así debe ser, sancionable penalmente. Hay autores que se muestran partidarios de la penalización por la intromisión al sistema informático, adelantando la barrera de protección penal, en atención a que para ellos el *hacking* blanco se trata de un delito de peligro abstracto. Entre otros argumentos, sostiene que la vulneración de un ámbito reservado para el titular de un sistema o de los datos que el intrusismo representa puede resultar paralela a la inmisión en un espacio físico que es la morada, por lo que resultará tan conforme o tan en contra a la intervención mínima

como se entienda la punición del allanamiento de morada. Del mismo modo, la violación de la confianza en el funcionamiento del sistema informático puede ser comparable con el interés en la seguridad en el tráfico rodado, o con la confianza en la transparencia de los mercados, cuya mayor tangibilidad excluye las dudas acerca de la conveniencia de tipificar las conductas que perturban esa confianza o seguridad, tan esenciales para el desenvolvimiento de nuestras relaciones diarias como puede ser la seguridad en el sistema virtual de comunicaciones[544].

La legislación española advierte que el mero intrusismo informático no está sancionado como tal en el Código Penal español, pues para su sanción tiene que estar acompañado de la producción de perjuicio económico; además, se muestra contraria a la tipificación por diversas consideraciones de corte dogmático y de política criminal[545].

Lo importante es el hecho que la estafa informática se trata un delito patrimonial y de resultado, donde es aplicable los criterios normativos de la teoría de la imputación objetiva. Para bien, se debe efectuar una delimitación en el entorno del delito de que se trate, toda vez que muy distinto determinar el riesgo permitido en el delito por ejemplo el homicidio que en el de estafa informática, puesto que el bien jurídico patrimonio, merecen la protección diferente en el entorno donde juegue, de esta manera para delimitar los límites del riesgo permitido en el delito estafa informática se debe determinar si estamos frente a una manipulación

[544] MATELLANES RODRÍGUEZ, Nuria, *Algunas razones para la represión penal autónoma del intrusismo informático, Derecho Penal y Criminología*, 2005, pág. 26.

[545] MORÓN LERMA, Esther, *Internet y derecho penal: hacking y otras conductas ilícitas en la red*, Editorial Aranzadi, Pamplona, 1999, pág. 161.

informática, efectuaba dentro o fuera de Internet, ya su vez, dentro Internet o fuera de ella, debe distinguirse si dice relación con el ámbito doméstico o negociar[546].

[546] PÉREZ MANZANO, citado por BALMACEDA HOYOS, Gustavo, *El delito de estafa*…op. cit., 210.

CAPÍTULO VIII

Naturaleza jurídica y Bien jurídico protegido en la estafa informática

I. Naturaleza jurídica del delito de estafa informática

La estafa y la estafa informática, protegen el mismo bien jurídico penal, el patrimonio individual, micro-social, y que si bien la estafa lo ampara frente a conductas engañosas, la estafa informática lo hace frente a aquellas afecciones de dicho bien jurídico penal, realizada por terceros con ánimo de lucro, manipulando informáticamente ordenadores o usando artificios semejantes. Por ello tiene relevancia jurídica la determinación de su naturaleza jurídica. Al hablar indistintamente de fraude o defraudaciones, desde un punto de vista objetivos, ambas figuras aluden a una conducta que trae consigo un montaje o ardid, llevando un ánimo de perjuicio ajeno en beneficio personal, siendo la voz fraude informático equivalente a defraudaciones informáticas, por ello la categoría criminológica funcional y amplia, concentra una multiplicidad de comportamientos contra interés económicos de distinta índole no clasificados, que son a su vez, beneficiados con la forma en que se trabaja en los sistemas informáticos. Siendo entonces estafa informática al parecer defraudaciones patrimoniales ocasionadas por medios informativos tratándose de un concepto más restringido que el de fraude informático. En el derecho comparado se podría decir entonces, que mayoritariamente la doctrina estima que el delito de estafa informática debe estudiarse vinculada a la estafa tradicional, dividiéndose a la hora de determinar los

límites de esa proximidad, como por ejemplo en Alemania la doctrina utiliza como criterio restrictivo, la aplicación de estafa informática, que el comportamiento debe corresponder a un engaño hacia la persona estafada, trayendo como consecuencia que sólo existiría una influencia de un proceso de tratamiento de datos confidenciales de resultado que se habría obtenido con un proceso adecuado y que únicamente se tendría en cuenta tales procesos cuando tengan importancia para el patrimonio siendo el perjuicio patrimonial, consecuencia directa de una posesión patrimonial, no siendo necesario que el operador de sistema y el perjudicado sean idénticos, siendo un directo defraude no de apropiación. En cambio en Italia la estafa informática se basa en el esquema de la estafa tradicional aplicándose la estafa informática a aquellos casos en que el computador remplazaría el proceso decisional del ser humano. Ahora bien, el Código Penal Español va de la mano con el delito de estafa clásico, señalando incluso algunos que la estafa informática sería una estafa impropia o una estafa general pero con rasgos distintos que impedirían su equiparación total con la estafa clásica, por ultimo las maquinas deben programarse y por lo mismo llevan a cabo las ordenes que se le indiquen pudiendo engañarse por ende una máquina, no correspondiendo el dominio de posesión al ordenador, pues como se dijo anteriormente sólo cumple y lleva a cabo las órdenes para lo cual fuere programado anteriormente, siendo la persona que prepara los equipos involucrados la afectada[547][548].

[547] BALMACEDA HOYOS, Gustavo, *El delito de estafa informática en el derecho europeo continental*, [en línea], Revista de derecho y ciencias penales, n° 17, Universidad San Sebastián, 2011, Chile, pág. 112. <https://dialnet.unirioja.es/.pdf>

[548] Ampliando lo indicado, nos indica el profesor BALMACEDA HOYOS, "en relación a la naturaleza jurídica del delito de estafa informática, que en el Derecho Europeo continental, la mayoría de la doctrina estima que el delito de estafa informática debería estudiarse estrechamente vinculado al delito de estafa tradicional. Sin embargo la opinión residirían a la hora de determinar los límites de esta proximidad. Por ello como en Alemania, la mayoría de la doctrina utiliza como criterio restrictivo para la aplicación del delito de estafa informática, señalando que el comportamiento de corresponder un *engaño* hacia personas como la estafa. Esto trae como consecuencia que sólo existiría un influencia sobre un proceso de tratamiento de datos cuando

II. Bien jurídico protegido, planteamiento

En palabras de don Miguel POLAINO NAVARRETE, el bien jurídico puede definirse como todo bien o valor normativamente evaluado y estimado como digno, merecedor y necesitado de la máxima protección jurídica. El bien jurídico puede ser de titularidad individual, (vida, integridad física) o colectiva (medio ambiente, salud pública, etcétera) y puede ser de carácter material (patrimonio, vida) o de naturaleza espiritual o inmaterial (honor, dignidad)[549].

Conceptualizar, el bien jurídico en determinada materia no es una tarea fácil, toda vez que se debe tomar en consideración el Derecho Penal, como última ratio al momento de tener que solucionar un problema jurídico, debiendo entender primero que todo, cual es la justificación de la intervención del Estado en esta materia, intervención coercitiva[550]. De esta manera, se debe encontrar, el valor relevante cuya infracción va a poner en marcha la labor del Estado en este sentido, es decir aplicar

---

difiera resultado que se habría obtenido con un proceso adecuado; que únicamente se tendría en cuenta tales procesos cuando sean relevantes para el patrimonio; que no se requeriría que el operador del sistema y el perjudicado sean idénticos; y, que se trataría de un delito de probatorio, no de *apropiación.* En Italia, por su parte, la mayoría de la doctrina sostiene que el delito de estafa informática se inspira en el esquema de la estafa tradicional, aplicándose la estafa informática a aquellos casos en que el computador reemplazaría el proceso decisorio del ser humano. En España, se sostiene que el delito de estafa informática presenta una estrecha vecindad con el delito de estafa clásico, emanándose dicha conexión, tanto del propio fin de cierre de lagunas alcanzado por el legislador con la tipificación de este delito, como de su propia proximidad sistemática. Con la base expuesta, en España algunos interpretan a la estafa informática como una *estafa impropia*, o como una *estafa general,* pero con rasgos que obstaculizan su equiparación total.

[549] NAVARRETE POLAINO, Miguel, *Lecciones de Derecho Pena Parte General, tomo II, segunda edición corregida y actualizada,* Editorial Tecnos, 2016. pág. 156.

[550] SÁNCHEZ BERNAL, Javier, *El jurídico protegido en el delito de estafa informática*, revista electrónica CT, pág. 109-110, 2009. Al respecto, refiere Javier Sánchez Bernal, ya en el lejano derecho romano, se entendía que la facultad de castigar del Estado, o de la comunidad misma, debía estar justificada por un precepto imperativo y general, como lo demuestra el aforismo *nullum crimen, nulla poena sine lege*. Y hoy en día, está legalidad del Derecho Penal, se ve reforzada por la unanimidad de la doctrina, que resalta por encima de cualquier otra cosa, la función protectora DVD jurídico que posee la norma penal.

la facultad que tiene el Estado de imponer un castigo a la persona, utilizando plenamente el *ius puniendi*[551], legitimando con ello la norma penal, apegándose a los criterios establecidos desde ya en la Constitución respectiva, sin desconocer entonces los principios que rigen tanto a la carta fundamental, como los principios que rigen el derecho que tiene el Estado en este orden[552]. Se hace hincapié, que la

[551] NAVARRETE POLAINO, Miguel, *Derecho Penal, Parte General, tomo I, fundamentos científicos del derecho penal, 6ª, edición actualizada, complementada renovada y puesta al día con la colaboración de Miguel Polaino- Orts*, Editorial Bosch, S.A., 2008, pág, 104 y sigs. El catedrático de Derecho Penal de la Universidad Sevilla don Miguel Polaino Navarrete, señala que en cuanto al *ius poenale y ius puniendi*, en cuanto a sus perspectivas dimensionales del Derecho Penal: Un criterio tradicional definición distingue entre Derecho Penal en sentido objetivo, (ius poenale) y el Derecho penal en sentido subjetivo (ius puniendi). El ius poenale es el conjunto de normas jurídicas públicas (Derecho positivo) que definen determinadas acciones como delitos imponen las penas correspondientes. El ius pouniendi es la facultad o potestad del Estado de imponer sanciones jurídico penales, es penas o medidas de seguridad, por la Comisión de delitos, esto es, la competencia de hacer valer su cometido constitucional de órgano legitimado para solucionar los conflictos criminales desencadenados en la sociedad, que conforme su escala de valores reconoce y se identifica con un ordenamiento punitivo, cuya única legitimidad titularidad es la estatal en el modelo del Estado de Derecho. A su vez, nos indica, que el hecho de la regulación normativa de la convivencia humana en sociedad es tan antiguo como el mismo hombre. Toda comunidad de seres humanos requiere de unas reglas o normas jurídicas para regir su convivencia. Para hacer valer las normas jurídicas se requiere de una situación de poder, una potestad sancionadora o conminatoria para obligar al cumplimiento de tales normas o para sancionar al que las incumpla. En el ámbito jurídico penal esa potestad sancionadora constituye el dios poniente del estado. Bien discutida es en la doctrina penal la naturaleza jurídica del ius puniendi.

[552] NAVARRETE POLAINO, Miguel, *Derecho Penal, Parte General, tomo I, fundamentos científicos del derecho penal, 6ª, edición actualizada, complementada renovada y puesta al día con la colaboración de Miguel Polaino- Orts*, Editorial Bosch, S. A, 2008, pág, 109 y sigs. El catedrático de Derecho Penal de la Universidad Sevilla don Miguel Polaino Navarrete, no señala en cuanto a la titularidad del ius puniendi, es indiscutible que el titular inmediato y directo del dios poniente y es el Estado, el cual a través de sus poderes (ejecutivo, legislativo y judicial), ejercerá esta potestad punitiva. La titularidad del ius puniendi del Estado encuentra nuestro sistema jurídico un fundamento constitucional: el artículo 140 9.1 de la Constitución española, al reseñar las materias de exclusiva competencia, señala la "administración de justicia" (apartado 5) "legislación mercantil, penal y penitenciaria" (apartado 6). Ello significa que la legislación penal compete al Estado y rige para todo el territorio del mismo. Ejemplo: el Código penal español, a diferencia determinadas normas civiles, tienen en los territorios forales secundaria aplicación. Este es el criterio seguido en los países de nuestro entorno jurídico (Alemania, Italia, Francia, Portugal). En Alemania, por ejemplo, existe un único código penal que rigen todos los Länder. Por contra en países como México cada Estado (que guarda cierta equivalencia con nuestras comunidades autónomas) tiene un código penal propio, diferente al de las demás: pues, 31 códigos, más 1 código penal Federal y un Código de Justicia Militar; en total son 33 Códigos Penal en dicho país. Aunque la doctrina tradicionalmente sostenga que nuestros días, difícilmente puede demostrarse que el *ius*

delimitación y la definición del bien jurídico protegido en esta materia, tiene de suma relevancia puesto que su extensión o la necesidad y alcance, van a determinar cuáles van a ser los efectos al momento de definir las figuras delictivas contenidas en la parte especial del Derecho Penal, toda vez que al definir o delimitar el bien jurídico, también se van a definir la tipicidad o atipicidad de una conducta determinada, también las consecuencias jurídicas, que van arrojar este tipo de delito, en este caso, informático, que no son otras que la interposición de una pena determinada.

El profesor Juan BUSTOS RAMÍREZ[553], indica que *el bien jurídico es una fórmula sintética de lo que se protege realmente*. Los presupuestos del mismo son las relaciones sociales, las posiciones que en ellos ocupan los individuos, su intermediación con las cosas y otros entes y la interacción que se produce entre ellos, reconociéndose que se trata de una relación dinámica.

En cuanto al bien jurídico propiamente tal, la protección del mismo que puede ser tomada en cuenta, por la legislaciones determinadas, son partes del mundo jurídico para proteger los bienes sociales, la intermediación de las cosas, o todo tipo de bien jurídico que interesa para la sociedad, dándose entonces la protección de variadas formas y no solamente en el ámbito del Derecho Penal, sino que también en otros ámbitos del derecho, por ello depende entonces, esta protección de las políticas criminales del lugar o del país en la cual se quiera proteger un bien jurídico determinado, tomando también en cuenta, la forma en que la delincuencia ataca el

---

puniendi, tenga un titular distinto del Estado, o, incluso, que éste lo comparta con otros poderes o instituciones y en crítica algunos autores como GARRAUD que el *ius puniendi*, es intransmisible, indelegable y no susceptible de ser compartido por una pluralidad de titulares, lo cierto es que a la luz de la conformación política de la Unión Europea estas opiniones se muestran, cuando menos, discutibles.

[553] BUSTOS RAMÍREZ, Juan, *Obras completas, tomo II, Derecho Penal Parte General*, Editorial Ara, Santiago de Chile, 2005, pág. 132.

bien jurídico determinado y el ámbito en el cual se protege, como sería en este caso la estafa por medio de sistemas informáticos, llegando así a la conclusión que todo el delito debe tener un bien jurídico preciso, concreto, que se deba proteger, por ello la legislaciones de todo el mundo constantemente están en la tarea de revisión de los tipos penales especiales, porque la sociedad y los modos en que la delincuencia actúa, cambian, más aún esta materia tecnológica, obligando al legislador a tener que analizar y estudiar, los bienes jurídico que deben protegerse, y a su vez estudiado las herramientas de protección penal para saber si ella están a la altura de los cambios de la sociedad.

Como se dijo anteriormente en esta breve investigación, en cuanto a los bienes jurídicos que tienen que ver con los delitos informáticos se refiere, depende de la postura que se adopte en cuanto a su tratamiento penal, así en aquellos casos en que se estime que los delitos informáticos, no están regulado en forma diferente o especial, sino que se deben ir ajustando a las figuras penales clásicas, el bien jurídico protegido estará entonces de acuerdo a la figura básica, ya regulada en el ordenamiento jurídico correspondiente. Ahora bien, en aquellas legislaciones donde se tomó, el tipo informático especial que regule el delito informático determinado, y de acuerdo a la forma de vulneración y ámbito de aplicación, se debe considerar entonces, el bien que conforme a la norma misma o a la historia fidedigna de su establecimiento se quiso proteger con la incorporación especial de este nuevo tipo delictivo, creando entonces un bien jurídico nuevo o muy semejante a la figura básica de la que nació, el tipo penal especial.

A diferencia del delito informático en general, como se trató en las partes anteriores de esta investigación, el bien jurídicamente protegido se centra o es colectivo, el cual redunda en la información, la cual se encuentra o almacenada, transmitida, a través de sistemas informáticos, siendo esto como un valor económico que se tiene, tanto para verlo de un punto de vista del Estado, gobierno o empresa.

Ahora bien. Podemos decir, que en el fraude informático, el verdadero bien jurídico a tutelar vendría siendo *el patrimonio,* puesto que el interés en que se centra el tipo penal que tiene una característica general, es el *adecuado funcionamiento del tratamiento electrónico de datos,* cuya importancia radica, en la economía y su administración, por lo mismo entonces resulta protegido sólo en forma consecuente. De esta manera desde la perspectiva europea, existen autores que clasifican los delitos entre aquellos en que los sistemas informáticos o sus elementos son el objeto material del mismo, y este último grupo también los autores los incluyen en los delitos cometidos mediante sistemas informáticos o utilizando elementos de naturaleza informática, que son el medio utilizado para la comisión de un ilícito patrimonial o socioeconómico[554].

A) Ofensividad, tipicidad y consecuencias jurídicas

El Derecho Penal constituye la herramienta *más enérgica* del Estado para evitar aquellos comportamientos que sean más intolerables a nivel social, pudiendo afirmar de esta manera que el conjunto normativo que constituye el Derecho penal posee sus cimientos en el hecho, que se erige como un recurso irremplazable para permitir la vida social. Ahora bien, teniendo presente que la función principal del Derecho Penal, que no es otra que el auxilio del sistema de convivencia social, deberíamos hablar que el Derecho Penal tiene un control social, por ende la sociedad, es la que otorga vida al bien jurídico que se debe amparar. En un Estado social y democrático de derecho, lo que se quiere proteger con la norma penal, no puede estar radicada solamente en el legislador, puesto que la determinación del bien jurídico y su origen corresponde a la base social, que mueve al legislador a tomar una decisión, la cual trae como consecuencia la creación o materialización de

[554] GONZÁLEZ RUS, Juan, *Protección penal de sistemas, elementos, datos, documentos y programas informáticos, En revista electrónica de ciencia Penal y Criminología*, número 1-14, 1999.

un tipo penal. Entonces, es la función de garantía del bien jurídico-penal que vendría a responder a la idea del mismo, como límite de la actividad punitiva estatal, permitiendo castigar solamente aquellos comportamientos que lesionen o lo pongan en peligro.

Ahora bien, para determinar el tipo penal, no es sólo una sumatoria de elementos subjetivos u objetivos, implica valorar otros parámetros, por lo mismo determinar la tipicidad o atipicidad una conducta constituye un proceso valorativo. Al respecto no indica SÁNCHEZ BERNAL[555], "que para cierto sector de la doctrina, señalar que el tipo penal es simplemente el continente de una acción cuya realización cotidiana por los demás elementos típicos da lugar a responsabilidad penal es cerrar por defecto, entendiendo, en suma, que dentro de cada tipo está expresada una situación social, una vinculación concreta entre dos o más sujetos en un contexto social, en el marco de un proceso interactivo. Uno de los puntos más discutidos en las disquisiciones acerca del bien jurídico en lo que se refiere a su contenido, se trata, básicamente, de poder marcar un criterio definidor, en la selección de los intereses a proteger en cada caso[556]."

[555] SÁNCHEZ BERNAL, Javier, *El bien jurídico protegido en el delito de estafa informática*, En cuadernos del Tomás Revista de estudio electrónica del C. M. Tomás Luis de Victoria, n° 1, Salamanca CT, 2009, pág. 113.

[556] GUTIÉRREZ FRANCÉS, María Luz, *Fraude informático y estafa*, 1ª Edición, Editorial Ministerio de Justicia, Madrid, 1991, págs. 204 y sigs. Quien señala que lo concerniente el sentido naturaleza el bien jurídico, por tanto su carácter social no parece la única solución defendible. "Las dificultades surgen al tratar de concretar en cada caso qué condiciones merecen la protección penal, porque la vida social se desarrolla de forma importante, a través de las relaciones dialécticas, y el legislador encuentra un elenco de necesidades sociales en clave de conflicto, detención. La consideración de esta dimensión de las relaciones sociales como sustrato del bien jurídico ha llevado a Bustos Ramírez, a definirlo como una síntesis normativa de una relación social dialéctica determinada y que implica en todo caso una valoración masiva y universal. Un rápido recorrido por el panorama doctrinal al hilo de la categoría del bien jurídico, pone de manifiesto que el punto álgido de discusión se encuentra en la concreción de su contenido, cuestión que quedó indeterminada en la construcción de FRANK, VON LIZT y en torno a la cual ha inspirado los esfuerzos principales de los penalistas posteriores. La preocupación por marcar un criterio rector en la selección de lo intereses a proteger es fácilmente explicable, pues la imprecisión en este tema

En definitiva, no sólo se debe centrar la mirada en la dimensión dogmática del bien jurídico, por el contrario se debe tener clara la función, que debe tener el Estado liberal democrático en la creación de tipos penales no pueden ser creados tipos penales en forma arbitraria, sin tomar en consideración el bien jurídico puesto que la sociedad al evolucionar en forma constante va generando estos nuevos bienes que deben protegerse por lo mismo el legislador a pesar de tener la facultad de poder crear tipos penales debe mirar siempre el bien jurídico al cual se debe proteger, tomando en consideración que el bien jurídico debe ir de la mano con las limitaciones que tiene el legislador, sabiendo desde ya que el derecho penal, tiene una función social y de control de la misma. Por esta razón, el derecho penal sólo cumplirá su función dentro de la sociedad en la medida que se vaya adaptando sea un mejor Derecho Penal, no uno más amplio, debe ser dinámico, no más abundante sin olvidar que el fundamento de la existencia de la pena como mecanismo de control debe tener su fundamento en el bien jurídico protegido, estableciendo entonces el binomio esencial, entre delito y pena[557].

---

malogra el sentido mismo y los fines del bien jurídico que queda convertido en una pieza inútil. Si, en último término, lo que marca la frontera de lo punible son los valores dominantes, entendidos como los valores de los que dominan, el esfuerzo por configurar esta categoría habrá sido baldío y el resultado no estará muy distante del que alcanzan las concepciones inmanentes, ajenas a la idea del bien jurídico como límite. A partir de esto, y dirigidas a superar la deficiencia reseñada, comienzan a sucederse una variada gama de construcciones que, finalmente, nos conducen al posicionamiento bicéfalo actual: de una parte las teorías constitucionales, que buscan en la norma fundamental los criterios selectivos de los intereses que pueden ser protegidos y, de otra, las construcciones estrictamente sociológicas, que remiten de forma directa a la realidad social como única vía para dotar de contenido material al bien jurídico".

[557] NAVARRETE POLAINO, Miguel, Derecho Penal, Parte General, tomo I, fundamentos científicos del derecho penal, sexta edición actualizada, complementada renovada y puesta al día con la colaboración de Miguel Polaino- Orts, Editorial Bosch, S.A., 2008, págs., 60 sigs. Quien señala, al tratar los fundamentos de la pena, la necesidad de la sanción penal, la pena se legitima por sus fines que son preventivos y tutelares, y se fundamenta en su necesidad. Como dijera MAURACH, "una comunidad que renunciara a su imperio penal renunciaría a sí misma". Ningún Estado, ninguna sociedad, puede prescindir de su poder coercitivo que nunca es poder ilimitado, pues éste es, sin duda, un medio lícito necesario para la consecución de un fin general: la seguridad jurídica. La necesidad de la sanción penal es, a la vez, fundamento y límite de la pena: se impone una pena la

Por último el bien jurídico posee una función sistematizado era, para crear un sistema penal coherente, toda vez que los mismos bienes jurídicos se configuran como un criterio para unificar criterios dentro de las normas penales positivas y los códigos y compendios de ellas[558].

B) Bien jurídico protegido, en la estafa informática

Vale hacer mención, que la creación del bien jurídico responde a la forma en que legislador opta, por entender el fenómeno propiamente tal de la delincuencia informática, puesto que si se enfoca solamente en ella, y no en la protección de bienes jurídicos para estas figuras, se crean viene jurídicos no reales o artificiales. El bien jurídico al tomar en cuenta el fenómeno de la delincuencia informática, puede recaer en la calidad o pureza y también en la idoneidad de la información contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan.

Según el profesor ÁLVAREZ FORTTE, ha presentado varias diferencias entre los legisladores en la actualidad, la creación de un bien jurídico, por cuanto se estima por algunos que el hecho de tratar estos hechos desde un punto de vista puramente fenomenológico, desvincula la nueva regulación del sistema de valoraciones subyacentes en el ordenamiento penal, dando lugar a problemas de legitimación y coherencia normativa, por cuanto se limita a aplicar sanciones a

---

medida en que la sociedad necesita, como condición de la vida comunitaria, tutelar bienes, prevenir futuros delitos, contribuir a la consecución de un orden de seguridad jurídica, etcétera: sólo la pena "necesaria" es una pena "justa".

[558] SÁNCHEZ BERNAL, Javier, *El bien jurídico protegido en el delito de estafa informática*, En cuadernos del Tomás Revista de estudio electrónica del C. M. Tomás Luis de Victoria, n° 1, Salamanca CT, 2009, pág. 113.

determinadas conductas que aparecen como típicas, prescindiendo de la razones que legitiman la incriminación[559].

Cuando el Derecho penal, toma en consideración como pilar fundamental para la creación de normas, sólo el amparar bienes jurídicos, evita con ello que se sancionen conducta sin daño, con esto el Derecho penal da cabida al principio de proporcionalidad con el fin de cautelar las consecuencias jurídicas del delito, la pena, evitando con ello un exceso en la misma. Sirviendo entonces, el análisis del bien jurídico al momento de crear un tipo penal como base, para que se castiguen ciertas acciones que vulneran derechos. Es justo y prudente en este párrafo señalar el cuestionamiento planteado en abstracto por el Dr. POLAINO NAVARRETE, quien citando a Dr. JAKOBS indica, "que indica que es un sinsentido afirmar que el derecho penal protegen bienes jurídicos, siendo así que dicho ordenamiento pone en marcha su mecanismo de protección una vez que el bien ya sido lesionado o puesta en peligro, quien de manera irreparable o sea como diría su maestro presente en el derecho penal actúa siempre demasiado tarde"[560]. Lo que cuestiona en el trabajo del profesor, que valía el derecho penal protege la vigencia de la norma, la autoconstatación del poder político del Estado, la defensa de una infraestructura de expectativas[561][562].

[559] ÁLVAREZ FORTTE, Héctor, *Los delitos informáticos*, Corpus Iuris, Revista jurídica regional N° 9, Chile, 2009, pág 101 y sigs.

[560] POLAINO NAVARRETE, Miguel, Derecho Penal, Parte General, fundamentos científicos del derecho penal, tomo I, 6ª edición actualizada, complementada renovada y puesta al día por POLAINO-ORTS Miguel, Editorial Bosch, S. A., 2008. pág. 135 y sigs.

[561] Sobre este punto, El Dr. POLAINO NAVARRETE, plantea el cuestionamiento y nos explica que desde la primera mitad del siglo XIX hasta bien entrado el siglo XX, durante un largo periodo de tiempo, nadie cuestionaba la virtualidad del concepto de bien jurídico como elemento definidor de la función esencial del Derecho penal. El bien jurídico en un dogma casi intocable la ciencia penal. Y, por eso, llegamos a lo mismo: durante todo ese tiempo, existía acuerdo en que la función esencial, legítimamente, del Derecho penal era la protección devine jurídicos, sea como fuera la forma en que éstos se entendían. El mismo profesor, también explica la revisión dogmática que

En el capítulo referente al concepto del delito informático, se pudo analizar las distintas definiciones del mismo que existen, y también sus clasificaciones. Además de ello se llegó a la conclusión que no existe una definición de delito informático legal, sino que sólo doctrinal[563], tal cual sucede con las distintos

realiza el Dr. JAKOBS del dogma del bien jurídico aceptado, de esta manera la concepción de Jacob no prescinde totalmente los componentes ético sociales en la protección penal, que definían y legitimaba la función de tutela punitiva en la concepción de su maestro HANS WELZEL, padre del idealismo jurídico penal. En efecto, en la construcción de su peculiar sistema funcionalista, no se aparta Jakobs totalmente de la doctrina finalista en lo referente a su mencionada teoría de la protección de los valores éticos sociales de conducta. Citando a WELZEL, dice JAKOBS que el derecho penal debe proteger valores éticos sociales, argumentando que así hay que comenzar si no se quiere entender los efectos del derecho penal al igual que el invierno y el verano, como sucesos de naturaleza, sino al igual que el enunciado la respuesta como hechos sociales. Pero a partir de ahí, como afirma el mismo JAKOBS, se apartan los caminos y quiebra la dogmática ontologista. JAKOBS, Günther / POLAINO NAVARRETE, Miguel / POLAINO ORTS, Miguel, Bien jurídico, vigencia de la norma y daño social, 1ª Edición, Editorial Ara, Perú. 2010. Pág. 42.

[562] Igualmente considero ilustrativo citar nuevamente al Dr. POLAINO NAVARRETE, quien con una increíble capacidad explicativa y de síntesis nos resume la concepción funcionalista normativa del Dr. Jakobs que critica la concepción tradicional del bien jurídico, en diversos sentidos: a) la lesión o puesta en peligro del bien no sirve para definir de manera exclusiva el contenido del injusto en el Derecho penal, en tanto que se trata de un suceso compartido con los fenómenos naturales. b) La secuencia delito-pena no puede explicarse de manera negativa (como imposición de un mal ante un mal cometido), sino positiva: como reafirmación de la dirigencia quebrada de la norma. c) En consecuencia, la norma pasa ser el elemento principal definidor de la dinámica de protección del Derecho penal, trasladándose la lesión o puesta en peligro devine jurídicos a un segundo plano. Y ello porque el concepto de bien jurídico ofrece deficiencias a la hora de definir el ámbito de protección o tutela penal: ante todo, porque la lesión consumada es, a veces, irreparable, de manera que ya entonces la protección devine jurídicos por parte del Derecho penal ha sido ineficaz. JAKOBS, Günther / POLAINO NAVARRETE, Miguel / POLAINO ORTS, Miguel, *Bien jurídico, vigencia de la norma y daño social,* 1ª Edición, Editorial Ara, Perú. 2010. pág. 47.

[563] GALÁN MUÑOZ, Alfonzo, *El fraude y la estafa mediante sistemas informáticos*, Editorial Tirant lo Blanch, Valencia, 2005, págs. 29 y sigs. Al respecto, señala en cuanto a las consideraciones previas en el determinado delito informático, que la aparición de nuevos tipos penales específicamente dedicados a sancionar aquellas conductas que atentas encontraré jurídicos tanto tradicionales como de nueva creación, mediante la utilización de nuevos medios tecnológicos que aporta la informática, ha llevado a que la doctrina se haya cuestionado la posibilidad de agrupar todas estas figuras bajo la denominación de delitos informáticos, concepto que sin embargo, carece de respaldo legal alguno, lo que dota de unos contornos difusos y controvertidos. Así pues, el concepto de delito informático es un concepto de naturaleza claramente doctrinal y no legal, habiéndose desarrollado definiciones del mismo de una enorme amplitud, con la única pretensión de dar cabida en su seno a todas las posibles figuras delictivas que tuviesen o pudiesen tener una conexión con el uso del sistema de tratamiento electrónico de datos, considerándose, por ejemplo,

conceptos en esta materia como son por ejemplo cibercrimen, o inclusive la distintas denominaciones que se dan a las personas que se involucran en este tipo de delitos como serían los hacker. Además de ello, se debe tomar en consideración la distintas disciplinas que están envueltas en esta materia, y por lo mismo podríamos hablar de una multiplicidad de bienes jurídicos que deben ser protegidos en cuanto al delito informático se trata, toda vez que puede estar envuelto tanto el patrimonio, la vida, el libre comercio en la red, o a través de los sistemas informáticos, puesto en el que todos ellos tienen como factor común que se cometen a través de los sistemas informáticos e Internet.

A este respecto, debemos tener primero que todo una aproximación a la noción de patrimonio, en esta materia el profesor Balmaceda Hoyos[564], señala que la doctrina y jurisprudencia comparada mayoritaria sostiene que el patrimonio, es visto en idéntico sentido que en el delito de estafa clásico o tradicional, es decir el bien jurídico-penal protegido en este delito, puesto *fraude informático* sintetiza una diversidad de comportamientos lesivos de múltiples intereses económicos, efectuados con ánimo de conseguir un provecho económico y explotando las singulares peculiaridades de los medios informáticos y su funcionamiento.

Observado el fraude informático, en un sentido amplio como defraudaciones por medio de computadores, mediante manipulaciones informáticas de cualquier tipo. Ahora, cuando se habla de defraudación, como una producción de un perjuicio económico por medio de una dinámica comisiva ideal, intelectiva, subrepticia o engañosa. En este mismo sentido, desarrolla la idea el profesor, BALMACEDA

---

que los delitos informáticos serían *todas las conductas criminales que se realicen a través del ordenador electrónico, o que afecten al funcionamiento de los sistemas informáticos.*

[564] Al respecto indica BALMACEDA HOYOS, Gustavo, *El delito….Op. cit.*, pág. 134 y sigs.

HOYOS[565], al referirse, también a la idea de *delito informático*. en la cual se efectúa una consideración tipológica en el marco de lo que se denomina "derecho penal global del riesgo informático y de la información", entendiéndose como una diferenciación entre el delito vinculado a la informática y el delito informático como delito que se denomina *del riesgo informático y de la información*, situándose en el primer grupo aquellas conductas que recaen sobre elementos físicos informáticos o aquellas que utilizan al medio informático, sin que se afecte en forma alguna a la información en sí misma, los datos, o los sistemas de su tratamiento y dentro del segundo grupo quedarían aquellos comportamientos que si utilizan al medio informático con daño a la información en sí misma, los datos, o los sistemas de su tratamiento.

Ahora bien, se debe tomar en consideración de alguna manera el concepto de patrimonio para determinar el bien jurídico protegido en la estafa informática, siendo necesario entender el origen del concepto patrimonio para poder entenderlo desde el punto de vista del Derecho Público, como es el Derecho Penal. Señala de al problema el hecho que la doctrina no está conteste, en su definición, naturaleza o contenido, existiendo autores entonces que tienen ciertas informática no sólo debería amparar el patrimonio individual, sino también de naturaleza colectiva, tomando en consideración la seguridad de los sistemas informáticos.

TIEDEMANN, citado por el profesor BALMACEDA HOYOS, en cuanto trata la concepción jurídica del patrimonio[566], opina que la estafa informática se sitúa en el grupo al que denomina *delitos que protegen bienes jurídicos supraindividuales*

[565] Al respecto indica BALMACEDA HOYOS, Gustavo, *El delito….Op. cit.*, pág. 135 y sigs.

[566] BALMACEDA HOYOS, Gustavo, *El delito de estafa informática*, Editorial Jurídicas de Santiago, 2009, pág 145 y sigs. "Tiedemann, 199, NM 128; Aús Batrrita, 1993, pág. 55 y sigs.; Huerta Tocildo, 1980, pág. 28 y sigs.".

intermedios, los cuales no pueden ser incluidos en la clase de los intereses jurídicos pertenecientes al Estado, pero tampoco pueden ser reconocidos dentro de los intereses del individuo interviniente en el tráfico comercial. Considera además, a la estafa informática como un delito económico en sentido amplio, ya que no surge para ser aplicado a las infracciones penales en el ámbito del Derecho administrativo regulador de la intervención del Estado en la economía[567].

[567] Resulta muy útil tener la visión del profesor BALMACEDA HOYOS respecto del patrimonio, el cual en lo medular indica que en cuanto El patrimonio individual micro-social como bien jurídico. La mayoría de la doctrina comparada ha sostenido que el tipo de la estafa informática busca resolver los problemas que los delitos denominados tradicionales muestran cuando se tiene que dar un ajustado resguardo al patrimonio en aquellos casos en los que, tanto el objeto en el que recae el comportamiento al lesionarlo, como el medio utilizado para llevarlo a efecto, poseen un carácter preferentemente informático. Fue así, por lo que a primera instancia se buscó efectuar otra lectura del delito de estafa tradicional. Ya que se reparó que éste es el único tipo legal de entre los clásicos delitos guardianes del patrimonio que lograría mostrarse como apropiado para castigar penalmente a estos nuevos cauces de lesión de dicho bien jurídico-penal, estimables, manifiestamente, de tal forma de castigo. Actualmente la mayoría de la doctrina comparada viene en sostener que el patrimonio es el bien jurídico que se protege en el delito de estafa tradicional, lo que exigiría un perjuicio patrimonial como resultado y también una instrumentalización de la víctima a través del engaño. De igual manera, debería abandonarse la tesis de que también en la estafa se protege la buena fe en el tráfico jurídico, ya que no existiría un *derecho a la verdad*, debido a que el engaño no poseería relevancia jurídico-penal y en general en el derecho comparado no se estima consumado el delito, sino hasta la producción de un daño patrimonial. Cabe hacer presente, que el ámbito del patrimonio no se reduce al derecho real de propiedad, sino que podría recaer en cualquier otro elemento que integre el patrimonio, por ello se entiende que en la estafa se protegería al patrimonio en sentido amplio.

Dicho profesor se refiere al Contenido del patrimonio, como la lesión del patrimonio consiste en su dimensión económica y para determinarla no habría más que estimar al patrimonio en su totalidad como *universitas iuris*, ya que el delito de estafa se consuma en el momento del perjuicio patrimonial, por lo que en definitiva, la estafa es imprescindible un perjuicio económico, cuya determinación podrá considerarse valorando al patrimonio en su conjunto, antes y después del delito, atendiendo al valor económico de sus componente y a la importancia económica que en el conjunto pueda tener menoscabo.

Asimismo se refiere al Concepto jurídico-penal del patrimonio. Es ampliamente debatido el concepto jurídico-penal de patrimonio a efectos del delito de estafa, y por ello la doctrina adopta diferentes posturas, vista como una concepción jurídica, una económica, una mixta o jurídico-económica, y por último, existen las teorías personales/funcionales del patrimonio. Resulta preciso destacar el criterio que se ha asumido en el anteproyecto de código penal chileno, cuyo artículo 159 prescribe: "El que con ánimo de lucro y mediante un engaño suficiente para provocar error en otro, obtenga que éste realice una disposición patrimonial con perjuicio propio o de tercero, será

Según expone SÁNCHEZ BERNAL[568], citando a GALÁN MUÑOZ, que el delito de estafa informática se caracteriza por ser un delito protector de un bien jurídico intermedio, por ende considerado un delito de peligro-lesión, negando la necesidad interpretar de forma vinculada el delito de estafa y el delito estafa informática, siendo protector de bienes jurídicos eminentemente colectivos, clasificado entre los

---

castigado con pena de reclusión menor en su grado mínimo a medio. La pena se podrá elevar en un grado cuando el hecho revista especial gravedad, en atención a la cuantía del perjuicio ocasionado o los efectos especialmente perjudiciales que tenga para la víctima. Tratándose de perjuicios de ínfima cuantía, el tribunal podrá prescindir de la pena de reclusión e imponer en su lugar solo la pena de multa de una a diez unidades tributarias mensuales".

Desarrolla también las concepciones existentes en relación con el concepto jurídico-penal de patrimonio: a) Concepción jurídica del patrimonio. En esta concepción, el patrimonio es el conjunto de derechos patrimoniales de una persona y por lo tanto no habría estafa en los siguientes casos: cuando no existe derecho defraudado; cuando dice relación con un negocio con causa ilícita, o cuando se engaña a otro en una expectativa de derecho, circunstancia que no parece responder a las finalidades político-criminales del delito de estafa. b) Concepción económica del patrimonio. Esta concepción fue predominante por mucho tiempo y con ciertas correcciones jurídicas, aún se conserva la definición básica, viendo al patrimonio como *el conjunto de bienes de valor monetario de una persona*, busca observar el patrimonio en su faceta de poder en el tráfico mercantil, pero se critica que no relaciones al patrimonio con una realidad objetiva, exigiendo valoraciones de orden valorativo. Esta idea sólo salvaguarda concepciones de carácter monetario, pero todas aquellas que posean dicho valor, siendo la crítica más relevante que se hace a esta postura, ya que estima la estafa solo cuando el menoscabo económico es originado, atacando un poder o señorío no tutelado en forma jurídica, así, se dice que acentúa el papel del engaño y que menosprecia la importancia del desvalor de resultado. c) Concepción mixta o jurídico económica del patrimonio. Cabe hacer presente que lo que se ha impuesto en la dogmática es un modelo económico de patrimonio al cual se le han incorporado correctivos normativos para eludir las contradicciones valorativas a que podía conducir la variante "pura" o "extrema" del mismo, dando lugar a la concepción dominante en derecho comparado. Según esta postura, el patrimonio debería entenderse en sentido amplio, es decir, como una suma de relaciones jurídico-patrimoniales que sean idóneas de valoración económica. d) Concepción personal del patrimonio. Esta concepción supone un paso más adelante, en el sentido que su concepto supera aquellas tesis que se circunscriben a implantar correctivos en el caculo del perjuicio para tener en cuenta una "personalización del perjuicio" que iría de la mano de una reformulación de la idea de patrimonio también *personal*. BALMACEDA HOYOS, Gustavo, El delito de estafa informática, Editorial Jurídicas de Santiago, 2009, pág 142 y sigs. (en esta nota al pie, lo que se trató de hacer fue extractar, siguiendo la estructura que sigue dicho profesor, de manera tal que se pueda, tener la visión general de dicho planteamiento, resumiendo sus ideas en estas líneas).

[568] SÁNCHEZ BERNAL, Javier, *El bien jurídico protegido en el delito de estafa informática*, En cuadernos del Tomás Revista de estudio electrónica del C. M. Tomás Luis de Victoria, n° 1, Salamanca CT, 2009, pág. 117.

delitos económicos en sentido amplio, hablando entonces de bien jurídico intermedio, protegiendo intereses de naturaleza muy diversa. Existiendo eso sí, el problema para diferenciar este tipo delictivo frente los tipos, que puede considerarse como meros delitos tour y ofensivos de peligro[569].

[569] GALÁN MUÑOZ, Alfonzo, *El fraude y la estafa mediante sistemas informáticos*, Editorial Tirant lo Blanch, Valencia, 2005, págs. 198 y sigs. Al desarrollar, la idea de la estafa informática como delito protector de un bien jurídico intermedio, señala que una vez que se niega la necesidad de la vinculación de la interpretación del delito de estafa y del delito de estafa informática, parece factible sostener que este nuevo delito vendría tutelar valores que trascendían los exclusivamente patrimoniales individuales, contemplando también la afección devine jurídicos de naturaleza eminentemente colectiva, postura que por otra parte fue la que permitió a Tiedemann, enclavar a la estafa informática entre los delitos económicos en sentido amplio. Dicha concepción del objeto jurídico el delito de estafa informática lleva a que haya de entenderse en este delito protegería un bien jurídico intermedio, caracterizado por el hecho de que el mismo aparecen vinculados mediante bienes de naturaleza diversa (individual uno y colectivo en otro); relación que, en el caso de la estafa informática, sólo podría basarse en el hecho de que tales bienes se encontrasen en la misma línea de ataque del comportamiento punible, ya que resultaría inadmisible considerar como viene jurídicos homogéneos a la seguridad o a la corrección de los sistemas informáticos y el patrimonio individual. Por otra parte, para apreciar la presencia de un verdadero y jurídico intermedio en un delito, no bastará con que una misma conducta supiese una afección de los bienes jurídicos de naturaleza diversa, puesto que de admitirse esta posibilidad resultaría imposible delimitar los delitos que protegen este tipo de bienes jurídicos, y aquellos otros que deberían ser considerados como meros delitos pro defensivos de peligro. En este sentido, Mata y Martín señalaba que, si por algo se caracterizaban los delitos protectores de un bien jurídico intermedio frente a los simples delitos defensivos de peligro, sería por el hecho que para su consumación siempre se exigirá la efectiva lesión de uno de los dos valores que lo conforman, el colectivo o individual, exigencia que sería la que dotaría los delitos protectores de bienes jurídicos intermedios de una estructura de delitos de lesión y peligro, claramente diferenciada de dar aquellos. Como consecuencia de lo expuesto, debemos concluir que para poder calificar el delito de estafa informática como un delito protector de un bien jurídico intermedio, se debería firmar que su conducta típica tendería a lesionar inmediatamente un bien jurídico individual, provocando con dicha lesión la simultánea puesta en peligro mediata de otro valor de naturaleza diversa a la del primero; pero ¿resulta realmente posible apreciar esta estructura del delito de lesión-peligro en el delito de estafa informática?. El pretendido bien jurídico intermedio protegido por el delito de estafa informática, vendría dado por el interés general en la corrección y seguridad del funcionamiento de determinados sistemas informáticos, bien jurídico que encontraría en el patrimonio su ineludible referencia individual, siendo precisamente la decisión de éste último la que supuestamente debería permitir apreciar la puesta en peligro de aquel. En efecto, la lesión del patrimonio como bien jurídico eminentemente individual aparece expresamente recogidas como exigencia típica del delito estafa informática de nuestro Código Penal, siendo exigida también por la doctrina mayoritaria de Alemania, lo que obliga a entender que el patrimonio sería el referente individual del presunto bien jurídico intermedio de naturaleza colectiva, como sería la seguridad de los sistemas electrónicos de transferencia de activos.

Es muy importante, referirse a la conclusión que llega el profesor BALMACEDA HOYOS, el cual, llega determina que la interpretación que parece más idóneo incoherente es aquella que concibe el delito de estafa como un delito contra el patrimonio, y que concibe al engaño típico como un riesgo del perjuicio patrimonial, es decir la instrumentalización de la víctima debería ser un proyecto de lesión patrimonial y el perjuicio, la concreción en el resultado de tal introdujo mentalización.

Por último, puede concluirse tal como lo hacen, GALÁN MUÑOZ, SÁNCHEZ BERNAL, BALMACEDA HOYOS, que el bien jurídico protegido en el delito de estafa informática es el patrimonio, pero entendido en una forma amplia, es decir como un conjunto de derechos, bienes, de relaciones jurídicas que puedes ser titular un sujeto encuadrando por tanto, este tipo de delito, dentro de una categoría genérica siendo un delito económico de enriquecimiento, con la particularidad de tratarse de un tipo de delito de apoderamiento[570].

A lo largo de este capítulo, se ha venido hablando de distinto tipos de fraudes informáticos sin dar una explicación mayor al respecto de los mismos. Muchos de ellos, se han escrito en idioma inglés, puesto que la mayoría han sido creados en países se habla inglesa. Se considera entonces necesario, que en el capítulo siguiente, antes que se trate el tema de la estafa informática propiamente tal, se analice en forma sintética, cuales son las figuras más usadas en el mundo de la

[570] GALÁN MUÑOZ, Alfonzo, *El fraude y la estafa mediante sistemas informáticos*, Editorial Tirant lo Blanch, Valencia, 2005, págs. 281 y sigs. Resulta indudable por tanto, lo denominado delitos de apoderamiento tenderían a proteger el patrimonio y que se diferencian del resto de delitos patrimoniales de enriquecimiento y entre ellos de las denominadas defraudaciones, como la estafa, no por tener un diferente bien jurídico sino por el diferente contenido del test valor de su conducta típica. Se convertiría así al patrimonio en el elemento determinante del contenido material de los injustos contemplados en la mayoría de los delitos contenidos en el título XIII del libro segundo del Código Penal, y entre ellos de los de apropiación como el hurto del robo, no pudiendo afirmarse, por tanto, que su protección fuese un rango distinto o exclusivo de las defraudaciones y de forma más específica de la estafa.

delincuencia informática en relación al tipo penal anunciado en esta parte de este estudio. De esta manera el lector de antemano, tendrá la posibilidad de obtener una visión general de dichas técnicas delictivas y poder con ellas hacer la adecuada relación con los tipos de legales que regulan la estafa informática en el mundo.

CONCLUSIONES

- La constante evolución de la tecnología de la información incrementada por el tipo de economía prevalente en el mundo, han hecho que internet se transformen el motor de movimiento de casi toda la vida, tanto de los países como de la persona, trayendo consecuencias tanto a nivel de mejora de la calidad de vida en muchos aspectos y también traído consecuencias nefastas. Por un lado la comunicación instantánea entre las personas, facilita la vida de todo punto de vista, nos entrega la posibilidad de poder entregar conocimientos en tiempo real como es hoy en día la educación a distancia, enviar o ver imágenes en tiempo real posibilitando con ello la cercanía entre las personas que se encuentran en países distintos, la posibilidad de obtener bienes y servicios que hace 20 años atrás sería impensable poder obtener, reemplazándose igualmente el dinero material por el virtual[571]. Con respecto a esto SILVA SÁNCHEZ, refiere que "los fenómenos de la globalización económica e integración supranacional sobre la delincuencia. Por un lado aunque interesa aquí en menor medida da lugar a que determinadas conductas

[571] "Es precisamente, en el ámbito social, donde la persona desarrolla todo su potencial, donde goza de los beneficios de la modernidad y del progreso, donde participa en tanto destinatario del núcleo social de los progresos que la propia sociedad alcanza un; sin embargo la contrapartida de los beneficios y bienestar que se han alcanzado hoy en día, radican precisamente en el incremento de los riesgos (sobretodo tecnológicos), que se producen precisamente como consecuencia del desarrollo social, sin embargo un factor a tomar en consideración es que muchos de los riesgos que se presentan en este ámbito difícilmente resultan detectables por la propia sociedad". COLINA RAMÍREZ, Edgar, *Sobre la legitimación del Derecho penal del riesgo*, Editorial Boch, Sevilla, 2014, pág. 25 y sigs.

tradicionalmente contempladas como delictiva, deban dejar de serlo, por lo contrario se convertirían obstáculo a las propias finalidades perseguidas con la globalización y la integración supranacional"[572]. Agrega el mismo autor, "los fenómenos económicos de la globalización y de la integración económica da lugar a la conformación de modalidades nuevas delitos clásicos, así como la aparición de nueva forma delictiva. Así, la integración genera una delincuencia contra intereses financieros de la comunidad ducto de la integración (fraude al presupuesto, criminalidad arancelaria, fraude de subvenciones), al mismo tiempo que contempla la corrupción de funcionarios de las instituciones de la integración[573].

- Al ver en forma general los delitos informáticos, se puede establecer que la relación que existe entre delito y la informática se explica desde el punto de vista de los delitos tradicionales, con los que se utiliza como medio de comisión la tecnología de la información y los delitos informáticos propiamente tales, cuando se emplea la informática, atacando algún sistema como el de datos o programas. La doctrina y también la jurisprudencia, utiliza términos diferentes para referirse a los delitos informáticos, ya su vez al bien jurídico protegido, entregando distintas clasificaciones y términos relacionados con los mismos, existiendo dificultad muchas veces para poder conectar una figura nueva delictiva informática, con los tipos penales, tanto por la variabilidad y evolución rápida que va teniendo la delincuencia informática, sumándose los componentes transfronterizos que envuelve al sistema de

[572] SILVA SÁNCHEZ, Jesús María, *La expansión del derecho pena, aspectos de la política criminal en las sociedades postindustriales*, 3ª Edición, Editorial Edisofer, España, 2011, pág, 89.

[573] SILVA SÁNCHEZ, Jesús María, *La expansión del Derecho penal*…, op. cit., pág. 90.

internet, siendo una tarea inmensa tanto para juristas como por la doctrina, poder desarrollar la prevención y la represión estos delitos, todo ello en vista a lo que se estudió respecto a la forma en que funciona la red y especialmente lo explicado respecto de la navegación anónima en la llamada internet oculta, pudiendo decir que hoy en día escapa a la regulación gubernamental o mundial cuando el delincuente utiliza este medio para llevar a cabo sus fraudes.

- Asimismo se estima que la problemática de los delitos informáticos y también su regulación jurídica, es un tema para todo complejo, por ello en la primera parte de esta investigación se abordó en forma general los delitos informáticos, su clasificación y elementos, y también las características especiales que adquieren dichos ilícitos puesto que se usa el medio de internet para lograr los fines delictivos. A su vez, también se llega a la conclusión que para poder hacer frente este tipo de delincuencia, todos los operadores jurídicos deben tener la instrucción suficiente, tanto para entender el mundo virtual y las características especiales de la informática, como para poder legislar adecuadamente respecto. Se ha visto, que él legislaciones como la chilena se ha tenido que forzar la ley penal, para poder adecuarla a los nuevos delitos, especialmente en el caso del fraude, debiendo ser un esfuerzo la judicatura para poder lograr que a base de la norma existente pueda sancionarse un hecho ilícito relacionado con la informática en este caso estafa informática. Podemos decir entonces, que es necesario adecuar la técnica legislativa a los nuevos tiempos, para ello las reuniones multinacionales y los constantes congresos o convenciones respecto del tema, son sumamente necesarios para unificar criterios a nivel internacional, toda vez que si no se legisla en conjunto muchas de las actividades que se realizan a diario, que pueden ser constitutivas de delito hoy en día en internet no lo son, tanto porque no se ha legislado de manera adecuada o simplemente porque no existe norma penal que lo

sancione, todo ello también debe ir de la mano de los derechos fundamentales, porque su vez al controlar o regular Internet de alguna manera tendrán que suprimirse las libertades totales que existen hoy en día la red, grupos internacionales defienden hoy en día el anonimato, arguyendo que los estados no pueden controlar la libertad de movimiento por decirlo alguna manera en el espacio virtual, siendo alterados los derechos fundamentales, como el derecho la intimidad y a la privacidad de las comunicaciones, sin embargo ello está en contraposición con muchas leyes internas de cada país, puesto que al no existir regulación se tiende a pensar que se puede realizar cualquier acción, como sería el caso de transacciones nacionales o internacionales virtuales, de sustancias ilícitas o de cualquier otro tipo de bien que esté prohibido en el comercio real. Asimismo cuando estamos frente la protección adicional de los derechos fundamentales, toda restricción de ellos debe estar fundamentada o autorizada la ley, por esta razón los países igualmente debe legislar respecto de la intervención de los medios de comunicación, puesto que de no ser así dejan a las policías especializadas en investigación informática, sin herramientas para poder controlar la delincuencia somática, las deficiencias en esta materia no solo existen a nivel nacional, sino también en desacuerdo con las grandes empresas transnacionales que han hecho del traspaso de información un negocio de millones de dólares, oponiéndose tenazmente a la posibilidad, de entregar información cuando es relevante, en el caso de delitos.

- En cuanto a las metodologías de investigación tradicional se ven sacudidas por la introducción de nuevas tecnologías, las cuales si bien no fueron creadas con fines maliciosos, son utilizadas por el crimen organizado cada vez con mayor frecuencia, toda vez que el crimen organizado se aprovecha de las ventajas de ecosistema que le brinda la Deep & Dark Web y las criptomonedas. El programa (TOR) y la criptomonedas son sólo herramientas, no son las

causantes del problema, desde siempre ha sido el hombre quien le ha dado un uso positivo o negativo a una determinada herramienta. Tratar de alguna manera regular sería asimilable como tratar de tapar el sol con la mano, puesto que debe existir una organización conjunta mundial para combatirla.

- El fraude electrónico tiene como principal característica el medio de comisión por el desarrollo inimaginable de la tecnología de la información, tecnología que opera en forma universal, de forma común y cotidiana sumando a todas las personas que tengan la posibilidad de acceso un ordenador conectado a la red para que pueda pertenecer al mundo virtual del intercambio de información y de bienes y servicios, siendo la red compuesta por un número sin precedente de instituciones, tanto bancarias como gubernamentales y privadas operando todas ellas bajo el sistema de la vía electrónica. En la materia que nos ocupa dicho fraude por la legislación española toma el nombre de estafa informática, la cual tiene como denominador la manipulación, interviniendo en la tecnología informática, sustituyendo con la conducta al titular legítimo del derecho, con la persona del delincuente, requiriendo para su consumación al igual que el tipo tradicional de estafa que se produzca un daño en el patrimonio de la víctima. Al desarrollarse la tecnología de la información, ha favorecido las múltiples formas, como se analizó respecto de las modalidades del fraude en la red, es como son por ejemplo el caso del phishing y el pharming considerándose estas formas de delincuencia tecnológica como los efectos colaterales a la nueva forma de transferencia y movilidad de los bienes de capital. Toda la información que existe, agrupada en agencias de datos del gobierno, o en entidades bancarias facilitan de una u otra forma el mercado para este tipo de fraudes, usándose entonces la red tanto para fines lícitos como ilícitos

- No existen teorías para poder explicar el fenómeno de la existencia del fraude electrónico y menos aún para la delincuencia informática. Sin embargo este

tipo de delincuencia se ha desarrollado por los recursos tecnológicos sofisticados, teniendo un acceso a comunicaciones sin fronteras y además totalmente despersonalizada y anónimas. Según ciertas teorías sobre la criminalidad informática, a pesar que sería un contrasentido hablar de grupos íntimos en la red, no impide que existan grupos selectivos y que se logre una intimidad a distancia, que a los efectos del aprendizaje equivale a la situación descrita por el criminólogo SUTHERLAND[574], puesto que lo íntimo tiene relación con el contacto de contigüidad física, pero en la red, la técnica pueden difundirse por la red, incluso a través de grupos íntimos de acceso restringido con características propias. Se sumó lo anterior, que hoy en día, existe una sensación diferente respecto de lo que es legal e ilegal, en cuanto a la información contenida en la red, siendo ambiguas imprecisas, entendiéndose por el común de la gente que cuando se encuentra en la red algún tipo de información se puede utilizar de cualquier manera no existiendo una relación de la propiedad intelectual o algún otro delito informático[575].

[574] GABALDÓN GERARDO, Luis, Fraude electrónico…Op. Cit., pág. 198.

[575] Gabaldón citando a Castell, nos indica que "[…] sugiere el desarrollo de una extensión mundial de redes criminales que, a su vez, contarían con identidades culturales ancladas en sus sitios de origen, y que les permitirían adaptarse a cambios en los patrones de persecución a nivel internacional. Aunque ese tema está planteado para las formas de delincuencia organizada mejor descritas, como el tráfico de drogas, armas, personas y materiales radioactivos, podría pensarse en una tendencia equivalente para otras formas de criminalidad, como los fraudes. Pero ¿qué de particularmente cultural e idiosincrático tiene el fraude electrónico, o cuál es el impacto de la localidad en sus manifestaciones? En su ensayo sobre el fraude telemático, sugiere un desarrollo futuro estratificado de las transacciones con tecnologías de la información: un nivel estará representado por el comercio e intercambio seguros, con protocolos y claves estandarizados, supervisados y reforzados, con primas por el acceso, y otro nivel inseguro y devaluado, sin supervisión, con intercambio azaroso y de libre acceso. Ambos niveles diferenciarán a los pudientes de los no pudientes en la era informática, una distinción que hasta ahora es algo borrosa. Esto podría equivaler a la distinción entre la economía formal e informal, o entre ricos y pobres, o entre urbanizaciones y barrios en una ciudad. ¿Cómo se manifestará el fraude entre estos dos mundos y qué espacio quedará para lo regional y lo local? Si los patrones de desarrollo planetario persisten y si la transferencia de bienes y servicios se generaliza mediante medios de pago electrónicos, habrá mucho que aprender de la diversidad y la estratificación, en cuanto a vulnerabilidad, modalidades,

- Después de este sintético análisis, respecto a los fraudes cometidos en internet, y más específicamente hablando de estafa informática, a simple vista parece que no es posible que este tipo de ataques o campañas delictivas continúen a pesar de toda la información que se tiene al respecto. Sin embargo, siguen desarrollándose amenazas más complejas cada día, puesto que el ciberdelincuente sabe que las técnicas funcionan por ello las van mejorando, porque su efectividad es probada.

- Tomando en cuenta lo anterior, se reflexiona a base del comportamiento que tienen las personas en la vida cotidiana, puesto que al parecer el mundo virtual, nubla o de alguna manera influye para que los usuarios no tomen los mismos resguardos, que en la vida real. En del caso, que las personas en lo cotidiano se preocupan de la seguridad, situación que cambia o no lo hacen en internet. Los usuarios comúnmente se informan respecto de los hechos delictivos, de cómo ocurren y cuáles son las causas, por ello, si las personas se preocupan de lo que ocurre en la vida real, igualmente debe existir la *información* acerca del mundo virtual y de todos los peligros que pueda haber en la red, con el fin de poder tener una reacción adecuada al momento de ser objeto de algún delito. Como podemos permitir que al momento de salir de nuestra casa, no *cerremos la puerta con llave*, por el contrario lo normal es que cada persona inmediatamente asegure su propiedad antes de salir, con candados, alarmas o sistemas de seguridad, con el fin de evitar que ingrese cualquier persona. En el

---

racionalizaciones y controles sobre los sistemas informáticos. Así como geográficamente han existido, y aún las hay, zonas más seguras y más peligrosas para el desplazamiento terrestre o marítimo, podrán desarrollarse, a nivel virtual, tales áreas diferenciadas, dependiendo de autocontrol o de controles externos, como sucede con la criminalidad en general. El espacio para estudiar la diversidad y la riqueza de la desviación podría expandirse, antes de contraerse debido a la estandarización. Nuevas identidades podrían manifestarse". GABALDÓN GERARDO, Luis, *Fraude electrónico y cultura corporativa*, Editorial Universidad Federal de Bahía, Mayo-Agosto, 2006, pág, 212. [accesible en], <www.redalyc.org/articulo.oa>.

mundo virtual, el ordenador es nuestra casa, y las llaves o candados son las contraseñas o claves de seguridad. Podemos decir entonces, que mientras más *complejas o mejor elaboradas sean nuestras contraseñas*, más llaves tendrán que abrir un delincuente informático, para realizar cualquier tipo de fraude.

Siguiendo con la idea anterior, podemos decir que la gente comúnmente *visita un médico,* tanto como para prevenir enfermedades, como para tratar las mismas. En el mundo virtual o digital, este parangón aplica de la misma manera, puesto que tal cual el cuerpo humano, los ordenadores y sus componentes son máquinas complejas, que funcionan de acuerdo una lógica y no en forma errática, por ello constantemente se debe analizar las máquinas que se usan donde se guarda la información que muchas veces es de relevancia, tanto económica como de afección, con el fin que funcionan en forma correcta, evitando con ello la infección de virus y la posibilidad que la información se pierda o ser víctima de un fraude. Del mismo modo, que en la vida real se evita andar o caminar por lugares desprovistos de luminosidad, o poco seguros, temiendo que algo suceda o ser víctima de algún posible delito, en internet sucede lo mismo. Se debe evitar ingresar a lugares desconocidos o sospechosos, no caer en alguna estafa, o abrir aplicaciones que pueden comprometer el ordenador tanto en la información que contiene, como los datos de seguridad que abren la posibilidad de ingresar tanto nuestro patrimonio, como el de otros, para ello antes de ingresar, en cualquier enlace que se nos ofrezca, se deben revisar el sitio al cual uno se dirige (protocolos HTTPS).

Por último, al continuar con estas recomendaciones existe un ejercicio que toda persona realiza antes de salir de su casa, esto es *mirarse al espejo,* dicho ejercicio tiene que ver no sólo con la apariencia, sino que está directamente relacionado, con la seguridad de antes de salir, es decir para verificar que se

lleva puesto, con el fin de no sentirse desprovisto de algo que falte, es decir si se trae todo consigo para salir sin inconvenientes de hogar. Análogamente en el mundo virtual, se puede quedar expuesto frente a desconocidos, que utilizan la información que las personas publican, por ello se debe tener especial cuidado, de todo lo que se sube a la red, porque esto es un espejo de nuestra vida, donde el delincuente informático estudia nuestras preferencias de privacidad, obteniendo con ello datos importantes para poder cometer un fraude.

Entonces, muchas de las cosas que se realizan a diario, se realizan también en un mundo virtual, por ello si se actúa de una manera determinada para resguardar nuestros bienes, propiedad o nuestra información, en la vida real, por llamarla de alguna manera de igual modo debe actuarse cuando se encuentra en el mundo llamado virtual, puesto que a pesar que la información digital no es algo que se pueda ver a simple vista, cuando se habla de información contenida en la red, o contenida en una nube, no por ello deja de ser real, y más aún deja de tener influencia o importancia en el mundo físico o más tangible, distinción que todas las personas tienen que tener en cuenta, al momento de ingresar a un sistema de procesamiento de datos, puesto que si no se toman los resguardos necesarios o se actúa con negligencia muchas veces van a ser víctimas de algún fraude.

De la misma forma, que no se puede erradicar la delincuencia la sociedad, toda vez que esto sería una utopía, siendo totalmente realistas es difícil que se mantenga los sistemas informáticos libre de virus, puesto que la cantidad de ellos y las técnicas aumentan cada día. Podría existir un sistema totalmente seguro, se podría crear existiendo una complejidad, y una vasta cantidad de certificados digitales, protegido por la comprobación de las firmas o claves al efecto, sin embargo ello no sería usado por los usuarios en general, toda vez que el mismo sistema con toda su seguridad sería muy poco amigable para

poder usarlo con normalidad, por ello es necesario una mancomunidad, entre la dogmática, el legislador ya su vez el conocimiento técnico de todos los operadores jurídicos involucrados para poder hacer frente a la delincuencia informática.

- En las últimas décadas años, la sociedad o el mundo entero ha sufrido un cambio sorprendente, esto es la instantáneadad de las comunicaciones, traspasando el flujo de información o conocimiento independientemente del lugar físico donde se encuentre el usuario, existiendo transferencias de información en tiempo real, existiendo hoy en día un gran número de empresas internacionales que se dedican a la transferencia de información, de datos de todo tipo, sonido e imágenes de además al comercio electrónico con el fin de abarcar mayor de clientes. Se dice que actualmente internet crece a razón de un 10% mensual, puesto que al nacer alguna organización que es el enlaza la red, también se tiene acceso a otras múltiples organizaciones, en un universo de decenas de millones de ordenadores interconectados, por ello aumenta de una manera exponencial, la cantidad de personas que están ideando alguna forma de cometer algún delito a través de esta red, fundamental es entonces la protección, y el desarrollo de la legislación en torno a la delincuencia informática. Conoce comete un delito, muchas veces se desconoce el motivo que tuvo el delincuente para realizar dicha acción, al ingresar un delincuente informático a nuestros sistemas, donde guardamos toda nuestra información y también nuestro patrimonio, se debe suponer de antemano que existe una mala intención, por ello si se recibe un reporte de algún ataque a redes informáticas, las intenciones casi siempre van hacer con el objeto de causar algún tipo de daño, como son la alteración de archivos, copia de información confidencial, reemplazo de software, para agregar puertas traseras o ingresar algún tipo de virus, debiendo las personas encargadas de mantener estos sistemas operativos,

pasar miles de horas intentando devolver la seguridad y confianza en los mismos.

- Los fraudes a través de medios informáticos a pesar que existe más conciencia de los delitos por parte los usuarios, han ido en aumento, los delincuentes siguen avanzando las técnicas recrear las estafas phishing, siendo más difíciles de diferenciar que los sitios que son reales o legítimos, aumentando la rentabilidad o ganancias que obtienen por la distintas modalidades del fraude phishing. De esta manera, la sofisticación técnica, va en aumento es así que se observan *malware*, más evolucionados que pueden ser utilizados con mayor potencial para causar daño, con los que se han creado para obtener información confidencial en particular, para autorizar el comercio en línea. Cuando se trató el tema del *spam*, se pudo analizar qué la prevención del mismo contribuye a la lucha contra el fraude informático, especialmente con la modalidad del *phishing*, puesto que los correos electrónicos que intentan atacar a los usuarios con esta modalidad, se valen del *spam*, para llegar a las personas, por ende los filtros de correo electrónico que se basan en listas de contenido, y mecanismos anti falsificación evitan que gran número correos electrónicos pueden llegar a las víctimas, sin embargo los *spammers*, continúan evolucionando para evitar dichas barreras. En la actualidad, el impacto financiero que esto conlleva y la sofisticación en el uso de los engaños técnicos en los correos dañinos.

- El tema en estudio nuevo, debe enfocarse desde el estudio científico del fenómeno delictual y ser analizado desde un punto de vista interno interdisciplinario, toda vez que contiene caracteres criminológicos y también de política criminal, todo lo cual va de la mano con la dogmática. Por ello, todo lo tratado debe estudiarse, analizando en profundidad el alcance de la criminalización a partir de estos nuevos delitos, recordando que la dogmática penal es fundamental para el entendimiento, y tratamiento específico de un tipo

de criminalidad naciente, como es la criminalidad informática. En cuanto la delincuencia informática, se ha ido mostrando cada vez, y en mayor medida como reflejo de una sociedad moderna que se caracteriza por la generación de riesgos que hace desaparecer al individuo del centro conflicto, se percibe una relación distinta entre ciudadanos y entidades inmateriales donde las personas desaparecen de la cúspide del problema. La regla generales aplicables a todas las infracciones de naturaleza penal, con el delincuente informático se han visto mermadas, puesto que existen limitaciones tanto a nivel legal, policial, jurisdiccional, respecto del tema. Si bien es cierto la delincuencia informática ha sido objeto de atención directa en todo el mundo, se ha abordado desde el punto de vista económico vinculando el alza de criminalidad con las condiciones económicas cambiantes de la sociedad. Sin embargo los operadores jurídicos deben no sólo tomar en cuenta, los factores económicos para determinar los volúmenes delincuencia son motivos, porque lo contrario sería un estudio parcial al momento de gestar una política criminal respecto de los delitos de carácter económico vinculados a la informática.

- En cuanto al delito de estafa básico en Chile mantiene su lineamiento clásico, en el sentido que se le sigue conceptualizando como un engaño suficiente que produce un error en una víctima logrando que ésta realice una disposición patrimonial perjudicial. Sin embargo se critica su falta de sistematicidad, en el sentido del lugar ubicado dentro del Código penal chileno, puesto que está dentro de los delitos contra la propiedad, siendo que su bien jurídico protegido es el patrimonio. En cuanto su elementos se discute respecto del ánimo de lucro, aunque la doctrina tradicional no lo exige, la jurisprudencia actual tiende a exigirlo, por su ubicación dentro de un mismo código y además también se discute acerca de la mentira como idónea para ser subsumidos en el tipo, cuando estamos hablando del elemento engaño, puesto que cuando se está

frente a ella la doctrina tradicional exige que sea algo más que una simple mentira, aunque hoy en día la doctrina no vacilan en admitirla como figura típica, abogando como justificación la necesidad igualdad ante la ley respecto del tratamiento punitivo.

En cuanto al fraude se trata, respecto de Chile, refiriéndonos a las conductas constitutivas de delincuencia informática y en especial al fraude informático a pesar del indicado anteriormente en el sentido que los autores indican que no existe legislación vigente para sancionar la estafa informática según la ley N° 19.223, que regula las figuras típicas relacionadas con la informática, estimo que puede ser sancionable con la figura de la estafa clásica, y por cierto la figura de la estafa calificada por el engaño, tomando los medios tecnológicos y adecuándolos a la figura básica, toda vez que el mismo o código se refiere a otros medios semejantes. Aunque estimo que es aplicable el tipo básico de estafa para el fraude informático, y aunque Chile fue pionero en Latinoamérica respecto de la promulgación de una ley que sanciona los delitos informáticos, hasta el día de hoy la legislación penal referente a esa materia no sido actualizada, existiendo dos proyectos en el parlamento que esperan ser aprobados para qué Chile pueda ponerse a la par de todos los países del mundo que han actualizado sus códigos punitivos o han creado leyes especiales para regular la materia, puesto que sólo Chile ha protegido la empresa, protegiendo los datos en sí mismo como parte integrante del sistema tratamiento información, dejando de lado al usuario los delitos informáticos.

- El legislador supranacional, optó por tomar la problemática de la criminalidad informática tomando en consideración las diversas repercusiones nacionales e internacionales de las conductas criminales, que hasta la fecha de las modificaciones del Código penal de 1995, eran abordadas en forma insuficiente o resultaban conductas atípicas, puesto que la realidad como se ha

dicho anteriormente superaba todas las expectativas toman en consideración el avance acelerado de las nuevas tecnologías. Por ello, cuando sesiona el Consejo de Europa, y establece una serie de directrices que tenían como propósito indicar a los estados miembros que tomen las cautelas necesarias y además pongan al día sus ordenamientos con el fin de mitigar el avance de las conductas criminales relacionadas con la información, en el ámbito de las nuevas tecnologías, de esta manera a través de la Decisión marco de 2001/413, y específicamente su artículo 8, se regula la llamada estafa informática, sin olvidar lo estudiado en el cuerpo esta tesis respecto a las críticas y reparos de la doctrina respecto a la redacción de dicho apartado. Al momento de legislar en forma interna, hubo distintas interpretaciones respecto de cómo tenía que incorporarse el delito en comentó, existiendo una brecha en la doctrina puesto que algunos indicaban que vivían existir conductas específicas respecto de las nuevas formas de criminalidad, y por otro lado se indicaba que tenía que ampliarse los tipos penales clásicos ya existentes, como es del caso en cuestión la estafa clásica o tradicional, servía de punto de partida para poder complementarla según sea necesario.

- Con respecto a la estafa informática el artículo 528 del código Penal anterior a 1995 establecía el delito de estafa el cual señalaba “el que con ánimo de lucro, utilizare engaño bastante para producir error en otro, induciéndole a realizar un acto de disposición en perjuicio propio o ajeno..." Así las cosas, se requería, para su configuración, la utilización de engaño bastante por el autor del delito y la producción de un error en la víctima del mismo. Al no existir una regulación específica, y con la necesidad de cubrir estos elementos impidió en mucha ocasiones por calificar un hecho como estafa cuando tenía lugar con la utilización de medios informáticos o cualquier otra forma relacionada con ellos. De esta manera es imposible subsumir la estafa realizada por una persona

con los utiliza un ordenador, por ejemplo cual se realizaba un delito de carácter informático tomando los datos de transferencia, realizando un traspaso de dinero a una cuenta que no era la del titular, existiendo ánimo de lucro y perjudicando a un tercero, no aparecían los elementos señalados en la antigua estafa, el engaño un tercero y el error bastante, todo lo cual se había realizado en el ordenador no pudiendo configurarse la producción del engaño en dicha máquina.

El legislador al incorporar nuevas figuras delictivas que tienen relación con aspectos tecnológicos o con las nuevas tecnologías que tienen que ver con la información, se ha ceñido con los esquemas dogmáticos tradicionales, completando figuras básicas o tradicionales para que haga alguna manera, se pueda atacar o frenar a la delincuencia informática, tal como ocurre con el artículo 248.2, donde la doctrina y la jurisprudencia lo han denominado como tipos de equivalencia, donde se ha ampliado a base de las figuras redituales existentes el tipo básico, como ocurre en el caso, de la estafa informática tratada en la tercera parte. Al analizar dicho artículo, nos encontramos que uno de los motivos que consideró el legislador, era la idea de sancionar conductas, que llevaban algún prejuicio para las entidades financieras o bancarias, puesto que se temía que los funcionarios de dichas entidades los conocimientos privilegiados pudieran manipular algunas transferencias bancarias, no teniendo como fin último regular lo que podía ocurrir con ordenadores y los fraudes cometidos con ellos o a través de ellos, surgiendo las críticas respecto de la forma en que puede operar la etapa clásica con sus elementos sobre el tipo de fraude informático ya legislado, toda vez que al hablar de máquinas no cabe el elemento intelectual o cognitivo puesto que no se puede engañar de acuerdo a los elementos clásicos a una máquina, naciendo entonces ideas o supuestos en que se utilizaban medios informáticos para estafar.

El presente artículo que regula las actuaciones delictivas en el ámbito informático con la estafa por este medio, el legislador incorporando elementos para nuevo tipo delictivo, a saber el ánimo de lucro; la acción típica, de valerse de una manipulación informática o artificio semejante, ya no existiendo engaño bastante y error; la transferencia de patrimonio en forma no consentida y por último perjuicio tercero, refiriéndose el ánimo de lucro cuando el sujeto actúa con la intención de enriquecerse a costa del patrimonio de otro. De esta manera tenemos un elemento diferenciador de la estafa clásica, cual es la transmisión patrimonial, puesto que en la materia en estudio, no se lleva a cabo por parte la víctima que está siendo engañada, sino que por el contrario el sujeto activo con las habilidades pertinentes, y los artificios tecnológicos puede y consigue, lograr la acción de transmisión patrimonial, por ende no tenemos la fase previa de engaño como la estafa clásica, el engaño y error están presentes de un modo indirecto, cumpliendo su fin el delincuente informático con la manipulación frente a una máquina, ya sea un ordenador o terminal bancaria, es decir de una primera lectura del artículo indicado, se puede apreciar una diferencia sustancial con el delito estafa tradicional o clásico, la disposición patrimonial propia del delito la acomete el propio sujeto activo y no la víctima. Esto tiene explicación, toda vez que el desarrollo de este tipo de delitos, que fueron introducidos por el artículo 248.2, da por sentado que engaño y error propios de la estafa tradicional, son elementos que tienen directa relación con la relación personal entre autor y víctima, algo que ya no sucede en la estafa informática puesto que se habla de manipulación informática o artificio semejante, de esta manera la disposición patrimonial realizada por el sujeto activo la lleva a cabo mediante lo indicado, obteniendo una transferencia no consentida.

En cuanto a la denominación o concepto de manipulación informática, se refiere a la conducta de alterar, modificar u ocultar datos informáticos de manera que, se realicen operaciones de forma incorrecta o que no se lleven a cabo, y también con la conducta de modificar la instrucciones del programa con el fin de alterar el resultado que se espera obtener. Con la manipulación, se realiza una transferencia no consentida donde una partida económica se desplaza del patrimonio del sujeto activo al de la víctima, dicho perjuicio afecta un tercero, ya que no en la propia víctima la que realiza la transferencia económica, sino el propio autor del delito. Vale señalar que no existe la comisión culposa, sino que el sujeto activo actúa siempre dolosamente, conociendo y queriendo realizar la acción delictiva, puesto que la manipulación informática lleva implícita en sí misma la intención fraudulenta de causar perjuicio en el patrimonio ajeno.

En el derecho comparado Alemania, con una orientación política criminal para combatir la delincuencia informática tuvo que legislar para poder llenar la Laguna legal existían, es creándose con ello la segunda ley tratada anteriormente denominada de lucha contra la criminalidad económica de 1986, y que no sólo modificó lo ya existente sino que también introdujo nuevos tipos penales que se hacen cargo de la delincuencia informática propiamente tal, entre ellos el espionaje de datos, la estafa mediante ordenador o fraude informático, y falsificación de datos probatorios, con ello dicho país comenzó controlar la materia en este caso.

La velocidad, con qué evolución en los sistemas técnicos pone a prueba la protección de los cibernautas, tomando una relevancia de tal magnitud el factor humano en la vulnerabilidad, de todo movimiento que se realizan en internet especialmente cuando se trata de transferencia de algún tipo de valor, por ello los estafadores ya no necesitan tantos conocimientos informáticos especiales

para poder llevar a cabo estos delitos, pues hoy en día cualquier ordenador es una herramienta a la cual puede acceder cualquier persona, sin embargo el código penal español se hace cargo de una manera satisfactoria en soportado a) del artículo 248.2 resolviendo entonces la estafa cometida mediante manipulación informática. Vale hacer presente, que las distintas legislaciones mundiales se está haciendo frente a la delincuencia informática creando tipos penales, en relación a las distintas figuras de rituales que van apareciendo en el medio de internet, sin embargo la doctrina muchas veces ha criticado la manera como el legislador toma en consideración el principio de legalidad, que da sustento a otras garantías individuales de carácter procesal, de esta manera el legislador debe identificar los bienes fundamentales que deben ser protegidos para la sociedad, y con ello considerarse ciertas conductas son perjudiciales realizando el ejercicio de abstracción para crear tipos penales, por ello al tomar en cuenta ciertas redacciones de tipos penales en cuanto a la materia se trata, quedan muchas veces preceptos generales que llevan al juzgador a tener problemas al momento de aplicarlos[576]. De acuerdo a lo anterior se estima que el Derecho penal no debe ampliarse, sino que a medida que se van legislando tomando en consideración la nueva forma delictual informática, debe mejorarse de acuerdo a la realidad social que va cambiando constantemente llevando legislador a crear tipos penales que sean estrictamente necesarios ya la ves que lleven al juzgador a una interpretación adecuada de las normas que se le entregan para aplicar al caso en particular, por ende cada vez que exista la necesidad de una modificación legal deben tomarse en consideración la opinión de la doctrina, y la jurisprudencia que va cada día aplicando el derecho a la nueva forma de criminalida

[576] FERRAJOLI, Luigi, *Derecho y Razón, Teoría del garantismo penal*, Editorial Trotta, Madrid, 1995, pág., 95.

BIBLIOGRAFÍA

Doctrina:

- A. PARDINI, Aníbal, *Derecho de internet*, Editorial La Roca, Buenos Aires, Argentina, 2002.
- ABOSO, Gustavo / ZAPATA María, *Cibercriminalidad y Derecho penal*, 1ª edición, Editorial B de F, Buenos Aires Argentina, 2006.
- ADÁN DEL RIO, Carmen, *La persecución y sanción de los delitos informáticos*, En revista Española Eguzkilore, Número 20, San Sebastián, 2006.
- ALASTUEY DOBÓN, Mª Carmen, *Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial*, Informática y Derecho (director) CARRASCOSA LÓPEZ, Valentín, Área De Derecho Penal, Facultad De Derecho De La Universidad Zaragoza, Editorial Aranzadi, España, 1994.
- ÁLVAREZ CARO, María, *Derecho al olvido en internet, el nuevo paradigma de la privacidad en la era digital*, Editorial Reus, Madrid, 2015.
- ÁLVAREZ CIENFUEGOS, José, *Informática y derecho penal. Los delitos relativos a la informática*, 1ª Edición, Editorial Ministerio de Justicia, Secretaría técnica, Centro de publicaciones, Madrid, 1996.
- ÁLVAREZ FORTTE, Héctor, *Los delitos informáticos*, Corpus Iuris, Revista jurídica regional N° 9, Chile, 2009.

- ÁLVAREZ VIZCAYA, Maite, *Consideraciones político criminales sobre la delincuencia informática, el papel del Derecho penal en la red, en internet y Derecho penal*, Cuadernos de Derecho Judicial, CGPJ, N° 10, 2001.
- ALTMARK, Daniel, *Informática y derecho aportes de doctrina internacional*, Vol. I y II, Editorial Depalma, Buenos Aires, Argentina, 1988.
- AMUCHATEGUI REQUENA, Griselda, *Derecho Penal*, Tercera Edición, Oxford, México, 2005.
- ANDRÉS VASCONCELOS, Jorge, *Informática II, Sistemas de información*, 1ª edición, Editorial Publicaciones Cultural, México, 2002.
- ANARTE BORRALLO, Enrique, *Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información,* Derecho y conocimiento, Vol. 1, facultad de derecho, de la Universidad de Huelva, España, 2001.
- ANGUITA RAMÍREZ, Pedro, *Acciones de protección contra google*, Editorial Librotecnia, Santiago de Chile, 2016.
- ANTÓN ONECA, José, *Estafas*, Mascareñas, Calos E. (dir.), *Nueva Enciclopedia Jurídica*, tomo IX, Editorial Francisco Seix, Barcelona, 1958.
- AZPILCUETA, Hermilio, *Derecho informático*, Editorial Abeledo- Perrot, Buenos Aires, Argentina, 1987.
- BACIGALUPO SAGGESE, Silvina / CANCIO MELIÁ, Manuel (coords.), *Derecho penal y política transnacional*, Editorial Atelier, 1ª edición, Barcelona, 2005.
- BACIGALUPO ZAPATER, Enrique, *Derecho penal, Parte general*, Editorial Hammurabi, 2ª edición, 1999.

- BACIGALUPO ZAPATER, Enrique, *Utilización abusiva de cajeros automáticos por terceros no autorizados*, Poder Judicial núm. Especial IX, CGPJ.

- BAJO FERNÁNDEZ, Miguel, / PÉREZ MANZANO, Mercedes / SUÁREZ GONZÁLEZ, Carlos, *Manual de Derecho penal, Parte especial, Delitos patrimoniales y económicos*, 2ª Edición, Editorial Centro estudios Ramón Areces, Madrid, 1993.

- BAJO FERNÁNDEZ, Miguel, *Los delitos de estafa del Código penal*, Editorial Universitaria Ramón Areces, Madrid, 2004.

- BAJO FERNÁNDEZ, Miguel, *Compendio de Derecho penal, Parte Especial*, volumen I, Editorial Centro de Estudios Ramón Areces, 1ª edición, Madrid, 1998.

- BALMACEDA HOYOS, Gustavo, *El delito de estafa informática*, Editorial Jurídicas de Santiago, Chile, 2009.

- BALMACEDA HOYOS, Gustavo, Revista de derecho y ciencias penales número 17, Universidad San Sebastián, *El delito de estafa informática en el Derecho Europeo Continental*, Chile, 2011.

- BALMACEDA HOYOS, Gustavo, *El delito de estafa, una necesaria normativizados y de sus elementos típicos*, Revista estudios socio-jurídicos, 13, U. de los Andes Chile, 2011.

- BAÓN RAMÍREZ, R, *Visión general de la informática en el nuevo Código Penal*, en Cuadernos de derecho judicial, 11, Barcelona, 1996.

- BARROS V. Oscar, *Ingeniería e-business ingeniería de negocios para la economía digital*, Editorial Lom S. A. Santiago de Chile, 2004.

- BARROS, Óscar, *Tecnologías de la información y su uso en gestión*, Editorial McGraw Hill, Santiago, 1998.

- BESIO HERNÁNDEZ, Martin, *Los criterios legales y judiciales de individualización de la pena*, Editorial Tirant Lo Blanch, Valencia, 2011.

- BARRIO ANDRÉS, Moisés. *El régimen jurídico de los delitos cometidos en internet en el derecho español tras la reforma penal de 2010, En Delincuencia informática, Tiempos de cautela y amparo,* Editorial Thomson Reuters Aranzadi, Navarra, 2012.

- BRIZZIO, Claudia R, *La informática en el nuevo derecho,* Editorial Abeledo-Perrot, Buenos Aires, Argentina, 2005.

- BULLEMMORE GALLARDO, Vivían, *Curso Derecho penal, Parte especial*, tomo IV, 2ª edición, Editorial LexisNexis, Santiago de Chile, 2007.

- BUSTOS RAMÍREZ, Juan, *Obras completas, Derecho penal, Parte general* tomo II, Editorial Ara, Santiago de Chile, 2005.

- BUSTOS RAMÍREZ, Juan, *Manual de Derecho penal, Parte especial,* 2ª edición, Editorial Ariel, Barcelona, 1991.

- BUSTOS RAMÍREZ, Juan / HORMAZÁBAL MALARÉE, Hernán, *Lecciones de Derecho penal, Parte general,* Editorial Trotta, Madrid, 2006.

- CÁCERES, NIETO, Enrique, *Lógica jurídica e información jurídica*, Revista de la facultad de Derecho Universidad Complutense, informática y derecho, monográfico 12, Madrid.

- CAICEDO, Fernando, / RIVERA LLANO Abelardo / PÉREZ LUÑO, Antonio, *Curso de informática jurídica*, Editorial Tecnos, Bogotá, 1998.

- CAMACHO LOSA, Luis, *El delito informático*, Editorial Madrid, 1ª edición, Madrid, 1987.

- CÁMPOLI KESSLER, Gabriel, *Principios de Derecho penal, Informático*, Editorial Ángel, México, 2004.

- CARBONELL MATEU, J / GONZÁLEZ CHUSCA, J, *Delitos contra la intimidad, el derecho a la imagen y la inviolabilidad del domicilio*, (coordinador), VIVES ANTÓN, Tomás, *Comentarios al Código Penal de 1995*, Editorial Tirant lo Blanch, Valencia, 1996.

- CASTELLS, M, *La galaxia, reflexiones sobre Internet, empresa y sociedad*, Editorial Areté, Barcelona, 2001.

- CASTRO SÁENZ, Alfonso, *Sobre la legitimación del Derecho penal del riesgo*, Editorial Bosch Penal, Sevilla, 2014.

- CHOCLÁN MONTALVO, José *El delito de estafa*, Editorial Boch, 1ª edición, Barcelona, 2000.

- CHOCLAN MONTALVO, José Antonio, *Fraude informático y estafa por computación, en internet y Derecho penal*, Cuadernos de Derecho Judicial, Escuela Judicial, X-2001, Consejo General del Poder Judicial, Madrid, 2001.

- CHOCLÁN MONTALVO, José, *Delincuencia Informática, Problemas de responsabilidad, Infracciones patrimoniales en los procesos de transferencia de datos*, (director) MORALES GARCÍA, Oscar, Cuadernos de Derecho Judicial IX-2002, Consejo General del Poder Judicial, Madrid, 2002.

- CHOCLAN MONTALVO, José Antonio, *Estafa por computador y criminalidad económica vinculada a la informática*, Revista actualidad penal, número 47, Trabajo que corresponde, en síntesis, con el texto de la conferencia pronunciada el día 15 agosto de 1997 con el título *Delitos patrimoniales cometidos con medios o procedimientos informáticos*, En los Cursos de

Verano de El Escorial, de la Fundación General de la Universidad Compútense. Madrid, 1997.

- COLINA RAMÍREZ, Edgar, *Sobre la legitimación del Derecho penal del riesgo*, Editorial Boch, Sevilla, 2014.
- CORCOY, Mirentxu / JOSHI, Ujala, *Delitos contra el patrimonio cometidos por medios informáticos*, En revista jurídica Catalunya, vol. 87 N° 3, 1988.
- CONTRERAS TORRES, Raúl, *El delito de Estafa*, Editorial Jurídica Conosur Ltda., Santiago, Chile, 1992.
- CORCOY BIDASOLO, Mirentxu, *Manual práctico de Derecho penal, Parte especial*, Doctrina y jurisprudencia, con casos solucionados, 2ª edición, Editorial Tirant lo Blanch, Valencia, 2004.
- COUTURE ETCHEVERRY, Eduardo, *Vocabulario jurídico*, 4° edición, Editorial Desalma, Buenos Aires, Argentina, 1991.
- CRESPI, Alberto, / STELLA, Federico / ZUCCALA, Giuseppe, *Comentario breve al Códice penale*, Milan, Editorial Cedan, Milano, 2003.
- CONDE PUMPIDO, Cándido, *Estafas*, Editorial Tirant lo blanch, Valencia, 1997.
- CRUZ DE PABLO, José, *Derecho penal y nuevas tecnologías, aspectos sustantivos*, Editorial Grupo Difusión, 1ª edición, Madrid, 2006.
- CORREA, Carlos, Derecho informático, Editorial Desalma, Buenos Aires, Argentina, 1999.
- CUELLO CALÓN, Eugenio, *Derecho penal, Parte especial*, tomo II, revisado puesta al día, por César CAMARGO HERNÁNDEZ, vol. 2, 14ª Edición, Editorial Boch, S.A., Barcelona, 1980.

- CURY URZÚA, Enrique, *Derecho penal, Parte general*, 10ª Edición, Editorial Universidad Católica de Chile, 2011.

- DAVARA RODRÍGUEZ, Miguel, *Manual de Derecho informático*, Editorial Thomson Aranzadi, 7ª Edición, Navarra, 2005.

- DAVIS, Martin, *Universal computer, The road from Leibniz to Turing*, Editorial W.W. Norton & Company, 1ª edición, Nueva York, 2000.

- DE PINA, RAFAEL / DE PINA DE VARA, Rafael, *Diccionario de Derecho*, 31ª Edición, Editorial Porrúa, México, 2003.

- DE URBANO CASTRILLO, Eduardo, *Delincuencia informática, tiempos de cautela y amparo, Las estafas*, Capitulo X, 1ª Edición, Editorial Aranzadi, Pamplona, 2012.

- DUNHAM, Ken / MELNICK, Jim, *Malicious Bots, An Inside Look into the Cyber-criminal Underground of the internet*, Editorial Taylor& Francis Group, Nueva York, 2009.

- ERDOZAIN, José Carlos, *Derechos de autor y propiedad intelectual en internet*, Editorial Tecnos, Madrid, 2002.

- ETCHEBERRY ORTHUSTEGUY Alfredo, *Delitos contra la esfera de intimidad*, *Derecho penal, Parte especial*, Editorial Jurídica de Chile, 3ª edición, Santiago de Chile, 1998.

- ETCHEBERRY ORTHUSTEGUY, Alfredo, *Derecho penal, Parte especial*, 3ª edición, Editorial jurídica de Chile, 1999.

- ETCHEVERRY ORTHUSTEGUY, Alfredo, *Derecho penal en la jurisprudencia*, tomo III, 3ª Edición, Editorial Jurídica de Chile, Santiago, 1987.

- BAJO FERNÁNDEZ, Miguel, *Los delitos de estafa en el Código penal,* Editorial Universitaria Ramón Areces, Madrid, 2004.

- FARALDO CABANA, Patricia, *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Editorial Tirant Lo Blanch, Valencia, 2009.

- FARALDO CABANA, Patricia, *Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática*, En Eguzkilore Cuaderno del Instituto Vasco de Criminología, número 21, 2007.

- FEIJOO SÁNCHEZ, Bernardo, *Imputación objetiva en Derecho penal*, Publicación del Instituto peruano de ciencias penales, Editorial Grijley, Lima, 2002.

- FERNÁNDEZ TERUELO, Javier, *Derecho penal e internet*, Editorial, Lex Nova, España, 2011.

- FERNÁNDEZ TERUELO, Javier, *Cibercrimen en los delitos cometidos a través de internet*, Editorial Constitutio Criminalis Carolina, Oviedo, 2007.

- FERNANDEZ DÍAZ, Álvaro, *Engaño víctima en la estafa,* Revista de derecho de la Pontificia Universidad católica de Valparaíso XXVI, Semestre I, Valparaíso, 2005.

- FERRAJOLI, Luigi, *Derecho y Razón, Teoría del garantismo penal*, Editorial Trotta, Madrid, 1995.

- FISCHER, Royal P, *Seguridad en los sistemas informáticos*, Editorial Díaz Santos, S. A., Madrid, 1988,

- FLORES PRADA, Ignacio, *Criminalidad informática aspectos sustantivos y procesales*, Editorial Tirant Lo Blanch, Valencia, 2012.

- FROSINI , Vittorio, *Informática y derecho*, Editorial Temis, Bogotá, 1988.
- GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos, análisis del artículo 248.2 Código penal,* Editorial Tirant Lo Blanch, Valencia, 2005.
- GARCÍA MEXÍA, Pablo, *Principios de derecho internet*, 2ª edición, Editorial Tirant lo Blanch, Valencia, España, 2005.
- GARCÍA SERVIGÓN, Josefina, *El fraude informático en España e Italia. Tratamiento jurídico penal y criminológicos*, En revista cuatrimestral de las facultades de derecho y ciencias económicas y empresariales, Número 74, España, 2008.
- GARCÍA ARÁN, Mercedes, *Constitución y Derecho penal, veinte años después*, Ediciones Universidad de Salamanca, Cuenca, 2001.
- GARCÍA ESPAÑA, Elisa / DÍEZ RIPOLLÉS, José / PÉREZ JIMÉNEZ, Fátima / BENÍTEZ JIMÉNEZ, María / CEREZO DOMÍNGUEZ, Ana, *Evolución de la delincuencia en España: Análisis longitudinal con encuestas de victimización*, En revista española, de investigación criminológica, núm. 8, Instituto Andaluz de Criminología, Universidad de Málaga, 2010.
- GARCÍA-PABLOS MOLINA, Antonio, *Informática y Derecho penal*, en Implicancias socio-jurídicas de las tecnologías de la información, Editorial Citema, Madrid, 1984.
- GARRIDO MONTT, Mario, *Derecho penal, Parte general*, tomo I, 2ª Edición, Editorial Jurídica de Chile, 2007.
- GONZÁLEZ RUS, Juan, *Nueva forma de delincuencia, Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos*

informáticos, Número especial IX, Consejo General del Poder Judicial, Madrid, 1988.

- GONZÁLEZ RUS, Juan, *Protección penal de sistemas, elementos, datos, documentos y programas informáticos*, En revista electrónica de ciencia penal y criminología, número 1-14, Córdoba, 1999.
- GONZÁLEZ RUS, Juan, *El cracking y otros supuestos de sabotaje informático* en Estudios Jurídicos Ministerio Fiscal, número 2, 2003.
- GONZÁLEZ RUS, *Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (artículo 264.2 del Código Penal)*, En la ciencia del derecho penal ante el nuevo siglo, 1ª edición, Editorial Tecnos, Madrid, 2003.
- GONZÁLEZ EXTREMERA, Josep, *La estafa mediante título mercantil abstracto*, Editorial Metropolitana, Santiago de Chile, 2008.
- GUDÍN RODRÍGUEZ-MAGARIÑOS, Faustino, *La lucha contra el ciberblanqueo como vía para acabar con el phishing*, En revista Aranzadi Doctrinal, número extra 9-10, 2014.
- GUTIÉRREZ FRANCÉS, María Luz, *Fraude informático y estafa*, 1ª Edición, Editorial Ministerio de Justicia, Secretaría técnica, Centro de publicaciones, Madrid, 1996.
- GUTIÉRREZ FRANCÉS, María luz, *Los fraudes informáticos en el nuevo Código penal*, Departamento de justicia al centro de estudios jurídicos y formación esp ecializada, Cataluña, 1996.
- GUTIÉRREZ FRANCÉS, María Luz, *Reflexiones sobre la ciberdelincuencia hoy. En torno a la ley penal en el espacio virtual*, En Revista electrónica del departamento de derecho de la Universidad de La Rioja, REDUR, número 3, 2005.

- GUTIÉRREZ FRANCÉS, María luz, *Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa*, En MAZUELOS COELLO, Julio, *Derecho Penal Económico y de la Empresa*, Editorial San Marcos, Lima, 2014.

- H. SANDERS, Donald, *Informática, Presente y futuro*, Editorial, Mc Graw Hill. México, 1987.

- HANCE, Oliver, *Leyes y negocios en la Internet, origen de la internet*, Editorial McGraw- Hill, México, 1996.

- HERRERA BRAVO, Rodolfo / NÚÑEZ ROMERO, Alejandra, *Derecho informático*, Ediciones Jurídicas la Ley, Santiago, 1999.

- HERRERA MORENO, Mirian, *El fraude informático en el derecho penal español*, Revista de Actualidad Penal, número 39, Sevilla, 2001.

- HUERTA MIRADA, Marcelo / LÍBANO MANSSUR, Claudio, *Delitos Informáticos*, Editorial Jurídica Conos Sur, 2ª edición, 1998.

- JAKOBS, GÜNTHER, *Derecho penal, Parte general, fundamentos y teoría de la imputación*, imputación (trad. Joaquín CUELLO CONTRERAS y José Luis SERRANO GONZÁLEZ DE MURILLO). 2ª edición corregida, Editorial, Marcial Pons, Madrid, 1997.

- JAKOBS, GÜNTHER / POLAINO NAVARRETE, Miguel / POLAINO ORTS, Miguel, *Bien jurídico, vigencia de la norma y daño social*, 1ª Edición, Editorial Ara, Perú. 2010.

- JIJENA LEIVA, Renato, *Delitos Informáticos, Internet y Derecho*, En delito, pena y proceso: Libro en homenaje a la memoria del profesor SOLARÍ PERALTA, Pontificia Universidad Católica de Valparaíso Facultad de

Derecho, (coordinador) RODRÍGUEZ COLLAO, Luis, Editorial Jurídica de Chile, 2008.

- JUDEL PRIETO, Ángel / PIÑOL RODRÍGUEZ, José, *Manual de Derecho penal, Parte general,* tomo I, 5ª Edición, Editorial Thomson Reuters Civitas, 2008.

- LABATUT GLENA, Gustavo / ZENTENO VARGAS, Julio, *Derecho Penal, Parte Especial*, tomo II, Santiago, Editorial Jurídica de Chile, 1996.

- LESSIG, Lawrence, *El Código y otras leyes del ciberespacio*, Editorial Grupo Santillana, Madrid, 2001.

- LAMAS PUCCIO, Luis, *Una aproximación a la teoría de la imputación objetiva, En cuestiones actuales de Derecho penal y Procesal penal*, 1ª edición, Editorial E&J Graff, Perú, 2013.

- LARA PEINADO, Federico, *Código de Hammurabí, estudio preliminar, traducción y comentarios,* 2ª Edición, Editorial Tecnos, Madrid, 1986.

- LATTANZI, Giorgio / LUPO, Ernesto, *Codice penale rassegna delito informático geieurisprudenza e di doctrina*, Volumen I, Editorial Anno di, Giuffre Milano, 2015.

- LEVIN B, Richard, *Virus informáticos*, Editorial, McGraw-Hill, México, 1992.

- LIMA MALVIDO, María de la Luz, *El delito electrónico*, Editorial Ariel, México, 1999.

- MAGALLÓN SANZ, José María, *Sociedad del conocimiento*, En revista de política, cultura y arte, Número 070, Madrid. Julio 2000.

- MAGLIONA MARKOVICTH, Claudio, *Análisis de la normativa sobre delincuencia informática en Chile, Derecho y Tecnologías de la Información*,

Fundación Fernando Fueyo Laneri y Escuela de Derecho Universidad Diego Portales, Chile, 2002.

- MAGLIONA Claudio / LÓPEZ, Macarena, *Delincuencia y fraude informático*, Editorial jurídica de Chile, Santiago, 2010.

- MANZINI VICENZO, *Tratado de derecho penal, Parte Especial,* Editorial del foro, Buenos Aires, Argentina, 1996.

- MARCHILI, Luis Alberto, *Como legislar con sabiduría y elocuencia, el arte de legislar reconstruido a partir de la tradición retórica,* Editorial Dunken, Buenos Aires, Argentina, 2009.

- MATA Y MARTÍN, Ricardo, *Delincuencia informática y Derecho penal*, Editorial Edisofer, Madrid, 2001.

- MATA Y MARTÍN, Ricardo, *Criminalidad informática: una introducción al cibercrimen*, En revista de actualidad Penal, número 37, (trabajo que forma parte del desarrollo del proyecto de investigación de la junta de Castilla y León, sobre Protección penal del consumidor en el comercio electrónico), 2003.

- MATA Y MARTÍN, Ricardo, *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago*, Editorial Edisofer Navarra, 2007.

- MATELLANES RODRÍGUEZ, Nuria, *Algunas notas sobre las formas de delincuencia informática en el Código pena*l, DÍAZ-SANTOS Diego/ SÁNCHEZ LÓPEZ, Virginia (coordinadores), *Hacia un Derecho penal sin fronteras*, Editorial Colex, 1ª edición, Madrid, 2000.

- MATELLANES RODRÍGUEZ, Nuria, *Algunas razones para la represión penal autónoma del intrusismo informático, Derecho Penal y Criminología*, 2005.

- MATEOS MUÑOZ, Agustín, *Compendio de etimologías greco-latinas del español*, Editorial Esfinge, Cuadragésima sexta edición, México, 2007.

- MAZUELOS COELLO, Julio, *Modelos de imputación en el Derecho penal informático,* En revista de Derecho Penal y criminología, Vol. 28, número 85, U. de Externado Colombia, 2007.

- MENÉNDEZ MATO, Juan / GAYO SANTA, Cecilia, María Eugenia, *Derecho e informática*. Editorial Bosch, 2014.

- MEZGER, Edmund, *Derecho penal, Parte especial, libro de estudio*, Traducción de la 4ª Edición alemana de 1954, traducida por el Dr. CONRADO A, Finzi, Traductor del Instituto de Derecho Penal de la facultad de derecho y ciencias sociales de Córdoba, Editorial bibliográfica Argentina, Buenos Aires, Argentina, 1959.

- MIR PUIG, Santiago, *Derecho penal, Parte general,* 9ª edición, Editorial Reppertor, Barcelona, 2011.

- MIR PUIG, Santiago, *Bien jurídico y bien jurídico-penal como límites del ius puniendi, en El Derecho penal en el Estado social y democrático de Derecho*, Barcelona, 1994.

- MIR PUIG, Santiago (director), PASTOR MUÑOZ, Nuria, *Comentarios a la jurisprudencia el Tribunal Supremo, Engaños punibles e mentiras impunes: un análisis de los límites del engaño típico en el delito estafa a la luz del caso de la sentencia del Tribunal Supremo de 18 de julio de 2003,* Anuario de Derecho penal y Ciencias penales, vol. LVI, 2003 Sección de jurisprudencia, Universidad Pompeu Fabra, Barcelona.

- MOLINA BLÁZQUEZ, Concepción, *La aplicación de la pena*, 2° edición, Editorial Boscn, Madrid, 1998.

- MORALES RÍOS, Hernando, *Enseñanza de derecho informático y condiciones objetivas*, Editorial Crei, Madrid, 1989.

- MORÓN LERMA, Esther, *Internet y derecho penal: hacking y otras conductas ilícitas en la red*, Editorial Aranzadi, Pamplona, 1999.

- MORÓN LERMA, Esther, *Internet y derecho penal: hacking y otras conductas ilícitas en la red*, 2ª edición ampliada, Editorial Aranzadi, Navarra, 2002.

- MUÑOZ TORRES, Ivonne, *Delitos informáticos, diez años después*, 1ª edición, Editorial Ubijus, México, 2009.

- BEGROPONTE, Nicholas, Ser Digital, Editorial Atlántida, Buenas Aires, Argentina, 1995.

- NANDO, LEFORT, Víctor, *El lavado de dinero, nuevo problema para el campo jurídico*, 2ª edición Editorial Trillas, México, 1999.

- NAVA GARCÉS, Enrique, *Análisis de los delitos informáticos*, Editorial Ed Porrua, México, 2005.

- NORA, Simón / Alain, MINC, *La informatización de la sociedad*, Fondo de Cultura Económica, México, 1982.

- NOVOA MONREAL, Eduardo, *Curso de Derecho Penal Chileno*, tomo II, Editorial Jurídica de Chile, Santiago de Chile, 1992.

- OLIVERA, Noemí, *El sistema jurídico de la sociedad de la información procesos y tendencias*, En la sociedad de la información en Iberoamérica. (coordinadora) ARELLANO TOLEDO, Wilma, Editorial INFOTEC, 1ª edición, México, 2012.

- ORTIZ PRADILLO, Juan, *Problemas procesales de la ciberdelincuencia.* Editorial Colex, Madrid, 2013.

- ORTS BERENGUER, Enrique / ROIG TORRES, Margarita, *Delitos informáticos y delitos comunes cometidos a través de la informática*, Editorial Tirant lo blanch, Valencia, 2001.

- PALAZZI, Pablo Andrés, *Delitos Informáticos*, Editorial Ad-Hoc, Buenos Aires, Argentina, 2000.

- PASTOR MUÑOZ, Nuria, *La determinación del engaño típico en el delito estafa*, Editorial Marcial Pons, Madrid, 2004.

- PÉREZ MANZANO, Mercedes, *Acerca de la imputación objetiva de la estafa, Hacia un Derecho penal económico europeo*, Jornadas en honor del profesor Klaus TIEMANN, Estudios jurídicos, Serie Derecho público, Boletín oficial del Estado, Madrid, 1995.

- PÉREZ MANZANO, Mercedes, *Las defraudaciones, Las Estafas*, en Compendio de Derecho penal. Parte especial, Vol. II, Miguel BAJO FERNÁNDEZ (dir.), Editorial Centro de Estudios Ramón Areces, Madrid, 1998.

- PÉREZ LUÑO, Antonio, *Ensayos de Informática Jurídica*, Editorial Biblioteca de Ética, Filosofía del Derecho y Política, México, 1996.

- PINOCHET CANTWELL, Francisco, *Los principios especiales del derecho de internet*, Editorial El Jurista, Santiago de Chile, 2015.

- PIÑA ROCHEFORT, Juan, *Fraude de seguros, cuestiones penales y de técnica legislativa*, Santiago, Editorial Jurídica de Chile, 2006.

- POLAINO NAVARRETE, Miguel, *Derecho Penal, Parte General, fundamentos científicos del derecho penal*, tomo I, 6ª edición actualizada, complementada renovada y puesta al día por POLAINO-ORTS Miguel, Editorial Bosch, S. A., 2008.

- POLAINO NAVARRETE, Miguel, *Lecciones de Derecho penal, Parte general*, tomo II, Editorial Tecnos en Madrid, 2013.

- POLAINO NAVARRETE, Miguel, *Derecho penal, Parte general*, tomo II, vol. I, Editorial Bosch, Barcelona, 2008.

- POLAINO NAVARRETE, Miguel, *Los delitos contra la propiedad intelectual en la reforma Penal española*, en ECHEBURÚA ODRIOZOLA, ARZAMENDI, JOSÉ LUIS Y DENDALUCE SEGUROLA, Iñaki (coords.), *Criminología y Derecho penal al servicio de la persona, Homenaje al Profesor Antonio Beristain, San Sebastián*, Instituto Vasco de Criminología, 1989.

- POLAINO NAVARRETE, *Miguel, El injusto típico en la teoría del delito*, Editorial Mario A. Viera Editor, Corrientes, 2000.

- POLAINO NAVARRETE, Miguel / POLAINO-ORTS, Miguel, *Niveles de intervención delictiva: un problema de imputación objetiva*, en Claus ROXIN / Miguel POLAINO NAVARRETE / Miguel POLAINO-ORTS, *Política criminal y dogmática penal. Cuestiones fundamentales*, ARA Editores E.I.R.L., Lima, 2013.

- POLAINO NAVARRETE, Miguel, *Protección de bienes jurídicos y confirmación de la vigencia de la norma: ¿dos funciones excluyentes?*, En Günther JAKOBS / Miguel POLAINO NAVARRETE / Miguel POLAINO-ORTS, *Bien jurídico, vigencia de la norma y daño social*, ARA Editores E.I.R.L., Lima, 2010.

- POLAINO-ORTS, Miguel, *Funcionalismo normativo. Bases dogmáticas para el nuevo Sistema de Justicia Penal, Fundamentos y función del Derecho penal*, Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas, México. D.F., 2014.

- POLAINO-ORTS, Miguel, *Las cuatro caras de la imputación penal. Acotaciones críticas al concepto kantiano de imputación desde una perspectiva funcionalista*, En Fernando MIRÓ LLINARES / Miguel POLAINO-ORTS, *La imputación penal a debate. Una confrontación entre la doctrina de la imputación kantiana y la imputación objetiva en Jakobs*, ARA Editores E.I.R.L., Lima, 2010.

- POLITOFF LIFSCHITZ, Sergio / MATUS Jean Pierre / RAMÍREZ María Cecilia, *Lecciones de Derecho Penal Chileno*, Editorial Jurídica de Chile, 2004.

- POLITOFF LIFSCHITZ, Sergio, *Texto y Comentario del Código Penal Chileno*, tomo I, Editorial Jurídica de Chile, 2002.

- PINOCHET CANTWELL, Francisco, *Los principios especiales del derecho en internet*, Editorial el jurista, Santiago de Chile, 2015.

- PRADA FLORES, Ignacio, *Criminalidad informática, aspectos sustantivos y procesales*, Editorial Tirant lo blanch, Valencia, 2012.

- PRIETO ESPINOSA, Alberto, *Introducción a la informática*, 3ª edición, Editorial Mc Graw Hill, España, 2002.

- QUINTANO RIPOLLÉS, Antonio, *Tratados de Parte especial del Derecho penal, infracciones patrimoniales de apoderamiento*, tomo II, 2ª edición puesta al día por Carlos GARCÍA VALDÉS, profesor de Derecho Penal de la Universidad Salamanca, Editorial Revista de Derecho Privado, Madrid, España 1977.

- QUINTANO RIPOLLÉS, Antonio, *Tratado de la Parte especial de Derecho penal*, tomo III, Editorial Revista Derecho Privado, 2ª edición, Madrid, 1978.

- REY HUIDOBRO, Luis Fernando, *La estafa informática: relevancia penal del phishing y el pharming*, En La ley Penal, revista de Derecho penal, procesal y penitenciario, número 101, 2013.
- RIBAS, Javier Alejandro, *Aspectos jurídicos del comercio electrónico en internet*, Editorial Aranzadi, Pamplona, 1999.
- ROJAS AGUIRRE, Luis, *Lo subjetivo en el juicio de imputación objetiva: ¿aporía teórica?*, En revista de derecho U. A. Chile, Vol. XXIII número 1°, 2010.
- RINCÓN, Antonio / PLAGARIO, Julio M, *Diccionario conceptual de informática y comunicaciones*, Editorial Paraninfo, Madrid, 1998.
- ROJAS AMANDI, Víctor, *El uso Internet en el derecho*, 1ª Edición, Editorial Oxford, México, 2001.
- RODRÍGUEZ VILLASEÑOR, Isabel / GÓMEZ GARCÍA, Juan, *Investigación y documentación jurídicas*, 2ª edición, Editorial Dykinson, Madrid, 2013, pág. 53 y sigs.
- ROMEO CASANOVA, Carlos, *Poder informático y seguridad jurídica, La función tutelar del derecho penal ante las nuevas tecnologías de información*, Editorial Fundesco, Madrid, 1988.
- ROMEO CASABONA, Carlos M, *Delitos informáticos de carácter patrimonial*, En revista Iberoamericana de derecho Informática, número 9/11, Mérida, 1996.
- ROMEO CASANOVA, Carlos, *Delitos informáticos*, En enciclopedia Penal básica, (director) LUZÓN PEÑA, Diego, Granada, 2002.

- ROMEO CASABONA, Carlos M, *De los delitos informáticos al cibercrimen*, El Cibercrimen, nuevos retos jurídicos-penales, nuevas respuestas Político-Criminales, Editorial Comares S. L., Granada, 2006.

- ROMEO CASANOVA, Carlos María, *De los delitos informáticos al Cibercrimen*, En PÉREZ ÁLVAREZ, Fernando, (editor), Homenaje Ruperto NÚÑEZ BARBERO, NÚÑEZ PAZ, Miguel / GARCÍA ALFARAZ, Ana (coordinadores), 1ª edición, Ediciones Universidad Salamanca, 2007.

- ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Editorial Comares, Granada, 2002.

- ROVIRA DEL CANTO, Enrique, *Hacia una expansión doctrinal y táctica del fraude informático*, En revista de derecho y nuevas tecnologías, Número 3, Editorial Thomson Aranzadi, 2003.

- ROXIN, CLAUS, *Derecho Penal Parte General*, Traducción de la 2° edición alemana de LUZÓN PEÑA / DÍAZ Y GARCÍA CONLLEDO / de VICENTE REMESAL), Editorial Civitas, Madrid, 1997.

- ROXIN, Claus, *La idea del bien jurídico en la teoría del injusto penal*, en Claus ROXIN / Miguel POLAINO NAVARRETE / Miguel POLAINO-ORTS, *Política criminal y dogmática penal. Cuestiones fundamentales*, ARA Editores E.I.R.L., Lima, 2013.

- ROXIN, Claus, *La imputación objetiva en el Derecho penal*, (trad. y edit. Manuel ABANTO VÁSQUEZ), Editorial Idemsa, Lima, 1997.

- SALAZAR CANO, Edgar, *Cibernética y Derecho Procesal Civil*, Ediciones Técnico-Jurídicas, Lima, 1979.

- SALVADORÍ, Iván, *Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5 /2010.* Perspectiva de derecho comparado, ADPCP, Vol. LXIV, 2011.

- SÁNCHEZ BERNAL, Javier, *El bien jurídico protegido en el delito de estafa informática*, En cuadernos del Tomás Revista de estudio electrónica del C. M. Tomás Luis de Victoria, n° 1, Salamanca CT, 2009.

- SÁNCHEZ CALERO, F, *Instituciones de Derecho mercantil*, Vol. II, 23ª Edición, Madrid, 2000.

- SÁNCHEZ PECAREVIC, Claudio, *Delito de almacenamiento de pornografía infantil*, Editorial Librotecnia, Santiago de Chile, 2010.

- SARRA, Viviana Andrea, *Comercio Electrónico y Derecho*, Editorial Astrea, Buenos Aires, Argentina, 2001.

- SCELZSI, José Licinio, *Defraudación por retención indebida*, Editorial Din editores, Buenos Aires, Argentina, 1992.

- SCHUNEMANN, Bernd. El *sistema moderno del derecho penal*. Editorial Edisofer, Argentina, 2012.

- SILVA SÁNCHEZ, Jesús María, *La expansión del Derecho penal, aspectos de la política criminal en las sociedades postindustriales*, 3ª Edición, Editorial Edisofer, España, 2011.

- Sieber, Ulrich, El control de la complejidad en el ciberespacio global: a armonización de los delitos informáticos, en Delmas-Marty, Mireille - Pieth, Mark y otros (directores) y Morales, Marta (coordinadora), Los caminos de la armonización penal (Valencia, Tirant Lo Blanch, 2009).

- Sieber, Ulrich, Legal Aspects of Computer-Related Crime in the Information Society COMCRIME. Study prepared for the European Commission (Santa Clara, University of Würzburg, 1998).

- SILVA SÁNCHEZ, Jesús María, *Aproximación al derecho penal contemporáneo*, Editorial Bosch, Barcelona 1992.

- SILVA SILVA, Hernán, *Las estafas, doctrina, jurisprudencia y derecho comparado,* Editorial jurídica de Chile, 2005.

- SNEYERS, Alfredo, el fraude y otros delitos informáticos, Editorial tecnologías de gerencia producción S. A., Madrid, 1990.

- SUÁREZ GONZÁLEZ, Carlos, En Rodríguez Mourullo Gonzalo, (dir.) t JORGE BARREIRO, Agustín, (coord.), *Comentarios al Código Penal*, Editorial Civitas, Madrid, 1997.

- SUAREZ, Carlos / JUDEL, Ángel / PIÑOL, José, *Delincuencia informática, tiempos de cautela y amparo, Las estafas*, Capitulo X, 1ª Edición, Editorial Aranzadi, Pamplona, 2012.

- TÉLLEZ VALDÉS, Julio, *Delitos cibernéticos en Informática y derecho*, Revista iberoamericana de derecho informático, número 27, 1998.

- TÉLLEZ VALDÉS, Julio, *Derecho informático*, 3ª Edición, Editorial Mc Graw Hill, México, 2003.

- TIEDEMANN, Klaus, *Criminalidad informática y Derecho penal, en su Derecho penal y nuevas formas de criminalidad* (traductor y editor: MANUEL ABANTO Vásquez), Editorial, Idemsa, Lima, 2000.

- TIEDEMANN, Klaus: «§ 263a», en LK, Tomo VI, Berlin, De Gruyter Recht, 1997.

- VALLE MUÑIZ, José Manuel, *Código penal y Leyes penales especiales*, 18° edic., Editorial Thomson Reuters Aranzadi, Pamplona, 2012.

- VALLE MUÑIZ, José Manuel, *El delito de estafa*, Editorial Bosch, Barcelona, 1987.

- VALLE MUÑIZ, José Manuel, *Tipicidad y atipicidad de las conductas omisivas en el delito de estafa*, en ADPCP, 1986.

- VALLE MUÑIZ, José Manuel, en QUINTERO OLIVARES, Gonzalo (dir.) y VALLE MUÑIZ, José Manuel (coord.), *Comentarios a la Parte Especial del Derecho Penal*, Pamplona, Aranzadi, 1996.

- VARGAS PINTO, Tatiana. *Manual de Derech penal práctico, teoría del delito con casos.* Editorial Abeledo-Perrot, Santiago de Chile, 2010.

- VELASCO NÚÑEZ, Eloy, *Delitos cometidos a través de internet, cuestiones procesales*, 1ª edición, Editorial La Ley, Madrid, 2010.

- VELASCO NÚÑEZ, Eloy (dir.), *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Editorial Consejo General del Poder Judicial, Escuela judicial, Cuadernos de Derecho Judicial, III, Madrid, 2006.

- VELASCO SAN MARTÍN, Cristos, *Las nuevas tecnologías de la información y comunicación*, Revista de investigación jurídica, Nova Iuris, Año I, núm. 1, México, 2005.

- VELASCO SAN MARTÍN, Cristos, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*, Editorial Tirant Lo Blanch, Valencia, 2012.

- VELÁSQUEZ SILVA, Juan / DONOSO ABARCA, Lorena. *Tratamiento de datos personales en internet. Los desafíos jurídicos en la era digital*, Editorial Thomson Reuters, Santiago de Chile, 2013.

- VERA QUILODRÁN, Alejandro, *Delito e informática, la informática como fuente del delito*, Editorial la Ley, Chile, 1996.

- VIVES ANTÓN, Tomás / GONZÁLEZ CUSSAC, José, *Delitos contra el patrimonio y el orden socioeconómico*, Estafas, 3ª edición, Editorial Tirant lo blanch, Valencia, 2010.

- VIVES ANTÓN, Tomás, *Derecho penal, Parte especial*, Editorial Tirant lo blanch, Valencia, 2004.

- VOGEL TÜBINGEN, Joachim, *Fraude y corrupción en el Derecho penal económico europeo, eurodelitos de corrupción y fraude*, ARROYO ZAPATERO, Luis / NIETO MARTÍN, Adán, (Coordinadores), Ediciones de la Universidad de Castilla- La mancha, Cuenca, 2006.

- VON HENTIG, Hans, *Estudios de psicología criminal, la estafa*, Volumen III, Traducción castellana y notas de José María RODRÍGUEZ DEVESA, 2ª edición, Editorial Espasa-Calpe, Madrid, 1964,

- WELZEL, HANS, *Derecho penal alemán, parte general*, Traducción del alemán por BUSTOS RAMÍREZ / Sergio YÁÑEZ PÉREZ, 11ª Edición, Editorial Castellana, Santiago de Chile, 1993.

- XALABARDER PLANTADA, Raquel, *Derecho y nuevas tecnologías*, PEGUERA POCH, Miguel (coordinador), Capítulo IX, Editorial UOC, Barcelona, 2005.

- YUBERO CANEPA, Julio, *El engaño en el delito de estafa, doctrina y jurisprudencia*, 2ª Edición, Editorial jurídica Cruz del Sur limitada, Chile, 2010.

- ZAMBONINO ALBÁN, Marco, *Problemas del derecho Tributario frente al comercio electrónico,* Editorial Abya-Yala, Quito, 2003.
- ZAPATA, María, / ABOSO, Gustavo, *Cibercriminalidad y Derecho penal, La información y los sistemas informáticos como nuevo paradigma del Derecho penal*, Editorial, B de F, Buenos Aires Argentina, 2006.

Legislación utilizada

Española

- Constitución Política de la Monarquía Española de 1978.
- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (Vigente hasta el 11 de Mayo de 2014)
- Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, o Ley de Servicios de la Sociedad de Información.
- Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal. Agencia de Protección de Datos (APD o AEPD).
- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
- Ley Orgánica 7/1984 de 15 de octubre, sobre tipificación penal de colocación ilegal de escuchas telefónicas.
- Ley de Enjuiciamiento Criminal (Real Decreto de 14 de septiembre de 1882)

- Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Legislación comunitaria e internacional

- Ley n° 19.423 Agrega disposiciones que indica en el Código Penal en lo relativo a delitos contra el respeto y protección a la vida privada y pública de la persona y su familia, Diario Oficial, 20 noviembre 1995.
- Tratado de Lisboa, de 13 de diciembre de 2007.
- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)
- La Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.
- Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
- Directiva 2013/48/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.
- Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

- Decisión Marco 2001/413/JAI del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.

- Decisión 91/242/CEE del Consejo, de 31 de marzo de 1992, relativa a la seguridad de los sistemas de información.

- Reglamento (CE) n° 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información.

- Comunicación COM (2012) 140 final, de 28 de marzo de 2012. Comunicación de la Comisión al Consejo y al Parlamento Europeo: La represión del delito en la era digital, creación de un centro europeo de Ciberdelincuencia.

- Comunicación COM (2011) 163 final, de 31 de marzo de 2001. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la protección de infraestructuras críticas de información: logros y próximas etapas: hacia la ciberseguridad global.

- Comunicación COM (2009) 149 final, de 30 de marzo de 2009. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre protección de infraestructuras críticas de información: Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia.

- Comunicación COM (2008) 448 final, de 14 de julio de 2008. Informe de la Comisión al Consejo basado en el artículo 12 de la Decisión Marco del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

- Comunicación COM (2007) 267 final, de 22 de mayo de 2007. Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones: hacia una política general de lucha contra la ciberdelincuencia.
- Comunicación COM (2001) 298 final, 6 de junio de 2001. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones: seguridad de las redes y de la información: Propuesta para un enfoque político europeo.
- Convenio 185 del Consejo de Europa sobre la Ciberdelincuencia celebrado en Budapest el 23 de noviembre de 2001.
- Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal celebrado en Estrasburgo el 28 de enero de 1981.
- Protocolo adicional al Convenio 185 del Consejo de Europa sobre la Ciberdelincuencia relativo a la incriminación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos de 2003.
- Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas de 16 de diciembre de 1966.
- Declaración Universal de Derechos Humanos de 10 de diciembre de 1948.
- Reporte Explicativo de la Convención sobre Cibercrimen del Consejo de Europa (Explanatory Report).

Legislación de otros países

Chile

- Constitución Política de la República de Chile de 1980.

- Código Penal de la República de Chile.
- Código Penal Alemán traducido a la lengua española por Claudia López Díaz. <http://www.unifr.ch/derechopenal/obras/stgb.pdf.
- Ley N° 18.168 General de Telecomunicaciones, Diario Oficial, 2 octubre 1982.
- Ley N° 19.233 Relativa de delitos informáticos, Diario Oficial, 7 junio 1993.
- Ley N° 20.009, Limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas, 2005.

EEUU

- Counterfeit Access Device and Abuse Act de 1984 [Referencia legal Pub. L. N° 98-473]. EEUU: Computer Fraud and Abuse Act de 1986.
- Economic Espionage Act de 1996 [Referencia legal Pub. L. N° 104-294].
- USA Patriot Act1 de 2001 [Referencia legal Pub. L. N° 107-56].

Alemania

- Zweites Gesetz zur Bekampfung der Wirtschaftskriminalitat (2.wikg) o Segunda Ley para la lucha contra la criminalidad económica, de 15 de mayo de 1986.

Italia

- Ley de reforma del Código penal de 1993.
- Ley de reforma del Código penal de 1995.

Literatura electrónica

- BIBLIOTECA CONGRESO NACIONAL CHILE: http://www.bcn.cl
- PÁGINA DE JURISPRUDENCIA: http://www.jurischile.cl
- BUSCADOR LEGAL: http://www.legalpublishing.cl
- FUNDACIÓN DE SEGURIDAD CIUDADANA: http://www.pazciudadana.cl
- PODER JUDICIAL CHILE: http://www.poderjudicial.cl
- POLICÍA DE INVESTIGACIONES DE CHILE: http://www.policia.cl
- TC CHILENO: http://www.tribunalconstitucional.cl
- PÁGINA DE ESTUDIOS JURÍDICOS: http://www.cienciaspenales.net
- BOLETÍN OFICIAL DEL ESTADO: http://www.boe.es/g/es/basesdatostc
- FUNDACIÓN SOCIAL NO GUBERNAMENTAL: http://www.cauce.org.ar.
- PÁGINA DE SEGURIDAD INFORMÁTICA: http://www.junk-o-meter.com
- AGENCIA DE PROTECCIÓN DE DATOS: http://www.agepd.es
- AGENCIA PROTECCIÓN DE DATOS: http://www.protecciónde datos.com.ar
- http://www.aedi.es/asp/
- ENCICLOPEDIA EN LÍNEA: http://www.biagrafíayvidas.com
- PÁGINA DE PROGRAMACIÓN E INTERNET: www.iawebdelprogramador.com
- PÁGINA TÉRMINOS JURÍDICOS EN LATÍN: http://latin.dechile.net/?Juridico
- REVISTA DIFUSIÓN JURÍDICA: http://www.tepantlato.com./reflexiones html
- PÁGINA BIBLIOTECA VIRTUAL: http://biblioteca.itam.mx/estudio/letra/html

- PÁGINA JURÍDICA PRIVADA: http://carlosparma.com.ar/sebatianchamo.htm
- SOCIEDAD DE PROTECCIÓN CIVIL: http://www.proyectoamparo.net
- PÁGINA U. ABIERTA: https://www.unifr.ch/ddp1/derechopenal/articulos/a
- PÁGINA DE ASESORÍA CONTRA VIRUS: http://www.pandasoftware.es
- PÁGINA DE INFORMÁTICA: http://www.publispain.com/antivirus
- PÁGINA OECD: http://www.oecd.org/
- OCDE: Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, http://www.oecd.org/
- PÁGINA DE CIBERSEGURIDAD: http://ciphertrust.com/resource/zombie.php.
- FUNDACIÓN CONTRA CIBERDELINCUENCIA: https:/www.shadowserver.org
- U. DE SEVILLA: http://ma1.eii.us.es/Material/Cripto_ii_Introduccion.pdf
- LA RAE: http://www.rae.es
- SITIO EDUCATIVO CHILE: wwwhttp://educarchile.cl
- BIBLIOTECA VIRTUAL: http:// www.feebooks.com
- GOOGLE ESPAÑA: http://google.es/activate
- PÁGINA CERTSI: https://www.certsi.es
- PÁGINA INCIBE: www.incibe.es
- PÁGINA GRUPO ANTI- PHISHING: http://www.anti-phishing.org
- ONU, PÁGINA WEB: http://www.un.org/es/
- ONU: http://www.uncjin.org/documents/irpc4344.pdf
- ANONYMUS: http://www.anonops.net/

- PÁGINA DE PROGRAMACIÓN: <http://www.lawebdelprogramador.com>.
- SITIO AUTORES CIENTÍFICOS-TÉCNICOS Y ACADÉMICOS: <www.acta.es>.
- PÁGINA TRABAJO DE BERNERS- LEE: <www.3.org/Berners-Lee.html>.
- ACTÍVATE, GOOGLE ESPAÑA: http://google.es/activate.
- PÁGINA DE ACTUALIDAD INFORMÁTICA: http://www.alegsa.com.ar.

Otras fuentes:

- Amenazas en la era digital, Informe sobre el Phishing y otras amenazas para las Entidades Financieras, [accesible en], <www.iberfinanzas.com.
- ARROYO BELTRÁN, Miguel, *Cibernética*, [accesible en] <http://razssosa.blogs
- BARINAS UBIÑAS, Desiré, *El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada*, En revista electrónica de Ciencia Penal y Criminología, número 15-09, 2013, pág. 3, [accesible en], <http://criminet.ugr.es/recpc/15/recpc15-09.pdf>.
- BATLLÓ, BUXÓ-Dulce, Luis, *Tarjetas de crédito y derecho penal*, Diario La Ley, Ref° D-6155, diciembre, 2004, España.
- BELTRAMONE, Guillermo / HERRERA BRAVO, Rodolfo, *Nociones básicas sobre los Delitos Informáticos*, Ponencia preparada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile, Et all, 1998.
- BEGROPONTE, Nicholas, *Ser Digital*, Editorial Atlántida, Buenas Aires, Argentina, 1995.

- BOLEA BARDÓN, Carolina/ ROBLES PLANAS, Ricardo, *La utilización de tarjetas ajenas en cajeros automáticos: ¿robo, hurto o estafa?*, Diario La Ley, 2001, Ref.º D-110, Tomo 4, España.

- BUENO ARÚS, Francisco, *El delito informático*, Publicación Aranzadi, número 11, Madrid, abril de 1994.

- BUITRAGO RUIZ, Ángela, *El Delito Informático*, Revista Derecho Penal y Criminología Vol. 18, número 59, 1996.

- CALLEGARI, Lidia, *Delitos Informáticos y Legislación en Revista de la Facultad De Derecho y ciencias Políticas de la Universidad Pontificia Bolivariana*, Medellín, Colombia, Número 70, 1985.

- CASTRO OSPINA, Sandra, Ponencia presentada dentro de las XXIII Jornadas Internacionales de Derecho Penal, Colombia, *Delitos Informáticos*, 15 de Julio 2002, [disponible en] http://www.delitosinformaticos.com/delitos.

- CARSTEN ULRICH, Computerbetrug (§ 263a StGB) JurPC: Internet-Zeitschrift für Rechtsinformatik, En revista de informática jurídica, JurPC Web-Dok. 189/1999, Abs. 1–45, [accesible en], www.jurpc.de.

- CARRIÓN, Hugo, *Presupuestos para la Punibilidad del Hacking*, 2001. [accesible en] www.delitosinformáticos.com/tesis.htm.

- Carta de la Global Internet Liberty Campaign (GILC) al Consejo de Europa acerca de la Convención sobre Cibercrimen, [accesible en], <www.gilc.org>.

- Centro de Estudios e Investigación Libertad y Desarrollo, Boletín Nº 3083-07, [accesible en], <www.lyd.com/lyd/centro-documents delito informatico.

- CASSOU RUIZ, Jorge, *Delitos informáticos en México*, En revista del Instituto de la judicatura Federal, Número 28, México, 2008.

- Código Penal y Leyes penales especiales, 18ª Edición, Editorial Aranzadi, (concordado por, VALLE MUÑIZ José), Pamplona, 2012, 87 y sigs.
- Congreso Nacional de Chile, Proyecto que modifica la Ley Nº 19.628 en lo que se refiere a la publicación de boletines con información de datos *personales y patrimoniales,* con el objeto de proteger más adecuadamente los derechos de las personas y de las pymes. Además, propone modificar la ley para dar una mejor protección a los *datos sensibles* y hacerse cargo de los problemas derivados del *spam* [accesible en], <http://sil.congreso.cl/pags.
- Convención sobre Delitos en internet del Consejo de Europa, de 29 de junio de 2001, [accesible en], <www.conventions.coe.Cybercrimen>.
- Diccionario de informática, Editorial Cultura S.A., Madrid, 2001.
- Diccionario de informática y telecomunicaciones, Inglés-Español, Editorial Ariel S.A., Barcelona, España 2001.
- Diccionario de informática e internet de Microsoft, Editorial Mcgraw-Hill, España, 2005.
- Diccionario De La Lengua Española, Tomo I, 22ª Edición, Editorial Espasa Calpe, Madrid, 2005.
- *Décimo Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente,* Naciones Unidas Viena, 2000.
- DELPIAZZO, Carlos E, *Del derecho informático al derecho telemático,* En acervo de la biblioteca jurídica virtual, "estudios en homenaje al Dr. Julio TÉLLEZ VALDÉS" UNAM, (documento sin fecha), México, [accesible en] <www.juridicas.unan.mx>.
- Departamento de Justicia de USA, sección dedicada al Cybercrime y a la Propiedad Intelectual, [accesible en] http://www.usdoj.gov/criminal/cybercr.

- Enciclopedia jurídica, *Estafa*, Editorial Francisco Seix, tomo IX, Barcelona, 1958.

- FERNÁNDEZ CALVO, Rafael, *Glosario básico inglés-español para usuarios de Internet*, 4ª edición, [accesible en] http://www2.ati.es/novatica/glosar.

- FERNÁNDEZ CALVO, Rafael, *El Tratamiento del Llamado Delito Informático, En el proyecto de Ley Orgánico del Código Penal*, (Comisión de Libertades e Informática), En Informática y Derecho, 2015.

- FONSECA MARTÍNEZ Claudia, *El Spam y el ejercicio de la Libertad en la Red*, Revista de Derecho informático, número 081 de Abril de 2005, [accesible en], <http://www.alfa-redi.org/rdi-articulo.shtml?x=95>.

- GABALDÓN GERARDO, Luis, *Fraude electrónico y cultura corporativa*, Editorial Universidad Federal de Bahía, Mayo-Agosto, 2006, [accesible en], <www.redalyc.org/articulo.oa>.

- GARCÍA BARCELÓ, Miguel, *Ponencia presentada al: Congreso sobre, Derecho Informático*, Universidad de Zaragoza, España, en junio de 2013.

- GALÁN MUÑOZ, Alfonso, *El nuevo delito del artículo 248.3 CP*: ¿Un *adelantamiento desmedido de las barreras de protección penal del patrimonio?*, Diario La Ley Nº 6037, Año XXV, de 10 junio de 2004, Referencia, D-130.

- GARCÍA-CERVIGÓN, Josefina, *El fraude informático en España e Italia, tratamiento jurídico-penal y criminológico,* En revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales, número 74, mayo-agosto 2008, ISSN: 02 12-7377.

- GUERRERO MATEUS, M, *La Ciberdelincuencia: La Ley Patriótica y sus efectos globales en las regulaciones nacionales y en particular en el caso*

colombiano, En Revista de Derecho privado, Volumen 16, N° 29, Colombia, 2012.

- Grupo Activo Anti-Phishing, Diccionario de informática, Ed Cultura S.A., Madrid, 2001, [accesible en], <www.anti-phishing.org>. (en inglés).
- Godfrain, Loi, Relative à la fraude informatique, [accesible en] <http://www.spi.ens>.
- HERNÁNDEZ DÍAZ, Leyre, *El delito informático*, En revista Eguzkilore, Número 23, San Sebastián, 2009.
- HERRERA BRAVO, Rodolfo, *Ciberespacio, sociedad y derecho*, En revista chilena derecho informático, U. De Chile, número 3, Santiago de Chile, 2003.
- HERRERA BRAVO, Rodolfo, *Reflexiones sobre la delincuencia vinculada con la tecnología digital, basadas en la experiencia chilena*, pág. 7. [accesible en] www.rodolfoher.com
- HUERTA MIRANDA, Marcelo, *Figuras delictivo informáticas tipificadas en Chile*, En revista de Derecho público de la Agrupación de Abogados de la Contraloría General de la República, Separata 12 2001, [accesible en], <www. biografias.bcn.cl>.
- H Wold, Geoffrey; CPA; CMA; CSP; CISA; CMC; y f. Shiver, Robert. "Computer Crime Tecniques Prevention". Ed. Bankers Publishing Company, Illinois, 1989.
- Instituto Nacional de Ciberseguridad de España S.A. (INCIBE). [accesible en], <www.incibe.es>.
- INTECO, Equipo que gestiona incidentes de phishing en España, [accesible en], <www. cert.inteco.es/ Fraude-Electrónico>.

- La revista de la Defensoría Penal Pública, *Internet, olvido y dignidad*, número 14, 2008.

- Comisión Europea, *Libro Verde sobre la Convergencia de los Sectores de Telecomunicaciones, Medios de Comunicación y Tecnologías de la Información y sobre sus Consecuencias para la Reglamentación*, Bruselas, diciembre de 1997, [accesible en] <http://www.europa.eu>.

- LIMA MALVIDO, María de la Luz, *Delitos electrónicos en criminalia*, México, Academia Mexicana de Ciencias Penales, Editorial Porrúa, Número 1-6. Año I., Enero-Junio 2004.

- LÓPEZ DA SILVA, Rita, *Direito penal, e sistema informático*, Editorial Revista dos Tribunais, Ciencia Derecho penal contemporánea número 4, (Coordinador) PRADO REGIS, Luis, Sao Paulo, 2003.

- LORENZO, Patricia, *Conceptualización y generalidades del fraude Delitos Informáticos*, [accesible en], <www.delitoinformático.com>.

- LOYOLA, H. Pablo / MARTÍNEZ A. Gustavo / VELÁSQUEZ, Juan, *Caracterizando la fijación ocular del usuario web en los contenidos de una página: Una aproximación basada en teoría de grafos*, Revista de Ingeniería de Sistemas, Volumen XXVIII, septiembre 2014, pág. 86. [accesible en] http://www.dii.uchile.cl/~ris/RIS2014/5webocular.pdf.

- MATEOS MUÑOZ, Agustín, *Compendio De Etimologías Greco-Latinas Del Español*. Editorial Esfinge, Cuadragésima sexta edición, México, 2007.

- TÉLLEZ VALDÉS, JULIO, *Regulación del spam en México*, [accesible en], <htpp: // www.razonypalabra .org.mx>.

- TÉLLEZ VALDÉS, Julio, *Aspectos legales de lo virus informáticos, en actas del III, Congreso Iberoamericano de informática y derecho*, Mérida, 1994.

- LECHUGA MATERNACH, Vicente, *Derecho, intimidad e informática*, En revista del Colegio de Notarios del Estado de México, Año 2, número 4, 1999.

- MAGLIONA MARCOVICTH, Claudio, *Delincuencia informática en Chile. Proyecto de Ley*, Asociación de Derecho e informática de Chile, 2003, [accesible en] <www. biografias.bcn.cl/pdf>.

- MATUS ACUÑA, Jean / HERNÁNDEZ BASUALTO, Héctor, *Anteproyecto de Nuevo Código Penal. Texto refundido y sistematizado del articulado aprobado en las deliberaciones de la Comisión Foro Penal del Ministerio de Justicia*, Desde el 8 de mayo de 2003, hasta el 10 de noviembre de 2005, En Política Criminal, número 1, DI: pág. 1-92. [accesible en] <http://www.politicacriminal.cl/n_01/pdf_01/d_l.pdf>.

- MATEOS MUÑOZ, Agustín, *Compendio de etimologías Greco- Latinas del Español*, Editorial Esfinge, Cuadragésima sexta edición, México, 2000.

- OECD, *Malicous software* (malware): A segurity therat to the Internet economy, what is a malware? [accesible en], <www.oecd.org/sti.pdf>.

- *Malicius Software* (malware): A security threat to the internet economy, Ministerial Background Report, DSTI/CCP/REG, 2007/ 2008. [accesible en], <http://www.oecd.org/datao-ecd.pdf>.

- MEDINA SCHULZ, Gonzalo, *Principales reformas en la legislación penal y procesal, (Alemania),* Revista Penal, Universidad de Friburgo en Brisgovia. 2006. [accesible en], www.uhu.es/revistapenal/index>.

- MILLETARY, Jasonn, *Tendencias técnicas en los ataques de phishing*, Documento del Centro de Coordinación (CERT) Universidad de Carnegie Mellon. ubica en la ciudad de Pittsburgh (Pensilvania). Destacado centro de

investigación superior de los Estados Unidos en el área de ciencias de la computación y robótica, [accesible en], <http://resources.sei.cmu.edu>.

- MORABITO, MARIO, *La regulación de los Delitos informáticos en el Código Penal argentino*, Editorial Thomson Reuters, La ley, [accesible en] <www.dab.com.ar>.

- PANIZA FULLANA, Antonia, *E-Consumidores, aspectos problemáticos en la normativa española*, En revista Chilena de derecho informático, número 8, 2006.

- PRANDINI, Patricia / MAGGIORE, Marcia, *Ciberdelito en América Latina y el Caribe*, Una visión desde la Sociedad Civil, Proyecto Amparo, 2013. [accesible en], www.proyecto amparo. ciberdelito.

- RAMÍREZ BASTIDA, Oscar, *Herramienta de autoestudio en telecomunicaciones básicas para la fuerza de ventas directa e indirecta*, Editorial Orbitel S.A., Universidad de Antioquia. [accesible en] <http://bibliotecadigital.udea.edu.com>.

- Real academia española de la lengua, Diccionario virtual de la, [accesible en],<http://www.rae.es/ existen

- RINCÓN, Antonio / PLAGARO, Julio, *Diccionario conceptual de informática y comunicaciones*, Editorial Paraninfo, Madrid, 1998.

- RÍOS ESTAVILLO, Juan, *Informática jurídica,* [sólo accesible en], <www.revistas.juridicas.unam>.

- RODRÍGUEZ-MAGARIÑOS, Fautino, *Nuevos delitos informáticos: phishing, pharming, hacking y cracking*, 2009, [Recuperado en] <htpp:/web.icam.es/index.php>.

- ROVIRA DEL CANTO, Enrique, *Hacia una expansión doctrinal y fáctica del fraude informático*, Revista de Derecho y Nuevas tecnologías, núm. 3, Editorial Thomson Aranzadi, 2003.

- SALLIS M, Exequiel, *Cibercrimen, Desafío de la investigación*, Área de cibercrimen, Policía Metropolitana, REMJA, Buenos Aires, Argentina, 2016. Material extraído, de la reunión de ministros de justicia u otros ministros, procuradores fiscales generales de la América. Grupo de trabajo en delito cibernético. Organización de los Estados Americanos.

- *Las organizaciones internacionales deben prestar más atención en este aspecto.* SCHJOLBERG, S, *La historia de la armonización global sobre la legislación de delitos informáticos*, En camino a Ginebra., Noviembre de 2015. [accesible en] http://www.cybercrimelaw.

- TRIGO ARANDA, Vicente, *Historia y evolución de internet*, En Autores científicos-técnicos y académicos, Madrid, [accesible en] <http://www.acta.es>.

- ONU: *Manual de las Naciones Unidas sobre prevención y control de delitos informáticos*, En Revista Internacional de Política Criminal, Editorial Naciones Unidas, número 43 y 44, 1994.

- ORGANIZACIÓN DE LAS NACIONES UNIDAS, Delitos Relacionados Con Redes Informáticas, Documento Antecedente Para El Curso Práctico Sobre Delitos Relacionados Con Las Redes Informáticas, En 10º Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente, Vienna, 2000.

- ORGANIZACIÓN DE LAS NACIONES UNIDAS, Informe del Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente.

- UNODC (United Nations on Drugs and Crime), Estudio exhautivo sobre le delito cibernético Oficina De Las Naciones Unidas Contra La Droga y El Delito, Naciones Unidas, Nueva York, 2013.
- Universidad de Sevilla, Ingeniería Informática, Curso número 5° de Criptografía, (Doc.Tec.) 2007/2008. [en línea] <www. ma1.eii.us.es>.
- Unión Internacional de Telecomunicaciones, *Cumbre Mundial sobre la Sociedad de la Información*, Ginebra 2003, Túnez 2005.

Jurisprudencia:

Española

Tribunal constitucional

- STC N° 49, de 05. IV. 1999 (Ponente: Magistrado don Tomas S. VIVES ANTÓN)

Tribunal supremo

- STS N° 807, Sala 2ª de lo Penal, de 03. III. 2003 (Ponente: Excmo. Sr. D. Andrés MARTÍNEZ ARRIETA)
- STS N° 948, Sala 2ª de lo Penal, de 08. VII. 2002 (Ponente: Excmo. Sr. D. José Manuel MAZA MARTÍN)
- STS N° 465, Sala 2ª de lo Penal, de 01 de VI. 2012 (Ponente: Excmo. Sr. D. Alberto JORGE BARREIRO)
- STS N° 187, Sala 2ª de lo Penal, de 08 II. 2002 (Ponente: Excmo. Sr. D. José Ramón SORIANO SORIANO)

- STS N° 1476, Sala 2ª de lo Penal, de 21. XI. 2004 (Ponente: Excmo. D. Enrique BACIGALUPO ZAPATER)
- STS N° 559, Sala 2ª de lo Penal, de 16. III. 2009 (Ponente: Sr. Siro Francisco GARCÍA PÉREZ)
- STS, Sala 2ª de lo Penal, N° 559, de 16. III. 2009, (Ponente: Sr. Siro Francisco GARCÍA PÉREZ)
- STS, Sala 2ª de lo Penal, Nº 834, de 25. X. 2012, (Ponente: Sr. Manuel MARCHENA GÓMEZ)
- STS, Sala 2ª de lo Penal, N° 328, de 5. V. 2015, (Ponente: Sr. José Ramón SORIANO SORIANO)
- STS, Sala 2ª de le Penal, N° 331, de 15. IV. 2014, (Ponente: Sr. Cándido PUNPIDO TOURON).
- STS, 2ª de lo Penal, N° 614, de 08. VII. 2016, (Ponente: Sr. Antonio del MORAL GARCÍA)
- STS, Sala 2ª, de lo Penal, N° 187, de 08. II. 2002, (Ponente: Sr. José Ramón SORIANO SORIANO)
- STS, Sala 2ª en lo Penal, N° 358, de 10 VI. 2015, (Ponente: Sr. Francisco MONTERDE FERRER)
- STS, Sala 2ª en lo Penal, N° 614, de 08. VII. 2016 (Ponente: Sr. Antonio DEL MORAL GARCÍA)
- STS, 2ª de lo Penal, N° 452, de 31. V. 2011, (Ponente: Sr. Juan Ramón BERDUGO GOMEZ DE LA TORRO)
- STS, Sala 2ª en lo Penal, N° 660, de 14. X. 2014 (Ponente: Sr. Ana María FERRER GARCÍA)

- STS, 2ª Sala de Lo Penal, N° 733, de 09. VII. 2009, (Ponente: Sr. Juan Ramón BERDUGO GOMEZ DE LA TORRE)
- STS, Sal 2ª en lo Penal, N° 298, de 14. III. 2003, (Ponente: Sr. José Ramón SORIANO SORIANO).
- STS, 2ª Sala en lo Penal, N° 358, de 10. VI. 2015, (Ponente: Sr. Francisco MONTERDE FERRER)
- STS, Sala 2ª en lo Penal, N° 662, de 14. X. 2008. (Ponente: Sr. Joaquín GIMÉNEZ GARCÍA)
- STS, 2ª DE LO PENAL, N° 368, DE 09. V. 2007, (Ponente: Sr. Juan Ramón BERDUGO GOMEZ DE LA TORRO)
- STS, 2ª DE LO PENAL, N° 622, DE 09. VII. 2013, (Ponente: Sr. Luciano VARELA CASTRO)
- STS, 2ª De Lo Penal, N° 364, de 11. V. 2011, (Ponente: Sr. Diego Antonio RAMOS GANCEDO)
- STS, 2ª Sala de Lo Penal, N° 358, de 10. VI. 2015, (Ponente: Sr. Francisco MONTERDE FERRER)
- STS, 2ª De Lo Penal, N° 524, de 15. X. 2014, (Ponente: Sr. Miguel Ángel AMEZ MARTÍNEZ)

Audiencia Nacional

- AEPD, Expediente Nº: E/00075/2005 (Ponente: Sr. José Luis PIÑAR MAÑAS)

Audiencia provincial

- SAP de Vizcaya, Sección 3ª, Nº 429, de 10. XI. 2016, (Ponente: Sra. María CONCEPCIÓN MARCO CACHO)
- SAP Nº 178, 04. V. 2015, (Ponente: Magistrado Sra. Beatriz PATIÑO ALVES)
- SAP de Madrid de N° 12, de 25. I. 2016, (Ponente: Magistrado Sr. Juan Antonio TORO PEÑA)
- SAP de Zaragoza, Sección 6ª, N° 358, de 02. XI. 2010, (Ponente: Magistrado Sr. Rubén BLASCO OBEDE)
- SAP de Santa Cruz de Tenerife, Sección 2ª, Nº 248, de 29. V. 2014, (Ponente**:** Magistrada Sra. María Jesús GARCÍA SÁNCHEZ)
- SAP de Cáceres, Sección 2ª, Nº 344, de 30. VII. 2015, (Ponente: Sr. Valentín PÉREZ APARICIO)
- SAP de León, Sección 3ª, Nº 524, 15. X. 2014, (Ponente: Sr. Miguel Ángel AMEZ MARTÍNEZ)
- SAP de Madrid, Sección 2ª, N° 782 de 23 IX. 2015 (Ponente: Sr. María Del Rosario ESTEBAN MEILAN)
- SAP, de Valencia, Sección 3ª, N° 363, de 21. V. 2010, (Ponente: Sr. Lamberto RODRÍGUEZ MARTÍNEZ)
- SAP, de Madrid, Sección 15, N° 293, de 15. IV. 2015, (Ponente: Sr. Carlos FRANCISCO FRAILE)
- SAP de Cádiz, Sección 1ª N° 181, de 08. VI. 2015, (Ponente: Sr. Francisco Javier GRACIA SANZ),

Chilena

- SCS Rol N° 5128, de 06. X. 2009
- SCA de San Miguel, Santiago, Rol N° 303, 11. IV. 2016
- SCS Rol N° 5.259, de 25. VII. 2009
- SCA San Miguel, Santiago, 16. VIII. 1993
- SCS Rol N° 5128, de 06. X. 2009
- STS 484/2008, de 5 de mayo y 787/2011
- S, 4°. J. G. De Santiago, RIT: 13685, 08. IX. 2009.
- S, J. G. De Concepción, RIT: 2294, 13. IV. 2010.
- Sentencia, TOP de Curicó, RIT: 81, acumulado a 86, 07. III. 2010.

ANEXO.

GLOSARIO TÉCNICO

A continuación se entrega un glosario técnico, con términos que se estiman que son los que se utilizan con más frecuencia en la actualidad tanto para referirse a las nuevas tecnologías de información, como a la delincuencia informática. Vale señalar que existe una distinción entre términos de la informática propiamente tal, los cuales tienen una base técnica y los términos o expresiones utilizadas en el mundo virtual, tanto para referirse a tipos de delitos o defraudaciones o a las formas de cometerlos. Además de ello, es necesario señalar que estos términos van variando o evolucionando según la ingeniería social, por ello se ha tratado de recopilar los que sean más cotidianos y de mayor utilidad. Por último, existen algunas definiciones que han sido analizadas con mayor detención en el cuerpo de esta investigación, toda vez que el mismo tema lo ameritaba, por ello puede existir que algunos de dichos términos están definidos en este glosario técnico, de alguna manera más resumida[577].

ADSL: Abreviación de *Asymmetric Digital Subscriber Line*, el ADSL es un método de transmisión de datos, a través de las líneas telefónicas de cobre tradicionales a velocidad alta. Los datos pueden ser descargados a velocidades de hasta 1.544 Megabits por segundo y cargados a velocidades de hasta 128 Kilobits por segundo. Esa es la razón por la cual se le denomina asimétrico. Esta

[577] Todos términos utilizados en esta investigación, y que no llevan nota al pie, tienen como fuente: www.lawebdelprogramador.com/www.alegsa.com.ar; diccionario de informática e internet de Microsoft, 2005.

tecnología es adecuada para la web, ya que es mucho mayor la cantidad de datos que se envían del servidor a un ordenador personal que lo contrario[578].

Android: Es un sistema operativo móvil desarrollado por Google para teléfonos inteligentes con pantalla táctil. Basado en el kernel de Linux. Es el sistema operativo móvil con más ventas en tabletas y teléfonos inteligentes desde 2013. *Android* permite utilizar el teléfono completamente desde la pantalla con gestos y toques. Emplea un teclado virtual en la pantalla para introducir texto.

Acortadores: A veces, una URL puede ser muy larga y complicada, por lo que puede ser difícil de memorizar, de copiar o de comunicar. Para solucionar este problema se emplean los acortadores de URL, un mecanismo que permite convertir una URL larga en una URL corta. Estos sistemas se han popularizado en los últimos años debido a la aparición de sistemas como Twitter, que limitan la longitud de los textos que se pueden escribir. Los acortadores de URL más populares en la actualidad son el de Google, el de bitly y el de owly[579].

Adware: Se trata de programas que recogen o recopilan información acerca de los hábitos de navegación del usuario en cuestión.

Acceso Múltiple de División de Llamada o CDMA: Una de las dos normas principales de telefonía celular digital.

AfriNIC, Centro de información de la red africana: AfriNIC es un Registro Regional de Internet (RIR), y es una organización sin fines de lucro responsable

[578] RAMÍREZ BASTIDA, Oscar, *Herramienta de autoestudio en telecomunicaciones básicas para la fuerza de ventas directa e indirecta*, Editorial Orbitel S.A. Universidad de Antioquia, pág. 1. [accesible en] <http://bibliotecadigital.udea.edu.com>.

[579] [disponible en] http://google.es/act.

de la administración y el registro de las direcciones de Protocolo de Internet (IP) en la región africana[580].

Agente o agent: En Internet un agente (también llamado agente inteligente) es un programa que recoge información o realiza algún otro servicio de forma planificada y sin la presencia del usuario. Habitualmente, un programa agente, utilizando parámetros suministrados por el usuario, busca en toda Internet, o en parte de ella, información de interés para el mismo y se la facilita de forma periódica, diaria o no[581].

Alteración de datos: La *Alteración de datos* como tal generalmente es comprendida por algunas legislaciones como parte integrante del llamado sabotaje informático como en Alemania y otros en cambio como Francia, se consideran como figuras diversas incluso a veces agravadas y como su nombre lo indica implica alterar o modificar los datos contenidos en un sistema de tratamiento de la información.

ANI, Identificación automática de números: ANI, igual que la ID de quien llama, ésta da información sobre la red telefónica de la parte que hace llamadas telefónicas. La ANI es diferente de la ID de quien llama por al menos dos características importantes: la ANI no puede ser bloqueada por la persona que llama; La ID de quien llama da el número real que llama, por ejemplo el número de marcación directa de una persona que llama desde una extensión en una

[580] Glosario ICANN. Org., [Accesible en] https://www.icann.org.

[581] FERNÁNDEZ CALVO, Rafael, *Glosario básico inglés-español para usuarios de Internet*, 4ª edición, pág. 02, [accesible en] http://www2.ati.es/novatica/glosar.

oficina corporativa. La ANI únicamente proporciona el número al que se factura, por ejemplo, el número principal de conmutador de una oficina corporativa[582].

***Anonymous* FTP:** (FTP anónimo). El FTP anónimo permite a un usuario de internet la captura de documentos, ficheros, programas y otros datos contenidos en archivos existentes en numerosos servidores de información, sin tener que proporcionar su nombre de usuario y una contraseña *password*. Utilizando el nombre especial de usuario *anonymous*, o a veces FTP, el usuario de la red podrá superar los controles locales de seguridad y podrá acceder a ficheros accesibles al público situados en un sistema remoto[583].

Anonimizadores: Servicio proxy que permite navegar sin que se sepa la IP del cliente[584]. Se trata de aplicaciones que por su funcionamiento esconden la dirección IP original, desde donde se realiza la petición de una página. Por ejemplo un *firewall* que posee una IP pública y por donde pasa cualquier solicitud de la red interna de una institución. En este caso se realiza un cambio de la IP privada a IP pública, es decir, cualquier petición de una página que se origine desde un computador de la red interna saldrá con la misma IP pública. Lo mismo ocurre con los sistemas caché implementados con *Proxy Server* y con la asignación de IP dinámicas, por parte de los internet *Service Providers*[585].

[582] Glosario técnico, Sección de Laboratorio de Delitos Cibernéticos, Delitos por Computadora y de Propiedad Intelectual, Departamento de Justicia de Estados Unidos [accesible en] https://www.justice.gov/criminal-ccips.

[583] FERNÁNDEZ CALVO, Rafael, *Glosario básico inglés-español para usuarios de Internet*, 4ª edición, pág. 82, [accesible en] http://www2.ati.es/novatica/glosario/glointv4.pdf

[584] Glosario e-legales, [accesible en] http://e-legales.net/glosario-de-terminos.

[585] LOYOLA, H. Pablo / MARTÍNEZ A. Gustavo / VELÁSQUEZ, Juan, *Caracterizando la fijación ocular del usuario web en los contenidos de una página: Una aproximación basada en*

AOL, América Online: El proveedor más grande de servicio de internet, el cual proporciona muchos servicios de valor agregado, además del acceso a internet.

APNIC, Centro de Información de Redes del Pacífico Asiático: APNIC es un Registro Regional de Internet (RIR), y es una organización sin fines de lucro responsable de la administración y el registro de las direcciones de Protocolo de internet (IP) en la región del Pacífico Asiático, dentro de la cual se incluyen Japón, Corea, China y Australia[586].

Apodo: Los usuarios del Internet *Relay Chat* (IRC) se identifican mediante un *sobre nombre* único que ellos mismos eligen (apodo), similar al nombre de usuario que normalmente no da ninguna indicación de la verdadera identidad[587].

***Archive site,* lugar de archivo o sitio de archivo[588]**: Ordenador conectado a internet que permite el acceso de los usuarios a una colección de ficheros en él almacenados. Un *anonymous* FTP *archive site*, por ejemplo, permite el acceso a dicho material mediante el protocolo FTP. Los servidores www pueden también actuar como sitios de archivo.

---

teoría de grafos, Revista de Ingeniería de Sistemas, Volumen XXVIII, septiembre 2014, pág. 86. [accesible en] http://www.dii.uchile.cl.

[586] Glosario, https://www.icann.org/resources/pages/glossary-bc-2014-02-04-es

[587] FERNÁNDEZ CALVO, Rafael, Glosario básico inglés-español para usuarios de Internet. Asociación de Técnicos de Informática, 4ª edición, pág. 3. [accesible en] www.ati.es/novaticaglosar.

[588] FERNÁNDEZ CALVO, Rafael…op. cit., pág. 3.

Arenero: Un mecanismo de seguridad que se utiliza para separar los programas que corren. Con frecuencia se utiliza para ejecutar códigos que no se han probado o programas de desconfianza como un código dañino[589].

ARIN, Registro Norteamericano de Números de Internet: ARIN es un registro regional de internet (RIR), y es una organización sin fines de lucro responsable de la administración y el registro de las direcciones de Protocolo de Internet (IP) en Norteamérica, partes del Caribe y el África Subsahariana[590].

Asignación de direcciones de protocolo de internet: Un número finito de direcciones IP están disponibles para su asignación a nivel mundial. Las direcciones de Protocolo de Internet (IP) se asignan, adquieren, venden y rentan dependiendo de las necesidades del usuario y viabilidad comercial. Las direcciones IP las administran geográficamente cinco Registros Regionales de internet (RIR): RIN, Registro Americano de Números de Internet, América del Norte y países del Caribe; RIPE, *Reseaux IP Europeans*, Europa, Medio Oriente y Asia Central; APNIC, Centro de Información de la Red de Asia Pacífico, Región Asia Pacífico; LACNIC, Registro de Direcciones de Internet de América Latina y el Caribe, América Latina y países de la región del Caribe; AfriNIC, Centro de Información de la Red Africana, para África[591].

Asignación estática de IP: La práctica de un proveedor de servicios de internet (ISP) mediante la asignación permanente de la misma dirección de protocolo de

[589] Glosario técnico. Sección de Laboratorio de Delitos Cibernéticos. Delitos por Computadora y de Propiedad Intelectual. Departamento de Justicia de Estados Unidos [accesible en] https://www.justice.gov/criminal-ccips.

[590] Glosario, [accesible en] https://www.icann.org/resources/pages/glossary.

[591] Glosario técnico, Sección de Laboratorio de Delitos Cibernéticos. Delitos por Computadora y de Propiedad Intelectual, Departamento de Justicia de Estados Unidos [accesible en] https://www.justice.gov/criminal-ccips.

Internet (IP) a un usuario[592].

Asignación dinámica de IP o Protocolo dinámico de configuración de Host (DHCP): Cuando un usuario se conecta a un proveedor de servicios de internet (ISP) por medio de una asignación dinámica de direcciones protocolo de Internet (IP), el ISP asigna una dirección IP al usuario. El ordenador del usuario retiene esa dirección IP durante la sesión. Una vez que el usuario se desconecta, la dirección IP estará disponible para su asignación a otros clientes[593].

ASP, Proveedor de Servicio de Aplicaciones: Empresa cuyo objetivo es ofrecer a sus clientes el alquiler, como alternativa a la compra, de aplicaciones para y a través de la red.

Página de Servidor Activo: Una página ASP es un tipo especial de página HTML que contiene unos pequeños programas (también llamados *scripts*) que son ejecutados en servidores *Microsoft Internet Information Server*, antes de ser enviados al usuario para su visualización en forma de página HTML. Habitualmente esos programas realizan consultas a bases de datos y los resultados de esas consultas determinan la información que se envía a cada usuario específico. Los ficheros de este tipo llevan el sufijo *asp*. (No confundir con Application Service Provider).[594]

---

[592] Glosario técnico, Sección de Laboratorio de Delitos Cibernéticos. Delitos por Computadora y de Propiedad Intelectual, Departamento de Justicia de Estados Unidos [accesible en] https://www.justice.gov/criminal-ccips.

[593] Glosario técnico, Sección de Laboratorio de Delitos Cibernéticos. Delitos por Computadora y de Propiedad Intelectual, Departamento de Justicia de Estados Unidos [accesible en] https://www.justice.gov/criminal-ccips.

[594] FERNÁNDEZ CALVO, Rafael, Glosario básico inglés-español para usuarios de Internet. Asociación de Técnicos de Informática, 4ª edición, pág. 4. [accesible en] www.ati.es/novaticaglosar.

Atajo o archivo LNK: Un archivo pequeño que contiene la ubicación de un blanco (como un archivo, programa o dirección electrónica) así como las horas de creación/escritura/acceso y opcionalmente otros parámetros. El uso más obvio de atajos es en los iconos en una computadora de escritorio de un usuario; sin embargo Windows también usa atajos en muchas otras situaciones donde tienen valor pericial[595].

Ataque de negación de servicio: Un ataque a la red que tiene el objetivo de desactivar a la víctima o bloquearle la comunicación con el resto de la red en lugar de violar su seguridad[596].

***Banner**:* Un mensaje que se presenta a un usuario al inicio de cada sesión, en particular se trata de una cláusula de desistimiento de los derechos a la privacidad[597].

Bit: La unidad más pequeña de información (datos) que una computadora puede procesar. Un *bit* puede tener un valor de cero o ningún valor. La palabra es una contracción del término dígito binario.

[595] Glosario técnico, Sección de Laboratorio de Delitos Cibernéticos. Delitos por Computadora y de Propiedad Intelectual, Departamento de Justicia de Estados Unidos [accesible en] https://www.justice.gov/criminal-ccips.

[596] Glosario técnico, Sección de Laboratorio de Delitos Cibernéticos. Delitos por Computadora y de Propiedad Intelectual, Departamento de Justicia de Estados Unidos [accesible en] https://www.justice.gov/criminal-ccips.

[597] Glosario técnico, Sección de Laboratorio de Delitos Cibernéticos. Delitos por Computadora y de Propiedad Intelectual, Departamento de Justicia de Estados Unidos [accesible en] https://www.justice.gov/criminal-ccips.

***BitTorrent*:** Un protocolo que se utiliza para compartir archivos de *peer-a-peer* que es particularmente eficiente para la distribución simultánea de contenido a un número muy grande de usuarios.

Bitácora: Sustantivo: Un archivo que contiene registros operativos de cierto tipo de evento (por ejemplo, registros de los accesos de visitantes al sitio electrónico). Una sola máquina puede tener bitácoras independientes para muchos tipos diferentes de actividad.

Bitácora de teclas o *Keylogging*: La práctica de registrar las teclas que se presionan en un teclado, por lo general de una manera en la que la persona que usa el teclado no percibe que está siendo monitoreado. El registro de teclas se hace con un dispositivo de hardware o con un programa de *software*. Ocasionalmente el término también se usa para describir las técnicas que registran más información aparte de las teclas que se presionan, por ejemplo, los programas que se corren o las imágenes de la pantalla.

***Blog* o bitácora**: Es un sitio web personal donde se escriben periódicamente, como un diario on line, sobre distintos temas que le interesan al propietario. Cada escrito está ordenado cronológicamente y en general posee enlaces a otras páginas.

Bloque IP: Un rango de direcciones IP consecutivas (por ejemplo, las 256 direcciones que van desde 193.5.6.0 hasta 193.5.6.255).

Bloqueo de escritura: Un dispositivo que se anexa al medio electrónico original durante las imágenes periciales que evita (bloquea), escribir en esos medios electrónicos. También se le conoce como bloqueador de escritura *write blocker.*

Boletín o BBS: Originalmente es un sistema que permitía a los usuarios conectarse y subir o bajar datos y leer o colocar mensajes. En las décadas de los 70 y 80, los usuarios por lo general se conectaban por medio de módems. En la

actualidad, el término ocasionalmente se utiliza para referirse a foros en la *web* o a tableros de mensajes.

Brinco: Cada segmento de la trayectoria que toma un paquete en internet entre su punto de origen y su destino se denomina brinco. Típicamente los paquetes pasan por una serie de ruteadores entres sus puntos de origen y destino.

Caballo de Troya: Es una clase de virus que se caracteriza por engañar a los usuarios disfrazándose de programas o archivos benignos (fotos, archivos de música, archivos de correo, etc.), con el objeto de infectar y causar daño. El objetivo principal de un troyano informático, es crear una puerta trasera que da acceso a una administración remota del atacante no autorizado. Los troyanos están compuestos por dos archivos; un cliente que es el que envía las órdenes y un servidor que recibe las órdenes del cliente, las ejecuta y devuelve resultados.

Canal: Un mecanismo en IRC que permite a un grupo de personas escribir mensajes que ven todos aquellos que participan en el *canal*.

CART, Equipo de respuesta y de análisis de ordenador: Es la unidad en el FBI que brinda asistencia en la búsqueda y aseguramiento de evidencia de los sistemas de cómputo así como peritajes y apoyo técnico para las investigaciones del FBI.

CERT de Seguridad e Industria (CERTSI): Es la Capacidad de respuesta a incidentes de seguridad de la información del *Ministerio de Energía, Turismo y Agenda Digital y del Ministerio del Interior*. Por Acuerdo del Consejo Nacional de Ciberseguridad de 29 de mayo de 2015, es operado técnicamente por INCIBE, y bajo la coordinación del CNPIC e INCIBE, el CERTSI, que se constituyó en el año 2012, a través de un Acuerdo Marco de colaboración en materia de Ciberseguridad entre los operadores de infraestructuras críticas, públicos o

privados, designados en virtud de la aplicación de la Ley 8/2011. En el CERTSI tienen su punto de referencia para la resolución técnica de incidentes de ciberseguridad que puedan afectar a la prestación de los servicios esenciales, según establece la resolución de 8 de septiembre de 2015 (publicada en el BOE de 18 de septiembre), de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los planes de seguridad del operador y de los planes de protección específicos. La Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la sociedad de la información. Actualmente es regulado mediante Acuerdo de 21 de octubre de 2015, suscrito por ambas Secretarías de Estado. (CERTSI es el CERT Nacional competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas).

Cibercrimen: cualquier actividad maliciosa realizada con el fin de comprometer la confidencialidad, integridad y disponibilidad de la información, aprovechando las vulnerabilidades que presentan Internet y los dispositivos y sistemas involucrados. El cibercrimen es similar al ciberdelito aunque este último se vincula más directamente con el quebrantamiento de las leyes, y con la consiguiente pena. El cibercrimen en cambio, puede ser considerado un término más amplio, que abarca toda acción indebida o reprensible que ocurre en el ámbito de internet[598].

[598] PRANDINI, Patricia / MAGGIORE, Marcia, *Ciberdelito en América Latina y el Caribe*, Una visión desde la Sociedad Civil, Proyecto Amparo, 2013, pág. 13. [accesible en], www.proyecto amparo. ciberdelito.

Ciberdelito: En argot usamos ese término para designar tales como la destrucción de ficheros informáticos, su robo, difusión de los códigos de acceso a bancos de datos restringidos, etc.[599].

Ciberespacio: Termino de argot informático que se popularizo el escrito William GIBSON y que usamos para referirnos a la realidad imaginaria compartida de Redes de cómputo, también se usa como sinónimo de internet[600].

Cibernética: Rama del aprendizaje que busca integrar las teorías y estudios de la comunicación y control en máquinas y organismos vivos.[601] Término acuñado por un grupo de científicos dirigidos por *Norbert Wiener* y popularizado por el libro de éste *Cybernetics or Control and Communication in the Animal and the Machine* de 1948. Viene del griego *kibernetes*, timonel o piloto, y es la ciencia o estudio de los mecanismos de control o regulación de los sistemas humanos y mecánicos, incluyendo los ordenadores[602].

Cinta Magnética: Sistema de almacenamiento de la información de un ordenador constituido por una cinta de material plástico recubierto por un oxido magnético[603].

Clave: Código de signos convenidos para la transmisión de mensajes secretos o privados[604].

---

[599] Diccionario de informática, Editorial Cultura S.A., Madrid, 2001, pág. 57.

[600] Diccionario de informática, Editorial Cultura S.A., Madrid, 2001, pág. 57.

[601] SANDERS, Donald, *Informática: Presente y futuro*, Editorial Mc Graw Hill, México, 1987, pág. 653.

[602] FERNÁNDEZ CALVO, Rafael…op. cit., pág. 11.

[603] Diccionario de informática, Editorial Cultura S.A., Madrid, 2001, pág. 58.

Cliente: Un programa o computadora que solicita información o servicios de otros programas o computadora (servidor) en una red. Por ejemplo, un *web browser* es un cliente que solicita una página electrónica de un servidor por medio de internet.

Cliente de correo electrónico: Una aplicación de *software* que se conecta a un servidor de correo electrónico para enviar o recibir correos electrónicos. *Outlook*, *windows mail y thunderbird* son algunos ejemplos de los clientes de correo electrónico.

Código fuente o código de objeto: El formato en el que un programador escribe un programa. El código fuente puede ser leído por un humano pero un ordenador no lo puede ejecutar directamente. Se tiene que capturar en un código de objetos que posteriormente podrá leer un ordenador.

Ordenador o computadora: Sistema electrónico que maneja símbolos y está diseñado para aceptar y almacenar datos de entrada, procesarlos y producir resultados de salida automáticamente, bajo la dirección de un programa almacenado de instrucciones detalladas paso por paso[605].

Correo electrónico o *email*: Un método para intercambiar mensajes digitales en internet. Los mensajes pueden ser texto simple o estar formateados y pueden incluir archivos anexos.

Ordenador en nube: La práctica de almacenar y/o procesar datos en recursos que se encuentran interconectados en red como lo son computadoras múltiples

---

[604] FERNÁNDEZ CALVO, Rafael…op. cit., pág. 28.

[605] H. SANDERS, Donald, *Informática: Presente y futuro*, Editorial Mc Graw Hill, México, 1987, pág. 652.

que se encuentran hospedadas con un proveedor externo. La nube tiene beneficios potenciales: es más fácil escalar los recursos, los usuarios no necesitan tener experiencia en la tecnología base y una organización no necesita invertir en infraestructura de cómputo. La computación en nube también tiene desventajas: las organizaciones dan el control de su información y dependen del proveedor de la nube.

***Cookie*[606]:** Un archivo de datos que por lo general coloca un sitio electrónico en la computadora de un cliente para ser utilizado posteriormente. Los datos podrán contener nombres de usuarios, *passwords*[607], actividad de *browser*[608], *o* productos que se hayan adquirido. Cada ocasión posterior que el cliente visite el *website,* de origen, éste lee los datos que se encuentran en la *cookie.* Las *cookies* pueden eliminarse. Las cookies son pequeños archivos de texto que son descargados automáticamente (si está permitido por las reglas de seguridad), al navegar en una página web específica, por ejemplo, para que cada vez que accedamos a una página esté adaptada a nuestro gusto (en un idioma determinado, con ciertos colores, etc.). También sirve para la persistencia de sesiones[609]. Llevar el control de usuarios, cuando un usuario introduce su nombre

[606] Su nombre proviene, pese a su tecnología, de las tradicionales galletas chinas de la suerte, en cuyo interior hay un papel escrito con algún augurio, así surgió la idea de las *cookies*, que hoy también designan en la vida laboral y empresaria a un plan o proyecto con una meta principal, y una meta oculta a largo plazo.

[607] En informática, la palabra *password* significa contraseña, clave, key o llave.

[608] *Browser:* navegador, hojeador, explorador.

[609] Técnicamente, las cookies son trozos de datos arbitrarios definidos por el servidor web y enviados al navegador. El navegador los devuelve al servidor sin modificar, reflejando así un estado (memoria de eventos anteriores) en las transacciones HTTP, que de otra manera serían independientes de ese estado. almacenamiento temporal de información que usan páginas de Internet. Estas cookies son enviadas por páginas web y son almacenadas y administradas por los navegadores de internet. Sin las *cookies,* cada petición de una página web o un componente de una página web sería un evento aislado, sin ninguna relación con el resto de peticiones de

de usuario y contraseña, se almacena una galleta para que no tenga que estar introduciéndolas para cada página del servidor. Sin embargo, una galleta no identifica a una persona, sino a una combinación de ordenadores de la clase de navegador-usuario.

***Cracker**:* Usuario de ordenadores y redes que busca los medios para entrar sin autorización en el sistema de información ajenos y con el fin de extraer de ellos copias ilegales de datos y programas o provocar daños en los mismos[610].

Crackeadas: También craquear, proceso de descubrir contraseña cifrada, por algún medio criptográfico.

Cracking: Es la acción en la cual el sujeto activo luego de introducirse de forma no autorizada en el equipo electrónicos o página web ajena, crea algún detrimento patrimonial mediante el menoscabo de la integridad física o lógica de cualquiera de ellos, sin más motivo que la producción misma del daño[611]

---

otras páginas del mismo sitio. Las *cookies* tienen implicaciones importantes en la privacidad y el anonimato de los usuarios de la web. Aunque las cookies sólo se envían al servidor que las definió o a otro en el mismo dominio, una página web puede contener imágenes y otros componentes almacenados en servidores de otros dominios. Las *cookies* que se crean durante las peticiones de estos componentes se llaman cookies de terceros. Las compañías publicitarias utilizan *cookies* de terceros para realizar un seguimiento de los usuarios, a través de múltiples sitios, es decir de todas las páginas donde ha colocado imágenes publicitarias o web. El conocimiento de las páginas visitadas por un usuario permite a estas compañías dirigir su publicidad según las supuestas preferencias del usuario. [accesible en] www.lawebdelprogramador.com / www.alegsa.com.ar.

[610] RINCÓN, Antonio / PLAGARO Julio, *Diccionario conceptual de informática y comunicaciones*, Editorial Paraninfo, Madrid 1998, pág. 92.

[611] COUTURE, J. Eduardo, *Vocabulario Jurídico* 4ª edición, Editorial Desalma, Buenos Aires, 1991, pág. 45.

Criptografía: Dícese de la ciencia que estudia la forma de codificar y descodificar documentos, de forma que solo puedan ser leídos por la persona que posee la clave de descodificación.

***Cybersquatting* o ciberocupación:** Practica de registrar furtivamente como nombres de dominio marcas conocidas sobre las que no se tienen derecho alguno. El cybersquatting o ciberocupación, es el registro de un nombre de dominio sabiendo que un tercero tiene un interés legítimo en ese dominio con una doble finalidad: una finalidad especulativa, es decir, pedirle una cantidad económica para que ese tercero lo compre, o bien, una finalidad publicitaria para atraer a visitantes y tráfico a la web sirviéndose de la reputación de ese tercero.

Decriptación: es el proceso de regresar el cibertexto a su formato original que puede ser leído *texto sencillo*.

Drive: En informática, drive (drives en plural) es una palabra inglesa que, en informática, se traduce como *unidad*. Es un dispositivo que lee o escribe datos en un medio de almacenamiento como disquetes, discos ópticos, etc. Por ejemplo, unidades de CD o lectograbadora de CD, *DVDs*, *Blu-rays.*

Dirección IP o Dirección del Protocolo de Internet: Una dirección numérica única que se asigna a cada dispositivo en una red IP. Las direcciones se usan para enrutar datos hacia el dispositivo correcto. Hay dos versiones del protocolo que se usa: IPv4 y IPv6.

Disco: En informática se llama disco al dispositivo que sirve para guardar o almacenar información de manera permanente[612].

[612] Diccionario de informática, Editorial Cultura S.A., Madrid, 2001, pág. 91.

Disco duro: Dispositivo de almacenamiento diseñado para permanecer dentro del ordenador, una capacidad mucho mayor y de mayor velocidad que otro, es un disco magnético para el almacenamiento duradero de datos. Suelen ser rectangulares y protegidos por una caja metálica herméticamente cerrada. Actualmente es el método de almacenamiento más extendido en ordenadores de escritorios. Poseen diversas capacidades de almacenamiento que cada vez es más elevada y que actualmente llega a más de 4 terabytes. Otros nombres usados para disco duro: disco rígido, disco duro, hard disk, HD, HDD.

DNS, Sistema de nombres de dominio: El sistema de nombramiento de las computadoras en internet. El sistema se usa para traducir el nombre de dominio de una computadora que puede ser leído por un humano (por ejemplo, google.com) en una dirección IP que utiliza internet para enrutar datos. Los servidores que realizan esta traducción se denominan servidores DNS o servidores de nombres.

E-mail: Es un servicio muy utilizado en internet, que permite el intercambio de mensajes entre usuarios. Se conoce como *electronic mail*, correo electrónico, o abreviado e-mail. El primer e-mail fue enviado en 1971. Para 1996, la cantidad de emails enviados superó a la cantidad de correos postales por primera vez.

Encabezado: Tanto los paquetes IP como los correos electrónicos tienen encabezados. Para un paquete IP: la fuente origen, destino e información de ruteo que se anexan al inicio de un paquete. En el caso de un correo electrónico: la información que se anexa al inicio de todos los correos electrónicos y que contiene información detallada sobre el remitente, la ruta y quien recibe. La mayoría de los encabezados pueden falsificarse parcialmente o por completo.

Encriptación: La práctica de alterar datos matemáticamente para oscurecer su significado, con frecuencia se trata de una medida de seguridad de la

comunicación. La información encriptada es el *cibertexto*. La Decriptación es el proceso de regresar el cibertexto a su formato original que puede ser leído (texto sencillo). La palabra, número u otro valor que se utilice para encriptar/decriptar un mensaje se denomina la *clave*.

Encriptación simétrica de claves: es la forma más tradicional de encriptación en la que se usa la misma clave para encriptar y decriptar el mensaje.

Encriptación asimétrica de claves o encriptación de claves públicas: se utilizan dos claves: una clave *pública* (con frecuencia se publica) y una clave *privada* (se mantiene en secreto). Cualquiera puede usar la clave *pública* de una persona para encriptar datos destinados a una persona. Esa misma clave *privada* de una persona es la única clave que podrá decriptar los datos. La encriptación de claves públicas con frecuencia se utiliza para enviar un correo electrónico de manera segura.

Error 404: (*Page Not Found*, HTTP 404 - Página web no encontrada). El error 404 o *página no encontrada*, es un código de respuesta del HTTP que se muestra cuando un cliente no puede comunicarse con un servidor o cuando el servidor no puede encontrar el recurso que pide el cliente. El error 404 no debe confundirse con el *server not found* o errores similares, donde directamente no existe ningún tipo de comunicación con el servidor.

Espacio de depósito: Las áreas de un medio de almacenamiento (como un disco duro) al final de cada archivo donde pudieran encontrarse fragmentos de archivos previamente eliminados. Por ejemplo, cuando se usa espacio de disco en secciones de 8 kilobytes (KB) (*clusters*), un documento de 8 KB ocupa

exactamente un *cluster*[613]. Si el usuario borra ese archivo, por lo general los datos permanecen intactos hasta que son sobrescritos por otro archivo. Si el usuario escribe un archivo nuevo en un *cluster* que únicamente tiene 5K, los restantes 3K de datos del primer archivo van a permanecer en el disco y un experto los podrá recuperar. Por lo general hay dos tipos de depósitos: depósito de archivo (se describe en el ejemplo) y el depósito de RAM. El depósito de RAM es el espacio innecesario entre el fin de un archivo lógico y el fin de su último sector (Una unidad más pequeña que un *cluster).* Se le denomina depósito de RAM porque los sistemas operativos antiguos llenaban el espacio con datos de la RAM.

Espionaje Informático: El espionaje informático es una especie de delito informático que consiste básicamente en la obtención de información de forma ilegítima, no autorizada, independiente de la finalidad perseguida, desde un sistema de tratamiento de la información[614]. En la doctrina se indica que este delito no requiere un ánimo especial diverso al ánimo real de obtener información no autorizada, cuestión que como se indicó, implica una de las grandes diferencias con el fraude informático, en el cual si se requiere ánimo de lucro y perjuicio patrimonial, en contrario podemos mencionar al autor Español ROMEO CASABONA para quien es esencial que se tenga un ánimo especial en

[613] Bloque de disco. Un *clúster* es la unidad de almacenamiento en un disco con una determinada cantidad fija de *bytes*. Un disco está dividido en miles de clústeres de igual tamaño y los archivos son repartidos y almacenados en distintos clústeres. El tamaño se determina en el formateo del disco y suele ser de 512 bytes. www.alegsa.com.ar

[614] HUERTA MIRADA, Marcelo y LÍBANO MANSSUR, Claudio, *Delitos Informáticos* Editorial Jurídica Conos Sur, 2ª Edición, 1998, pág. 132-133.

materia de espionaje, cual es el de obtener una ventaja de naturaleza económica[615].

***Ethernet**:* Un conjunto de normas de cableado y señalización que se utilizan en redes cableadas.

Etiqueta: Como metadato, una etiqueta o *tag*, es un tipo de información que describe o define algún aspecto de un recurso de información (como un documento, una imagen, una página web, etc). Las etiquetas son un tipo de metadato que capturan conocimiento en forma de descripciones, categorizaciones, clasificaciones, semánticas, comentarios, notas, hiperenlaces o referencias. Las etiquetas permiten capturar relaciones, dependencias, atributos o puntos de vista asociados con un recurso de dato. Las etiquetas son consideradas una expansión de la información en sí mismas, que agregan valor, contexto y significado adicional a la información.

***Extranet**:* Una extensión de la red privada de una organización que tiene el objetivo de compartir información con otras entidades como los proveedores o socios. Una extranet es privada pero puede correr en una infraestructura pública.

Fichero o *file:* En informática, un archivo es un grupo de datos estructurados que son almacenados en algún medio y pueden ser usados por las aplicaciones. La forma en que un ordenador organiza, da nombre, almacena y manipula los archivos se denomina sistema de archivos y suele depender del sistema operativo y del medio de almacenamiento (disco duro, disco óptico, etc).

[615] ROMEO CASABONA, Carlos, *Poder Informático y Seguridad Jurídica*, pág. 141 citado por Claudio MAGLIONA y Macarena LÓPEZ, *Delincuencia y Fraude Informático*, (Derecho Comparado y Ley Nº 19. 223) 1ª edición, Editorial Jurídica de Chile, 1999, pág. 58.

Firewall: Un sistema diseñado para permitir el acceso autorizado pero negar el acceso no autorizado en una red. Un *firewall* puede ser un dispositivo dedicado en una red como una computadora especial entre una red interna corporativa y la internet. Un *firewall* también puede ser un programa en una computadora, por ejemplo Windows Firewall. Una técnica específica de *firewall* es el filtrado de paquetes. El filtrado de paquetes revisa cada paquete de manera individual y lo acepta (le permite pasar) o lo rechaza (lo saca) dependiendo de las reglas. Asimismo, escudo de protección, en el entorno de internet, o las medidas de seguridad que se forman en la red para proteger información, prevenir que los usuarios no causen ningún daño a los sistemas principales o controlas los accesos[616].

GigaByte: Unidad de almacenamiento. Existen dos visiones distintas de gigabyte (GB) dependiendo de la exactitud que se desee. Un gigabyte, en sentido amplio, son 1.000.000.000 bytes (mil millones de bytes), o también, cambiando la unidad, 1.000 megas (MB o megabytes). Pero para más exactitud, 1 GB son 1.073.741.824 bytes o 1.024 MB.

Google: Empresa especializada en búsquedas por internet, publicidad online y gran variedad de productos de software y hardware. Está radicada en *Mountain View, California* (EE.UU.). La misión de Google, en su propia declaración es *organizar la información del mundo y hacerla universalmente accesible y útil.* Fue fundada por Larry PAGE y Sergey BRIN, cuando eran estudiantes en la universidad de *Stanford* el 27 de septiembre de 1998. El nombre *Google*, se origina de *googol*, unidad que representa un "1" seguido de mil ceros.

[616] Muro de Fuego - Cortafuego

GSM o Sistema global de comunicación móvil: Una de las dos normas para el servicio de telefonía celular digital en Estados Unidos. Se trata de la norma dominante en Europa, Japón y Australia y aproximadamente 100 países en el mundo. Los datos del suscriptor GSM se transfieren en un módulo de identidad del suscriptor (SIM, por sus siglas en inglés) que se inserta en el teléfono. Como resultado, el suscriptor tiene la posibilidad de usar la tarjeta SIM para transferir su identidad a un dispositivo nuevo.

Hacker: Persona apasionado de los sistemas informáticos y de las telecomunicaciones, que adquiere una gran destreza en su manejo y en particular, en la navegación por las redes de datos.

Hackers (tipos de hackers): Dependiendo de su motivación y habilidades: *Hacker sombrero negro*: Un hacker dañino que irrumpe para obtener algo ilícito o con propósitos vandálicos; *Hacker sombrero blanco*, se refiere a un *hacker* ético (por lo general un experto en seguridad de redes) que identifica las vulnerabilidades de seguridad para beneficio del público, la industria o la academia; *hacker sombrero gris*, el cual se trata de un *hacker* cuyos objetivos y actividades no son claros; *Joven Script*, alguien que no es experto, pero sin embargo, entra a los ordenadores utilizando solamente *scripts* y herramientas desarrolladas por otros; *Cracker o ladrón de códigos y programas*, término que algunos utilizan para diferenciar a aquellos que tienen intenciones maliciosas de los que tienen objetivos más benignos.

Hacking: Es la acción en la cual un tercereo, no titular de un equipo o un sitio Web determinado, accede al mismo por la utilización de código de programación o *software* específico. En materias de delitos de *hacking,* se les conoce como tal en general a los accesos no autorizados a sistemas de tratamiento de la información por jóvenes fanáticos en la computación y sin mayor tecnología, el

hacking propiamente tal sería este simple acceso no autorizado para satisfacción personal, una especie de logro del *hackers*, pero hay que tener presente que puede darse que este acceso sea con la finalidad de cometer otro delito y se reconduciría conforme a la intención del agente a las otras figuras delictuales ya vistas o bien al fraude.

***Hacktivismo*:** Ataques que se cometen en sistemas de cómputo con objetivos activistas políticos; ocasionalmente sus transgresores los describen como *la desobediencia civil electrónica*.

***Hardware**:* En un sistema, dícese de todo elemento en el que predominan los componentes físicos o materiales. Dicho término en inglés que hace referencia a cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con el ordenador. No sólo incluye elementos internos como el disco duro, CD-ROM, disquetera, sino que también hace referencia al cableado, circuitos, gabinete, etc. E incluso hace referencia a elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos. El hardware contrasta con el software, que es intangible y le da lógica al hardware (además de ejecutarse dentro de éste). El hardware no es frecuentemente cambiado, en tanto el software puede ser creado, borrado y modificado sencillamente.

Hash: Una función matemática que se utiliza para convertir una serie datos en un valor pequeño de tamaño fijo. El término *hash* también se refiere al resultado de dicha función. Las funciones *Hash* están diseñadas para que la probabilidad de que dos conjuntos de datos tengan el mismo valor *hash* sea astronómicamente baja. En el análisis pericial, las *hashes* son útiles porque las que coinciden muestran que dos series de datos son iguales. Las *hashes* se usan como huellas dactilares para identificar los archivos conocidos (es más rápido comparar los valores *hash* de dos archivos que los archivos mismos) y para comprobar que no

haya cambiado un grupo de evidencia (si se compara un valor conocido preciso de *hash* con el valor actual).

Host: Máquina conectada a una red. Tiene un nombre que la identifica, el *hostname*. La máquina puede ser un ordenador, un dispositivo de almacenamiento por red, una impresora, etc. Cualquier tipo de ordenador puede ser uno personal o un servidor, puede ser un *host*, siempre y cuando pueda transmitir paquetes que cumplan con el protocolo de internet.

HTML, **Lenguaje de marcación de hipertexto:** Un lenguaje que se usa para crear páginas *world wide web*. En ingles *hyper text mark-up*, o lenguaje de marcas de hipertexto. Lenguaje desarrollado por el CERN que sirve para modelar texto y agregarle funciones especiales (por ej. hipervínculos). Es la base para la creación de páginas web tradicionales.

HTTP, Protocolo de transferencia de hipertexto: El protocolo que se utiliza para transmitir archivos hacia y desde servidores web.

IMAP, Protocolo de acceso de mensajes en internet: Uno de los dos protocolos más comunes para recuperar correos electrónicos de un servidor.

IMEI, **Identidad internacional de equipo móvil**: Un número de identificación único de cada teléfono GSM.

Indexar: En el contexto de la evidencia digital: el proceso de creación de un mapa que muestra dónde se encuentra cuál información, como el índice de un libro. El valor de esta acción, es que una vez que se dedica tiempo a la creación de un índice, las búsquedas son mucho más rápidas.

Informática: Disciplina técnica y científica dedicada al estudio y procesamiento de información, en particular mediante procedimiento y nociones automáticas. Sinónimo de computación.

Ingeniería social: Un método de *hacking* que no es técnico, donde se llama a personas como el administrador de un sistema o funcionarios de una compañía y se les extrae información útil como los *passwords* o *códigos de cuenta.*

Internet: Podemos hablar acerca de la llamada red de redes o Internet definiéndola como un conjunto de elementos tecnológicos que permite enlazar masivamente redes de diferentes tipos, para que los datos puedan ser transportados de una red a otra red. También se dice que es una red de redes de ordenadores interconectados. La Internet es una red conmutada de paquetes (los datos se transmiten en paquetes) que se basa en una familia de protocolos denominados TCP/IP. Asimismo se puede decir que es sistema que aglutina las redes de datos de todo mundo, uniendo miles de ellas mediante el protocolo TCP/IP. El mayor conjunto que existe de información, personas, ordenadores y *software* funcionando de forma cooperativa. La i mayúscula la diferencia de una internet convencional, que simplemente une varias redes. Al ser única se la conoce también simplemente por la *red*.

Internetwork: Dos o más redes conectadas.

Intranet: Una red privada reservada para ser utilizada por personas internas en una organización. Los ejemplos incluyen redes corporativas y universitarias internas. Aunque las intranets son privadas, éstas usan tecnologías de internet.

IP, Protocolo de Internet: El protocolo que usan todos los *hosts de Internet* para comunicarse entre sí mediante paquetes. La IP, (*Internet Protocol*), es parte del conjunto de protocolos TCP/IP encargada de la interconexión de redes. Es el

fundamento básico y de más bajo nivel de Internet. Es el protocolo responsable del envío de paquetes de información entre dos sistemas que utilizan la familia de protocolos TCP/IP, desarrollados y usados en Internet. El envío de paquetes permite dividir la información en bloques que pueden ser remitidos por separado y después reagrupados en su destino.

Input*: (*Entrada Salida avanzada Prorammable Controlador de entrada), sistema de entrada de información. Entrada/Salida. En ocasiones, los dispositivos o controladores de entrada y salida de datos se describen con su nombre inglés o con las siglas «I/O» en lugar de «E/S»

ISP, Proveedor de Servicios de Internet: Un proveedor que brinda acceso a internet (por ejemplo, América Online, Comcast, Verizon). Los ISPs ocasionalmente también ofrecen un grupo principal de utilidades y servicios de internet como el correo electrónico, hospedaje del sitio electrónico personal y acceso a *Usenet*.

JPEG o JPG: Un método de compresión de imágenes, un archivo en ese formato o la extensión de archivo de dicho archivo. El acrónimo se refiere al nombre del comité que creó la norma, el Grupo Conjunto de Expertos Fotográficos.

Keylogger: Registrador de teclas, programa informático que registra todas las pulsaciones que se realizan sobre un teclado para ser guardadas en un archivo o para ser enviadas por internet. El fin de un keylogger puede ser malicioso porque quién lo instala puede hacerlo de forma oculta y lograr así, saber todo lo que se escribe sobre el teclado. Incluso hay programas malignos como troyanos, virus o gusanos que pueden incluir un keylogger para sus fines.

LACNIC, Registro de Direcciones de Internet Latinoamericano y del Caribe. LACNIC es el Registro Regional de Internet (RIR) para Latinoamérica y el Caribe.

LAN, Red de área local: Una red de ordenadores distribuidas en un área física pequeña como edificio de oficinas o una casa.

Link*:* Dícese del programa cuya misión es asegurar la conexión entre dos programas principales.

Linux: Sistema operativo que posee un núcleo del mismo nombre. El código fuente es abierto, por lo tanto, está disponible para que cualquier persona pueda estudiarlo, usarlo, modificarlo y redistribuirlo. El término Linux se utiliza para describir al sistema operativo tipo Unix que utiliza filosofías y metodologías libres y que está constituido por la combinación del núcleo Linux con las bibliotecas y herramientas del proyecto GNU[617], además de otros proyectos libres y no libres.

Memoria ram (ROM): (*Read Only Memory*) o Memoria de sólo lectura. ROM es un tipo de memoria no volátil usada en computadoras y otros dispositivos electrónicos. Los datos almacenados en una memoria ROM no pueden ser modificados o, en ocasiones, sólo pueden ser modificados lentamente y con dificultad. Por esto son muy usadas en el *firmware* o *software* que está estrechamente ligado al hardware y no necesita actualizaciones frecuentes o en el software de cartuchos. Estrictamente hablando, las memorias de sólo lectura se refieren a las memorias que están soldadas al hardware, que no pueden cambiarse

[617] Sistema operativo completamente libre, el sistema GNU, es un acrónimo recursivo que significa *GNU No es Unix*. El sistema GNU fue diseñado para ser compatible con UNIX, un sistema operativo que no es libre.

ni sacarse. Tampoco pueden actualizarse ni arreglarse errores que se detecten luego.

Metadata, metadatos: En el sentido más amplio, los metadatos son datos sobre otros datos. En el peritaje de sistemas de cómputo, con frecuencia se refiere a la información sobre un elemento o hallazgo clave. Los ejemplos incluyen la creación, modificación, fechas y hora de acceso de un archivo; permisos y propiedad de un archivo y la ubicación del archivo.

MODEM: Dispositivo que modula y demodula señales transmitidas sobre medios de comunicación de grados de voz.

Motor de búsqueda: Un motor de búsqueda es una pieza de software, accesible a todos los usuarios de la web, que les permite localizar los sitios relacionados con una palabra clave. Un usuario, por ejemplo, puede pedir conocer los sitios que en su descripción contengan las palabras *Derecho penal*, el motor de búsqueda devolverá entonces una lista de todos los sitios que presenten referencias a esos vocablos.

Negación de servicio distribuido o Ataque DDoS: Un ataque a la red en el que se utilizan múltiples sistemas (con frecuencia son muchos) para desbordar el ancho de banda o recursos de una víctima para así desactivarlo o bloquearle su comunicación con el resto de la red.

Nombre de dominio: Una dirección que puede ser leída por un humano que se expresa en un texto que representa un lugar en Internet. Nombre único que permite ingresar a un servidor sin saber la dirección IP exacta donde se encuentra. Asimismo se puede decir que es un conjunto de letras (dos o más caracteres) que determinan el ámbito o país de una página web. Por ejemplo, los

dominios *.es* pertenecen a España, los *.com* a sitios comerciales, los *.org* a organizaciones, etc.

Olfateador de paquetes: El software equivalente al dispositivo de intervención telefónica que se usa para monitorear el contenido del tráfico de paquetes en una red. Las autoridades de procuración de justicia y los hackers utilizan los olfateadores de paquetes. Después de irrumpir en un *host* de una red y conseguir los privilegios raíz, con frecuencia un hacker instala programas de olfateo de paquetes para conseguir los pares de nombre de usuario / password de los usuarios que se conectan con otros *hosts.* (Esto da al *hacker* un medio fácil para entrar y aprovechar esos otros *hosts.)*

OS, Sistema operativo: Software de computación que administra funciones básicas como la administración de archivos y entradas y/o salidas (por ejemplo, acciones del teclado o del *mouse;* pantalla y sonidos). Los ejemplos de sistemas operativos son Windows, MacOS y Linux.

Página Web: Resultado en hipertexto o hipermedia que proporciona un navegador del *WWW* después de obtener la información solicitada. Su contenido puede ir desde un texto corto a un voluminoso conjunto de textos, gráficos estáticos o en movimiento, sonido, etc. Algunas veces el citado término es utilizado incorrectamente en orden de designar el contenido global de un sitio web, cuando en ese caso debería decirse sitio web.

Pharming*:* Explotación de una vulnerabilidad en el software de los servidores DNS (*Domain Name System*) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio, a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de

internet a la página web que el atacante haya especificado para ese nombre de dominio.

***Password*:** Palabra clave, dícese del conjunto de caracteres ordenados de una forma específica que el ordenador nos va a requerir para poder acceder al proceso siguiente o para poder entrar dentro de una base de datos[618].

Phreaking: Consiste en el acceso no autorizado a sistemas telefónicos para obtener de manera gratuita el uso de las líneas, con el objeto de lograr conexión mantenida por esta vía a las redes informáticas, ya sean nacionales o internacionales.

***Phreaking* telefónico**: Aprovechar las debilidades de la red telefónica, por lo general, para conseguir gratuitamente servicios de llamadas de larga distancia o de conferencia. En el pasado, cuando la mayoría de los usuarios tenían acceso a otras computadoras mediante módems de marcación, frecuentemente también se producía el hacking y phreaking ya que el phreaking permitía a los hackers ocultar mejor su identidad y conectarse a computadoras distantes sin costo.

Phishing: En cuanto a esta modalidad delictual se puede resumir que se conoce como tal al robo de datos personales, el lograr obtener datos de terceros sin derecho para ello usando diversas modalidades tecnológicas, siendo generalmente el envío de correos electrónicos, envió de páginas *web* falsas que hacen creer al destinatario que están operando en páginas legítimas y por ende entrega información que en otro caso no entregaría, información que es usada con fines o intereses económicos, ya que generalmente es para fraudes, esto es, lograr usar dichas claves para obtener un enriquecimiento patrimonial ilegítimo . Dentro de este concepto amplio de robo de datos podemos incluir dos nuevas

[618] Diccionario de informática. Ed. Cultura S.A., Madrid, 2001. p.123.

modalidades que han surgido con el avance de la tecnología y análisis de los casos más frecuentes, a saber, el llamado *Pharming,* esto es, la modificación fraudulenta que se efectúa en el sistema computacional de *resolución de nombres,* es decir, la manipulación al proceso de conversión de un nombre a una dirección IP lo que permite el desvío del usuario a una página *web* falsa y obtener así sus datos e información necesaria para efectuar fraude, y la otra técnica es la conocida como *Vishing,* en que la obtención fraudulenta de datos personales se efectúa mediante una combinación de técnicas de envío de *mail* fraudulentos con llamados telefónicos o mensajes de texto, a fin de hacerle creer al usuario que es estrictamente necesaria la modificación o revisión de sus datos para evitarse un perjuicio patrimonial y lograr que ingresen a páginas falsas y obtener ilícitamente la información necesaria.

Ping: Una herramienta de la red que se utiliza para probar si está disponible un *host* remoto en una red. El ping envía una solicitud de eco y escucha al *host* remoto para que le envíe una respuesta de eco. También se puede usar en un ataque de negación de servicio si se inunda a la víctima con solicitudes de eco - *ping.*

Programas de acceso remoto: que permiten el acceso de un tercero a su ordenador para un posterior ataque o alteración de los datos.

Protocolo: Un conjunto de normas para intercambiar datos en la red. Los *hosts* en internet se comunican mediante el Protocolo de Internet.

Procesador: En informática puede referirse a al *procesador digital llamado* CPU (Unidad Central de Proceso) y el *procesador el DSP* (Procesador digital de señal). También pueden referirse a *tipos de programas informáticos* que procesan algo, por ejemplo: los procesadores de texto.

Puerto: En informática, un puerto puede hacer referencia a, *puerto de datos* o *puerto de red.* El primero puede se refiere a interfaz, por la cual pueden enviarse o recibirse datos. Esa interfaz puede ser física o de software. Si es física pueden ser, por ejemplo un puerto USB. Si es de *software*, puerto de navegación http, puerto de IRC, etc. El segundo puesto interfaz para comunicar programa a través de una red. Por otro lado, vale señalar que técnicamente es un número que significa un canal discreto de comunicación en la red. Un solo ordenador puede distinguir entre múltiples conexiones simultáneas de la red asignando a cada una un número de puerto virtual que va de 0 a 65,535. Algunos números de puerto se consideran puertos bien conocidos con asignaciones estándares, por ejemplo, el puerto 80 se usa para el protocolo de transferencia de Híper Texto (HTTP, por sus siglas en inglés), el puerto 25 se usa para el protocolo de transferencia sencilla de correo (SMTP, por sus siglas en inglés) y el puerto 110 se usa para el protocolo *post office* (POP, por sus siglas en inglés). En algunas situaciones, una aplicación usa un puerto no-estándar para evadir las medidas de seguridad.

Puerto USB: Puerto para que transmite a gran velocidad la información entre los periféricos y la computadora. USB, significa en inglés *Universal Serial Bus*, Soporta transferencias de 12 MBps. Un sólo puerto USB permite ser usado para conectar más de 127 dispositivos periféricos como ratones, módems, teclados, impresoras, etc.

P2P, Peer-to-peer: Cualquiera de los varios tipos de red donde un ordenador actúa como cliente y servidor simultáneamente (los ordenadores actúan como iguales). Las redes P2P tienden a ser más robustas que las configuraciones tradicionales cliente-servidor, porque las redes P2P están descentralizadas. También tienden a ser más eficientes y escalables porque se usan los recursos de todos los participantes (poder del ordenador, espacio de almacenamiento y ancho

de banda). Los ejemplos de las redes P2P incluyen *BitTorrent, Gnutella y FastTrack.*

RAM, Memoria de acceso aleatorio: Una forma de almacenaje de datos en una computadora. Por lo general es mucho más rápido acceder datos en RAM que en el disco duro, entonces es más probable que los datos que usa actualmente un ordenador sean almacenados en la RAM.

Red: En informática, es el conjunto de ordenadores, dispositivos de procesos de datos y aplicaciones que se encuentran conectados entre sí.

Red de *robots o Botnet*: Un grupo de robots que opera en coordinación, de manera autónoma o automática. Por tradición, era más probable que el término hiciera referencia a un grupo de robots IRC. Ahora, por lo general se refiere a un grupo de computadoras programadas para correr códigos maliciosos aunque éstas por lo general se controlan mediante IRC. A una persona que se dedica a controlar a remoto una red de robots se le denomina *pastor de robots* o robot maestro.

Robot: Un programa que corre una tarea automatizada. Diferentes tipos de robots realizan diferentes tareas; por ejemplo, los robos de telaraña acceden y analizan información en sitios electrónicos y los *chatterbots* (Robots de plática) responden preguntas y enunciados sencillos en inglés en ambientes de chateo en línea. Los robots también pueden cometer actividades dañinas como participar en ataques de negación de servicio, fraude *click* o spam. El término es la abreviatura de robot y ocasionalmente también se usa para hacer referencia al ordenador que corre el programa.

Rogue antivirus (Rogueware) – Es un software que aparece como beneficioso desde una perspective de seguridad pero que provee limitada o ninguna

capacidad de seguridad, generando un significativo número de erróneas o engañosas alertas, o intenta convencer al usuario de participar en transacciones fraudulentas a través de técnicas de ingeniería social.

Ruteador: Un dispositivo que conecta múltiples redes. El ruteador envía datos de una red a otra. Por ejemplo, un ruteador podrá conectar una red doméstica o una red corporativa a internet. Muchos ruteadores también tienen funciones de filtrado y registro en bitácora.

Sabotaje Informático: En forma general está constituido por aquellas conductas que atentan contra la integridad de un sistema de tratamiento de información o de sus partes componentes, su funcionamiento o de los datos contenidos en él. Este delito afecta el soporte lógico del sistema, caso contrario, si se afecta el soporte material no estamos hablando de un delito informático sino simplemente de un delito común de daño. Dentro de las modalidades usadas para el sabotaje informático se pueden indicar, entre otras las de *crash programs*, que son programas que afectan los soportes lógicos de un sistema de información generalmente en forma reiterada en el tiempo y con distancia espacio-temporal, como son las *bombas lógicas*, programas que se insertan a los sistemas de tratamientos de la información para que bajo una condición o en un tiempo determinados se activen y produzcan la destrucción del mismo, surgió esta técnica generalmente por los mismos fabricantes de los programas computacionales como una forma de asegurar el pago de sus derechos y la no utilización en caso de incumplimiento, pero a nivel doctrinario en el mundo se ha discutido la validez de esta técnica cuando es usada por el propietario ya que implica el hacerse justicia por propia mano.

Server: Servidor. Término con el que se descarga al ordenador o la aplicación que se encarga de suministrar información u otros recursos a aplicaciones del

cliente que se conecta a él. Los servidores de la red y servidores de correo electrónico son dos tipos comunes de servidores.

Servidor *proxy:* Son otra forma de navegar anonimamente. Consiste en armar un pasadizo (*gateway)*, entre el equipo o la red local y la red de Internet. Normalmente se usan para filtrar las solicitudes de un usuario, a través de un cortafuego (*firewall*) que intercepta todas las peticiones y las resulve para dar la navegacion al cliente. El proxy espera la petición en el cortafuegos y la envía al servidor remoto en el exterior del cortafuegos, interpreta la respuesta y la envía de vuelta al cliente. En la práctica todos los clientes en una subred salen a través del mismo proxy, este sirve como servicio de caché[619], de documentos que son pedidos por muchos clientes. Con esto se reduce el coste de tráfico de red ya que los peticiones más frecuentes son recuperadas desde el caché local una vez que la petición inicial ha sido hecha. De este modo un servidor proxy se asemeja a un anonimizador, ya que es él el que recupera las páginas *web*, en lugar de la persona que está navegando. Sin embargo, presentan una serie de limitaciones frente a los anonimizadores: No impiden que las cookies se sigan almacenando en el disco duro del usuario. Todas las visitas quedan registradas en el proxy. La dirección IP del servidor proxy contiene el nombre de dominio.

Servidor autorizado o *Proxy:* Un servidor que actúa como la pieza intermedia para que una computadora acceda a recursos de otro servidor. Se utilizan con

[619] En informática, un caché es un componente que almacena datos para que los futuros requerimientos a esos datos puedan ser servidos más rápidamente. Generalmente son datos temporales. La idea de duplicación de datos se basa en que los datos originales son más costosos de acceder en tiempo con respecto a la copia en memoria caché. Los datos almacenados en un caché pueden ser valores que se han computado recientemente o duplicados de valores almacenados en otro lugar. Si se solicitan los datos contenidos en el caché, estos son servidos rápidamente; de lo contrario, los datos deben ser recomputados o tomados de su ubicación original, lo cual suele ser más lento. Un caché almacena datos de forma transparente, esto significa que un cliente que requiere los datos de un sistema, no sabe de la existencia del caché. http://www.alegsa.com.ar.

propósitos de eficiencia, seguridad y anonimato. Un *proxy* puede acelerar el procesamiento de solicitudes de *web* al capturar las respuestas de tal forma que no se necesita que una solicitud completa llegue hasta el servidor verdadero cada vez que un cliente solicita una página. En un contexto corporativo, es posible utilizar un *proxy* para mantener el anonimato de sus máquinas por razones de seguridad. Una persona también puede usar un *proxy* para ser anónima al cometer actividades ilícitas.

Servicio de hospedaje o *hosting* de la Red: Un servicio que almacena y ofrece conectividad a internet que permite a otros dar un sitio electrónico. Los tipos de hospedaje de la red - *web hosting* incluyen un hospedaje dedicado donde un sitio electrónico tiene un servidor (o servidores) dedicado, el hospedaje compartido cuando hay más de un sitio electrónico (dominios) hospedado en el mismo servidor, el hospedaje de co-ubicación cuando el servicio únicamente proporciona la energía y la conectividad a internet y hospedaje de páginas electrónicas personales cuando un usuario crea una página personal en un sitio electrónico de servicios como Facebook y MySpace.

Sistema informático: Un sistema informático es la síntesis de hardware, software y de un soporte humano. Un sistema informático típico emplea un ordenador que usa dispositivos programables para almacenar, recuperar y procesar datos.

Sistema informático: Conjunto de programas fundamentales, sin los cuales no sería posible hacer funcionar el ordenador con los programas de aplicación que se desee utilizar. Sin el sistema operativo, el ordenador no es más que un elemento físico inerte. Todo sistema operativo contiene un supervisor, una biblioteca de programación, un cargador de aplicaciones y un gestor de ficheros. *MS-DOS, Windows, Linux y Macintosh* son los más conocidos, pero hay muchos

más. Es un software que actúa de interfaz, entre los dispositivos de *hardware* y los programas usados por el usuario para manejar un computador. Es responsable de gestionar, coordinar las actividades y llevar a cabo el intercambio de los recursos y actúa como estación para las aplicaciones que se ejecutan en la máquina.

SIM, Módulo de identidad del suscriptor: Una tarjeta inteligente que se inserta en un teléfono móvil para identificar al suscriptor en la red. Una tarjeta SIM almacena una identidad internacional de suscriptor móvil del usuario (IMSI). Una tarjeta SIM por lo general se puede cambiar de un teléfono a otro.

Sitio: Por lo general es la abreviatura de sitio electrónico.

***Software**:* Conjunto de elementos de un sistema informático, como programas, reglas y procedimientos informáticos, los programas de ordenador, la lógica que permite realizar tareas al hardware (la parte física).

Spam: Inundar. Acción consistente en enviar gran cantidad de información a Usenet, enviar un artículo a un gran número de grupos inapropiados o mandar a un IRC grandes cantidades de texto con el objeto de interrumpir las conversaciones todo con tus propios mensajes.

SSL, **Capa de *Sockets* Seguros**: Un protocolo criptográfico que brinda seguridad e integridad de datos para la comunicación en la red. Muchos sitios electrónicos usan el protocolo para transmitir y recibir información confidencial del usuario como los números de tarjeta de crédito. Por ejemplo, en URL https://www.quicken.com/products, "https" indica una conexión segura. TLS es el sucesor de SSL.

Técnica del salami: Fraude informático consistente en efectuar numerosas transacciones monetarias en cantidades pequeñas por canales electrónicos, con el fin de evitar su detección o su fiscalización pos los organismos oficiales[620] .

Terminal: en informática, término que se usa para determinar el conjunto de una pantalla y un teclado en el que se muestran e intercambian informaciones cuando se encuentra conectado a un sistema central[621].

TLS, Seguridad en la Capa de Transporte: Un protocolo criptográfico que brinda seguridad e integridad de datos para propósitos de comunicación en las redes. Muchos sitios y páginas electrónicas (Web sites) usan el protocolo para transmitir y recibir información confidencial del usuario como números de tarjetas de crédito. Por ejemplo, en la URL https://www.quicken.com/products, "https" indica una conexión segura. TLS es la sucesora de SSL.

TLD, Dominio de alto nivel: La sección a la extrema derecha de un nombre de dominio como *.com, .net, .org, or .edu*. Los TLDs (genéricos) no se relacionan con ninguna ubicación geográfica específica, a diferencia de los ccTLDs (código de país). Los ejemplos de estos últimos incluyen .es (España), .fr (Francia), y .ru (Rusia). Nota: El hecho de que un dominio indique una relación con un lugar geográfico no significa que su servidor tenga que encontrarse físicamente en ese mismo sitio.

Trashing: Se refiere a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por

[620] RINCÓN, Antonio / PLAGARO Julio, *Diccionario conceptual de informática y comunicaciones*, Editorial Paraninfo, Madrid, 1998, pág. 360.

[621] Diccionario de informática, Editorial Cultura S.A., Madrid, 2001, pág, 320.

la persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas.

TOR: Es una tecnología que permite a los usuarios comunicarse de manera anónima. Se trata de una red de anonimato que enruta la comunicación por medio de servidores autorizados múltiples *proxies* múltiples, cada uno con una capa independiente de encriptación. TOR es sumamente eficaz en lo que hace, sin embargo, tiene varias debilidades. Por ejemplo, TOR encripta datos mientras estos pasan por la red TOR, pero no puede encriptar datos entre la red TOR y su destino final, entonces es posible escuchar indebidamente la información. De igual manera, teniendo visibilidad del tráfico entrante y saliente de la red TOR, es posible correlacionar los dos flujos de tráfico mediante el análisis de tráfico para relacionar a un usuario con su actividad. Se sabe que la sigla TOR significa *el ruteador de cebolla*, por sus capas múltiples de criptografía.

Unix: Sistema operativo utilizado originariamente en grandes sistemas informáticos a los que tienen acceso simultaneo gran cantidad de usuarios. Hoy en día existen multitud de variantes que se adaptan a todo tipo de equipos informáticos. Linux es su variante gratuita y de código abierto. Debido a que fue diseñado para funcionar en red, es el sistema operativo más difundido en servidores conectados a Internet.

URL, Localizador Uniforme de Recursos: Una dirección que especifica dónde se encuentra un recurso de red y cómo accederlo. Un ejemplo sencillo es *http://www.google.com/index.html*. Por lo general un URL tiene el siguiente formato: protocolo, *host*, puerto (opcional), trayectoria hacia el archivo, consulta (opcional), ancla (opcional). Esta dirección, permite acceder a un archivo recurso como ser páginas, html, php, asp, o archivos gif, jpg, etcétera. Se trata de una cadena de caracteres que critica cada recurso disponible en la *www*, es decir

cuando se solicita la URL, en un formulario web, lo que se está pidiendo esa dirección de un sitio e incluso la dirección un perfil de usuario, como podría ser por ejemplo Facebook.

Ventana emergente: En informática, una ventana emergente es cualquier tipo de ventana que aparece en la pantalla luego de iniciar un programa, una página web, al hacer clic sobre algún botón o enlace, etc. También llamadas *pop-up* que es un tipo de ventana *web* que aparece delante de la ventana de un navegador al visitar una página web. Suelen ser molestos porque obstruyen la vista, especialmente cuando se abren múltiples ventanas tipo pop-up. Suelen utilizarse para publicidad online.

Virus: Programas informáticos que tienen por objeto interferir con el hardware y/o con los sistemas operativos del ordenador causando daños en el mismo, la mayoría de los virus son irreparables[622].

***WAP*, Punto de acceso inalámbrico**: Un dispositivo que permite a otros dispositivos inalámbricos tener acceso a una red. Por ejemplo, dispositivos inalámbricos en una casa podrán conectarse a un *wap* que a su vez se conecta a un ruteador y luego a internet. El *wap* y ruteador con frecuencia están integrados.

Web: Término que se utiliza para referirse de forma abreviada a la world wide web[623].

Web browser o Browser: Un programa (por ejemplo, Firefox; Internet Explorer; Safari) que se utiliza para buscar y mostrar páginas electrónicas desde sus respectivos *web hosts.*

[622] Diccionario de informática, Editorial Cultura S.A., Madrid, 2001, pág. 347.

[623] Diccionario de informática, Editorial Cultura S.A., Madrid, 2001 pág. 351.

Web Page: Página Web, dícese del documento HTML situado en el world wide web, en el que figuran diversos enlaces de hipertexto con otros documentos del Web situados en enlaces distintos[624].

WWW, *World Wide Web*: El sistema de documentos hipervinculados que se acceden en Internet. El término se refiere a las páginas interconectadas y sus contenidos pero también se utiliza, incorrectamente, para referirse a toda la internet. Igualmente, se puede explicar como medio de divulgación de datos, creado por el CERN la cual reconoce alguna solicitud en términos simples, gracias a los enlaces de hipertexto, es decir los diferentes estilos, imágenes, sonidos y videos, los cuales están insertados en el texto por el autor. Con ello el usuario puede ingresar a Internet movilizarse dentro de la red, es decir navegar usando múltiples servidores.

[624] Diccionario de informática, Editorial Cultura S.A., Madrid, 2001, pág, 351.