Escuela de Graduados

Trabajo final para optar por el titulo de:

Maestría en Derecho Penal y Procesal Penal

“Criterios Generales del Derecho Comparado para catalogar los delitos de alta tecnología en la República Dominicana”.

Sustentante:

Massiel Victoria Pichardo Bido

2008-1511

Asesora:

Varleny I. Díaz Payano, MA

Santo Domingo, D. N.

Diciembre, 2014.

INDICE

ANEXOS.-

I. Anteproyecto de trabajo final; septiembre 2014.
II. Glosario.
III. Entrevista.

LISTA DE TABLAS

1. **Capítulo I – Conceptos generales, antecedentes y tratamiento de los delitos de alta tecnología.**

2. **Capítulo II- Categorización de los delitos de alta tecnología.**

LISTA DE FIGURAS

1. **Capítulo I – Conceptos generales, antecedentes y tratamiento de los delitos de alta tecnología.**

2. **Capítulo II- Categorización de los delitos de alta tecnología.**

RESUMEN

La ley No. 53-07, sobre crímenes y delitos de alta tecnología, es la norma que regula los delitos de esta especie en la República Dominicana. Sin embargo, esta ley no ha establecido los parámetros bajo los cuales se ha realizado la categorización de los delitos que la misma sanciona. Esta situación aunada a la creciente aparición de conductas denominadas, en el derecho comparado, como delitos de alta tecnología motivó la presente investigación. El objeto de la misma es analizar los criterios extraídos del derecho comparado que puedan utilizarse en el marco de la ley 53-07, para catalogar los delitos de alta tecnología en la República Dominicana. Tras el análisis exhaustivo de legislación y doctrina extranjera se realiza la presentación de una propuesta de criterios sencillos que permiten reconocer la presencia o ausencia de los delitos de alta tecnología. Los resultados presentados no solo constituyen nuevos criterios de reconocimiento y división, sino que se va más allá presentando tipos penales pasibles de ser incluidos en nuestra legislación. Los ilícitos presentados son extraídos de trabajos e investigaciones de campos científicos como la ingeniería e informática por lo cual se hizo necesario demostrar, mediante el empleo de la teoría del delito, que las conductas identificadas bajo los criterios propuestos cumplen con los elementos necesarios para ser catalogadas como delitos de alta tecnología.

DEDICATORIAS

Este trabajo final está dedicado a principalmente a **Dios**, que es el motor y dueño de mi vida. Por nunca desampararme a lo largo del camino y guiarme por el mismo. Por darme la fuerza y la fe necesaria para continuar cada día, superar los obstáculos y permitirme conocer a ángeles que han alumbrado mi vida.

A mi madre **Santa Lucia Bido**, por su apoyo incondicional y soporte. A mi hermana **Ninoska L. Pichardo**, licenciada en derecho.

Al **Ing. Pablo Iván Rojas Mora**, por acompañarme durante todo el proceso de selección de tema y elaboración de este proyecto.

A todos aquellos que de una u otra forma han confiado en mí y a los cuales no pretendo defraudar.

AGRADECIMIENTOS

Agradezco de forma muy especial a la **Lic. Varleny I. Díaz Payano**, por su asesoría y compromiso con este proyecto. Sin dudas una mujer preparada, competente y digna de admiración, que asumió junto a mí este ultimo reto. Gracias a sus correcciones, aportes y opiniones hoy tengo en las manos un trabajo final que me llena de orgullo.

Al **Ing. Pablo Iván Rojas Mora**, mi novio, por su apoyo incondicional.

A mis compañeros de maestría, Lauren Vargas, Filda Carolina Noboa, Julio Aybar, Maryori Hernández, Zaida Vásquez, Tania Valentín, Mairene, Félix Heredia, William Encarnación, Osiris Blanco, Víctor Suarez, Alexis Santil, Rafael de los Santos, Gegorit, Bernardina, Scarlet Lockart, Robinson Lebrón y José Altagracia. Todos ellos profesionales admirables y amigos incondicionales, con quienes compartí los miércoles y viernes de los últimos dos años. Gracias por estar presente en aquellos momentos difíciles y por provocar grandes momentos de felicidad.

Debo hacer un apartado especial para dos grades amigas, **Ángela de los Santos Ramón** y **Gregoria A. Motero**, quienes fueron testigo de todo el trabajo y esfuerzo dedicado en este proyecto y con las cuales comparto los resultados de dicho esfuerzo. ¡Gracias chicas!

A nuestros maestros y mentores, por compartir sus conocimientos con cada uno de nosotros y por hacer, en cada encuentro, el mayor de los esfuerzos para empujarnos cada día a ser mejores profesionales.

A **Abnel García** por su asistencia técnica y colaboración para este trabajo final. Gracias por poner tu sello en él.

INTRODUCCIÓN

En los últimos años la tecnología ha experimentado un desarrollo vertiginoso. Cada día se descubren un sin número de posibilidades y aplicaciones científicas que van separando el ayer del mañana. Las ciencias en su conjunto más amplio, las artes y la humanidad se han visto permeadas por la alta tecnología o "*hig-tech*", lo cual nos ha vuelto dependientes y hasta cierto punto vulnerables. En definitiva los avances tecnológicos han facilitado nuestras vidas en innumerables formas, sin embargo, como cualquier herramienta esta depende del uso que se le dé y más aún, del sujeto que la posea y su intención.

Desde hace más de una década hemos observado cómo la tecnología, una herramienta tan poderosa, ha servido de base para la comisión de una serie de delitos. En principio sirvió como canal; tal es el caso de las clonaciones de tarjetas de crédito por medios electrónicos; sin embargo hoy el canal se ha convertido en el delito mismo, por ejemplo en los casos de sabotaje donde se altera o maltrata un sistema electrónico.

La ley General de las Telecomunicaciones No.153-98 del 27 de mayo de 1998, representa el primer antecedente legislativo en materia de alta tecnología. Esta ley estatuía la obligación de respetar la inviolabilidad de las telecomunicaciones y prohibía su uso cuando fuera contrario a las leyes y las buenas costumbres. Sin embargo, esta norma se circunscribía a las telecomunicaciones estrictamente, dejando a un lado una serie de ilícitos penales especializados que hasta ese momento no podía ser juzgado. En atención a esta situación y con la creciente globalización nace ley No. 53-07, sobre Crímenes y delitos de alta tecnología. Esta norma cuenta con un amplio glosario con los términos esenciales que son tocados en la ley y define de forma restringida el sentido en el cual estos deben interpretarse. En su estructura esta ley cuenta con un segundo título, donde se enuncian los crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información, los delitos de contenido, los

delitos de propiedad intelectual y afines, los relativos a las telecomunicaciones y los crímenes y delitos contra la nación y actos de terrorismo.

A nivel sustantivo esta ley recoge conducta genéricas tratando de abarcar de una forma absoluta actividades especificas. La clasificación empleada por la ley, la división realizada por esta y las definiciones que la misma emplea revela su carácter estático, lo cual va encontrar del dinamismo imperante en el ámbito tecnológico. De igual forma la ley no explica bajo qué criterios ha sido realizada la división de los delitos que la misma sanciona. La ausencia de un criterio efectivo para la categorización de los delitos de alta tecnología es evidente en el cuerpo de la ley, pues no se explica cuales estándares han sido tomados en cuenta para la identificación de estos ilícitos.

El objeto del presente trabajo final es analizar los criterios extraídos del derecho comparado que puedan utilizarse en el marco de la ley 53-07, sobre crímenes y delitos de alta tecnología, para catalogar los delitos de alta tecnología.

La investigación propuesta acerca de los delitos de alta tecnología tiene su origen en una serie de casos que se han venido suscitando, en los cuales el medio común es la tecnología y el uso de la misma. Al revisar algunos de estos casos nos encontramos con una serie de hechos cuyas características y elementos nos lanzan hacia un nuevo modo de operación delictivo, donde los elementos constitutivos de los delitos comunes han cambiado.

Al adentrarnos a la busqueda de un concepto de delitos informáticos, nos encontramos con el aportado por Téllez Valdés, J. (citado por Landa Duran, 2007) quien define los delitos informáticos como: “Conductas típicas, antijurídicas y culpables, en las cuales las computadoras pueden ser el instrumento o el fin”. (P. 233). Sin embargo, el gran aporte de este autor no radica en la definición que nos brinda, sino en la calasificación que realizó de los delitos de alta tecnología al dividir los mismos acorde a su uso como instrumento o como objeto.

De igual forma la investigacion se sustenta en un analisis critico de la ley No. 53-07, sobre crimenes y delitos de alta tecnologia, la cual define en su art. 4 el delito de alta tecnologia como: “Aquellas conductas atentatorias a los bienes jurídicos protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Se entenderán comprendidos dentro de esta definición los delitos electrónicos, informáticos, telemáticos, cibernéticos y de telecomunicaciones”.

Partiendo de la doctrina estudiada y con apoyo en el marco legislativo existente en la materia, se pretende ofrecer de forma sencilla los criterios generales que existen en el derecho comparado para catalogar a los delitos de alta tecnologia, con la finaliodad de adaptar los mismos a nuestra realidad existente y de este modo catalogar de forma efectiva esta clase de delitos.

En cuanto al aspecto metodológico, debemos resaltar que la presente investigación tiene un carácter aplicado, debido a que su finalidad será el ejercicio práctico de los conocimientos adquiridos. Una vez identificados los criterios de categorización de los delitos de alta tecnología contaremos con los parámetros necesarios para establecer cuando una conducta nueva constituye un ilícito de esta especie. A partir de la identificación y recolección de la documentación e información escrita existente sobre el tema de estudio se presenta de forma estructurada los aspectos más relevantes en materia de ciberdelitos. El análisis comparado y descriptivo empleado nos permitió reseñar los parámetros establecidos en legislaciones y doctrina extranjera para la división de los delitos de alta tecnología.

Como parte de las técnicas empleadas para la obtención de la información se utilizaron la recopilación documental y la entrevista. La primera técnica no presento ningún tipo de dificultad, pues consistió en la búsqueda, identificación, lectura y análisis de la información relevante para la investigación. La segunda técnica empleada, consistente en la aplicación de una entrevista estructurada a profesionales seleccionados en las áreas de la informática, la ingeniería en sistemas y el derecho, no arrojo los resultados esperados. Todo esto debido a que

la información obtenía a partir de la misma resulto de poca relevancia y hasta cierto punto no lleno las expectativas requeridas a nivel técnico para nuestra investigación. Las interrogantes planteadas en la entrevista fueron respondidas con el auxilio de la doctrina y marcos legislativos.

A nivel estructural este trabajo final tiene una división funcional que nos permite presentar el contenido de una forma ordenada y sintetizada en dos capítulos. El primer capítulo recoge de forma práctica los principales conceptos presentados a nivel doctrinal de los delitos de alta tecnología, presentando a seguidas los principales antecedentes históricos de los mismos y el tratamiento que se les ha dado tanto a nivel nacional como internacional. El segundo capítulo presenta los principales criterios de categorización de los delitos de alta tecnología, extraídos del derecho comprado. Este ultimo capitulo presenta una propuesta de clasificación de esta clase de delitos enumerando los criterios que deben tomarse en cuenta para ello y analiza desde la perspectiva de la teoría del delito dos nuevas clase de delitos.

CAPÍTULO I

CONCEPTOS GENERALES, ANTECEDENTES Y TRATAMIENTO DE LOS DELITOS DE ALTA TECNOLOGÍA.

1.1 ANTECEDENTES Y CONCEPTO DE LOS DELITOS DE ALTA TECNOLOGÍA.

1.1.1 ANTECEDENTES DE LOS DELITOS DE ALTA TECNOLOGÍA.

El origen y evolución de la tecnología está directamente ligado al desarrollo del ser humano y las necesidades del mismo al momento de crear formas para satisfacerse. En la medida en que las sociedades inician los procesos de mutación social, económica y cultural, asimismo cambian sus necesidades, inquietudes y conocimientos, lo cual impulsa a la ciencia de manera progresiva al borde de sus límites.

A nivel conceptual, la palabra “tecnología” es un término amplio que abarca un conjunto de técnicas, conocimientos y procesos, los cuales sirven para el diseño y construcción de objetos a los fines de satisfacer necesidades humanas. El Diccionario de Informática y Tecnología Alegsa (2014) señala que la palabra tecnología proviene del griego tekne (técnica, oficio) y logos (ciencia, conocimiento). La Universidad de Castilla-La mancha , 2014 en publicaciones de su Escuela de Ingenieros Industriales, plantea de forma interesante la concepción de la tecnología y la evolución de la misma. Estos refieren como punto focal del desarrollo de la tecnología al siglo XVIII, específicamente el año 1777, donde Johann Beckmann, profesor de la Universidad de Gotinga, publicó un texto en el cual describía esta palabra como: “Una curiosa unión de una rica sabiduría y un conocimiento técnico.”

El diccionario de la Real academia de la Lengua Española[1] presenta varias acepciones sobre el término tecnología, destacándose las siguientes:

1. Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico.
2. Tratado de los términos técnicos.
3. Lenguaje propio de una ciencia o de un arte.
4. Conjunto de los instrumentos y procedimientos industriales de un determinado sector o producto.

La tecnología ha sido asociada a aéreas especificas del conocimientos o ciencias con el objeto de aplicar los caracteres de la misma a las ciencias a intervenir. La información y la comunicación es una de las áreas que más ha sido permeada por la tecnología, esto debido al carácter de continuidad y dinamismo que la misma requiere. Orti, C. explica que, no existe una única definición sobre la Tecnología de la Información y Comunicación, comúnmente conocida como "Las TIC´s" asegurando que: "Las TIC se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las telecomunicaciones. Las TIC's son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido,...)". Cabero, J. (citado por Orti, C.) en su obra recoge las principales características de las TIC´s, listando las siguientes: inmaterialidad, interactividad, interconexión, instantaneidad, digitalización, innovación y sobre todo penetración a todos los sectores (culturales, económicos, educativos, industriales, entre otros).

El nivel de impacto de las TIC´s se refleja de forma directa en todos los ámbitos y trasciende las fronteras. La interconexión y la instantaneidad, en ocasiones, dificultan el seguimiento y conocimiento de las mismas. Sin duda alguna el manejo de la información y procesamiento rápido y efectivo de la misma es una necesidad actual de las sociedades modernas, sin embargo, ¿Son las TIC´s siempre sinónimos de avance y progreso? ¿Qué efectos traen consigo estas nuevas tecnologías? ¿Podrían las TIC´s tener implicaciones negativas?

[1] El *Diccionario de la lengua española* (*DRAE*) es la obra de referencia de la Academia. La última edición es la 23. ª, publicada en octubre de 2014.

Todas estas interrogantes pudieron ser el motor para que el Derecho Penal intentara responder las mismas. Nuestro derecho por tradición es escrito y a medida que pasa el tiempo se consolida y va tomando fuerza, contrario a la tecnología cuyo cambio es constante e inminente. Autores como Gamba J. (2010) explican la evolución del vínculo entre el derecho como ciencia y las tecnologías de la información, señalando de una forma concisa, los tipos de vinculo que se dan entre estas. Bajo este contexto social y tecnológico, con características especiales, es donde surgen los delitos de alta tecnología o delitos informáticos. El delito per se es una conducta reconocida que va en contra de la ley y las buenas costumbres y a razón de esto el derecho penal, visto como ciencia estudia y reconoce este tipo de conductas haciendo que las mismas puedan ser pasibles de una sanción penal.

El origen de los delitos de alta tecnología, como todo hecho inherente al ser humano, está íntimamente ligado al desarrollo del hombre y a los avances tecnológicos que están a su disposición. Bien podríamos asegurar que existe una relación directamente proporcional entre los avances tecnológicos y los delitos de alta tecnología, a diferencia de los delitos comunes donde los medios y objetivos de comisión son los mismos. Los delitos de alta tecnología son altamente mutables y van siempre un paso a delante.

En principio esta clase de delitos fueron vistos y estudiados a partir de una óptica económica, debido al medio en el cual se desarrollaban. La historia de los delitos informáticos se relata a partir de casos aislados de ilícitos penales cometidos a través de medios informáticos o alta tecnología. Según Manjarres, I. y Jiménez F. (2012) “Los primeros estudios empíricos del delito informático o delito vinculado a la informática se llevaron a cabo a partir de mediados de los años 70, aplicando métodos científicos de investigación criminológica. (P. 73)

(Cotrina, 2009) Presenta una síntesis de los casos más importantes en materia de delitos informáticos, dentro de los cuales menciona:

- El caso de Jhon Draper comúnmente conocido como "Capitan Crunch". El nombre vino a raíz de que Draper descubrió como duplicar la intensidad de la frecuencia de 2600 hz de una línea de WATS, mediante el premio que venía en la caja de cereal de Capitan Crunch, lo cual le permitía hacer llamadas telefónicas gratis.

- Bill Gates y Paul Allen dos de los nombres más importantes e influyentes en la tecnología, softwares, sistemas operativos y equipos de computación, durante sus años universitarios se dedicaron a hackear softwares.

- Kevin Mitnick es otro de los nombres claves en la historia de los delitos informáticos. En 1980 este joven burlo la seguridad del sistema informático de su colegio con el objeto de alterar sus notas. Luego de este suceso, Mitnick junto a dos de sus amigos perpetraron las instalaciones de la compañía COSMOS (Computer Systems for Mainframe Operations), para entonces violentar una base de datos utilizada por la mayor parte de las compañías telefónicas norteamericanas para controlar el registro de las llamadas, con el objeto de obtener manuales y claves de acceso de las sucursales de esa empresa.

- Los sistemas de seguridad de la Casa Blanca, el Pentágono y BellSouth Corp. categorizados como impenetrables fueron penetrados por Ian Murphy, conocido como "Captain Zap". La finalidad de estos actos no estaba más lejos del terrorismo y la peligrosidad que el termino delito infiere, pues Murphy solo dejo su curriculum en la base de datos de estos sistemas.

Cassou Ruiz, J. (2009) indica que, en materia de delitos informáticos, los Estados Unidos de Norteamérica ha sido pionero. A nivel legislativo se presento la primera propuesta de ley en 1977 por el senador Ribicoff en el Congreso Federal. En 1983 en la ciudad de Paris, Francia, la OECD[2] organizo un comité de expertos con el objeto de discutir a fondo las nuevas conductas delictivas relacionadas con las computadoras, así como la necesidad de actualización de las leyes vigentes en ese aspecto.

El Octavo Congreso Criminal de las Naciones Unidas celebrado en el año 1990 y la Conferencia de Wurzburgo, en Alemania en el año 1992 fueron escenarios donde diferentes comités discutieron estos temas. En 1996 el Comité Europeo para los Problemas de la Delincuencia convoca a varios expertos en el tema de los delitos informáticos.

Tal y como señala Cassou Ruiz, J. (2009) los ezfuerzos de estas comisiones condujeron a que el 23 de noviembre de 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 un docuemnto hoy conocido como "Convenio de Budapest, sobre delitos informáticos". El objeto fundamental de este convenio era armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático. Asi mismo proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas, y establecer un régimen dinámico y efectivo de cooperación internacional.

[2] La Organización para la Cooperación y el Desarrollo Económicos (OCDE), fue fundada en 1961, agrupando a 34 países miembros y su misión es promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo. La OCDE ofrece un foro donde los gobiernos puedan trabajar conjuntamente para compartir experiencias y buscar soluciones a los problemas comunes.

1.1.2. CONCEPTO DE LOS DELITOS DE ALTA TECNOLOGIA.

Conocer los orígenes y antecedentes de los delitos de alta tecnología nos ha permitido observar los diferentes ámbitos en os cuales estos se pueden desarrollar y las diversas formas que pueden adoptar. De este modo vemos como el nombre del ilícito cambia según el país, la legislación y el área afectada. Esta mutabilidad y capacidad de adaptación de estos delitos especiales imposibilita la unificación de un concepto sobre los mismos.

Faz, J. (s. f.) Describe en su investigación como en principio los países trataron de ajustar los delitos informáticos dentro de los tipos penales ya conocidos por el derecho común. Sin embargo el medio y la especialidad con que los mismos son cometidos revelo la necesidad de identificar tipos penales especiales y establecer una norma adecuada para la regulación y posterior sanción de los mismos.

El primer reto que presentan estos delitos especiales es el establecimiento del término adecuado. En la República Dominicana nuestra legislación reconoce esta clase de delitos bajo el nombre de “Delitos de alta tecnología”, Sin embargo, la doctrina y legislaciones extranjeras reconocen términos como “Delito informático” “Ciberdelitos” “Cibercrimen” “crímenes por computadora”, pudiendo en ocasiones usar los términos indistintamente.

Autores como, Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014) advierten una clara diferencia entre los términos delito informático y ciberdelitos, aduciendo que para los primeros es necesario valerse de elementos informáticos, sine embargo los segundos hacen referencia a una posterior generación delictiva vinculada a las TIC en el que intervienen la comunicación telemática abierta, cerrada o de uso restringido.

La definición que se plantea sobre los ciberdelitos supone una concepción internacional, estos es en atención a los componentes del delito mismo. Es evidente que un suceso o ilícito internacional exige un procedimiento más

extenso, sistemático y sobretodo la cooperación internacional para la persecución de los mismos por su carácter transnacional.

Faz, J. aclara que no existe una definición concreta sobre lo que son los delitos informáticos, sin embargo reconoce la labor de Téllez Valdez al citar sus palabras:

> No es labor fácil dar un concepto sobre delitos informáticos, en razón de 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, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún.

Esta expresión, tomada de su libro "Derecho Informático" de 1996, revela la condición especial en la cual aparecieron los delitos informáticos. Debemos destacar que la afirmación de Téllez Valdés, se produjo en un contexto social y jurídico en el cual aun no existían las leyes especiales adjetivas con las cuales contamos en el día de hoy.

A lo largo de su investigación Faz J. (s. f.) expone el punto de vista de varias figuras y las consideraciones de las mismas sobre esta clase de ilícitos. Sarzana, C. es uno de los autores mencionados, para este, los crímenes por computadora comprenden: "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo".

Partiendo de esta idea (Sánchez) establece su propio concepto al definir delitos informáticos como: "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático".

Cassou Ruiz, J. (2009) expone un concepto global de delito informático, explicando que por este se entiende: “Toda aquélla conducta ilícita susceptible de ser sancionada por el derecho penal, consistente en el uso indebido de cualquier medio informático”. (P. 217)

Esta definición supone en primer término una generalidad absoluta y precisa que la misma sea analizada. Al utilizar la expresión “cualquier medio informático” el autor cubre los canales actuales y futuros, lo cual hace que la definición sea perdurable y aplicable en el tiempo. No obstante, el concepto resulta ser impreciso dejando subsistir ambiguedades en la materia, pues no se precisa o delimita lo que es un medio informático.

La Organización para la Cooperacion y Desarrollo Economico (OCDE) define los delitos informáticos como: “Cualquier conducta, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos”. Esta definición parte de un marco internacional y la generalidad de la misma permite que se adapten diferentes conductas o sea ampliado con delitos o conductas especiales. El término “cualquier conducta no ética o no autorizada” abre una brecha que solo puede ser llenada por la legislacion especial de cada pais, pues la etica resulta ser muy subjetiva y depende de la cultura.

Paulino J. (2007) asegura que: “El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, estafa, sabotaje, etcétera. Sin embargo, la intervención de técnicas informáticas en su cometida, han revelado la necesidad de ser puntuales en su categorización y respectiva sanción”.

Callegari, Nidia (Citado por Acurio del Pino S., 2008) define al delito informático como: “Aquel que se da con la ayuda de la informática o de técnicas anexas”. Para esta lo que configura el delito informático es el medio y no el objeto del mismo.

Téllez Valdés (citado por Paulino J. 2007) ofrece el concepto de delito informático en forma típica y atípica, entendiendo por la primera: “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin” y por las segundas “actitudes ilícitas en que se tienen a las computadoras como instrumento o fin”. Es importate destacar como Téllez Valdés aborda el concepto desde dos perspectivas, una como medio y otra como fin. Existen delitos en los cuales el delito no es el canal sino el objeto en si mismo.

Paulino J. (2007) define delito de Alta Tecnología como: "Aquellas conductas atentatorias a los bienes jurídicos protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Se entenderán comprendidos dentro de esta definición los delitos electrónicos, informáticos,telemáticos, cibernéticos, y de telecomunicaciones". Ésta definición intruduce un nuevo término “bien juridico protegido”, con el cual se hace referencia al objeto de protección de la ley. En atención a la diversidad de bienes jurídicos protegidos y los delitos que a su vez pueden vulnerarlos, se hace necesario cubrir de forma general todos aquellas que nuestra legilación enuncie.

Otro de los términos utilizado por los autores para referirtse a los delitos de alta tecnologia es el denominado abuzo informático. Ruiz Vadillo (citado por Acurio del Pino S., 2008) indica que abuso informático es: “todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos”. Esta definición hace referencia un término distinto pero similar en cuanto al contenido, pues trata en esencia de hechos contrarios a la ley en el campo de la informatica y el tratamiento de datos.

Rodriguez, D. (citado por Acurio del Pino S., 2008) define al delito informático como: “La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software”. En este concepto puede verse como se

empiezan a insertar componentes y terminos utilizados en la informatica para especificar y delitmitar este tipo de delitos. Los términos hardware y software aluden a la parte externa e interna, respectivamente, de los diferentes componentes tecnológicos.

El término “Ciberdelito” es uno de los conceptos empleados por autores como Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014) quien explica que:

> Se entiende por “ciberdelito”1 o “cibercrimen” cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito. (p. 211)

Todos estos conceptos hacen referencia al delito en si mismo, sin embargo ninguno menciona el componente activo o sujeto que comete la acción propiemente dicha. Campoli, G. (citado por Cassou Ruiz, J., 2009) señala que:

> Los delitos informáticos son aquéllos 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 indebida de medios informáticos, agrega que delitos electrónicos o informáticos electrónicos, son una especie del género delitos informáticos, en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad de los equipos electrónicos y la intimidad de sus propietarios. (p. 217)

Esta definicion no solo menciona al tipo penal en si, sino que toma en consideracion los actores que intervienen en el mismo. Identificar los autores que intervienen en este tipo de delitos permite presentar nuevas caracteristicas de estos ilicitos, pues no solo se tiene un medio especial para la comision de los mismo, sino que los sujetos no son los que conocemos comunmente en los delitos tradicionales.

1.1.3 SUJETOS DE LOS DELITOS DE ALTA TECNOLOGÍA.

En los delitos informáticos intervienen dos sujetos: el sujeto activo que realiza la acción y el sujeto pasivo que la recibe. En este sentido Manjarres, I. y Jiménez F. (2012) refiere sobre el sujeto activo lo siguiente:

> Las personas que cometen los "delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Asimismo Edwin Sutherland, criminólogo norteamericano, (citado por Manjarres, I. y Jiménez F. 2012) advierte que: "El sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional".

El reconocido criminólogo norteamericano, Sutherland, E. (citado por (Sánchez), resalta que la definición de los delitos informáticos es de acuerdo al sujeto activo y no entorno al interés protegido como ocurre en los delitos convencionales que conocemos. Asimismo señala que, generalmente, el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por factores comunes como la pobreza, la carencia de recursos o la poca educación. Este autor compara los sujetos activos de los delitos informáticos con los denominados "delitos de cuello blanco".

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. En primer término tenemos

que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros. (Manjarres, I. y Jiménez F. 2012).En términos generales podría asegurarse que el sujeto pasivo es quien recibe o sufre la acción.

La ley 53-07 sobre Crímenes y Delitos de Alta tecnología también reconoce los sujetos que intervienen en este tipo de delito. El artículo 4 establece, dentro amplio glosario, lo siguiente:

- Sujeto Activo: Es aquel que intencionalmente viole o intente violar, por acción, omisión o por mandato, cualquiera de las actuaciones descritas en la presente ley. A los fines de la presente ley se reputa como sujeto activo a los cómplices, los cuales serán pasibles de ser condenados a la misma pena que el actor principal de los hechos.

- Sujeto Pasivo: Es todo aquel que se sienta afectado o amenazado en cualquiera de sus derechos por la violación de las disposiciones de la presente ley.

De igual forma la ley hace una distinción sobre el "usuario" a los fines de evitar el uso indiscriminado entre los términos usuario y sujeto activo. La ley define usuario en su artículo 4 al usuario como: "Persona física o jurídica que adquiere de manera, legítima bienes o servicios de otra".

1.2TRATAMIENTO DE LOS DELITOS DE ALTA TECNOLOGÍA EN EL ÁMBITO DEL DERECHO COMPARADO.

Ante el constante proceso de globalización presente en los países del mundo, la continua evolución de los medios de información y la permeabilidad de los mismos, los Estados se dieron cuenta de que solo mediante la adopción de una legislación adecuada, especial y actualizada acorde a los nuevos tiempos podría

combatirse el aumento de la ciberdelincuencia y los continuos delitos informáticos o de alta tecnología. Sin embargo todas las normas y leyes por adecuadas y actuales que pudieran ser no serian suficiente para frenar un fenómeno transnacional como lo es la ciberdelincuencia, por lo cual se hizo necesario la cooperación internacional y el compromiso mutuo de las naciones del mundo.

El convenio sobre la ciberdelincuencia del Consejo de Europa, celebrado en Budapest, el 23 de noviembre del año 2001, es el instrumento internacional más importante en materia de delitos de alta tecnología y ciberdelincuencia. Los Estados miembros del consejo de Europa y los demás estados signatario de dicho convenio plantean desde su preámbulo él un marcado interés en intensificar la cooperación entre los Estados participantes en atención a la necesidad de aplicar, a nivel internacional, una política penal común sobre ciberelincuencia.

> Convencidos de que el presente convenio resulta necesario para prevenir 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, mediante la tipificación de esos actos, tal y como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable.

Como se ve en el párrafo anterior los Estados firmantes reconocen una necesidad y ante todo se comprometen a buscar las herramientas pertinentes (en este caso códigos y leyes adjetivas) para la solución efectiva del problema planteado.

Para la elaboración del convenio de Budapest fueron tomados en cuenta el Convenio de Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales del año 1950, el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas de 1966 y otros tratados internacionales aplicables en materia de derechos humanos, a los fines de que el

objeto de cada uno de ellos y los derechos contenidos en los mismos se viera reflejado dentro de la nueva herramienta.

A nivel estructural el convenio contiene cuatro capitulo dentro de los cuales se recoge de forma ordenada los artículos en los cuales se plasma a nivel general el compromiso de los Estados firmantes. El primer capítulo abarca las definiciones técnicas presentes en el convenio a los fines de que las mismas sean interpretadas en ese sentido. Sin embargo, estas definiciones son resultan ser limitativas para una materia tan especial como es la ciberdelincuencia. La terminología a emplear es técnica por lo cual debería incluirse un glosario adjunto donde se establezca el concepto general por el cual se deberán entender estos términos dentro del convenio.

El segundo capítulo menciona las medidas que deberán adoptarse a nivel nacional. Este capítulo traza la pauta para que los Estados que efectivamente desee formar parte puedan establecer de forma sustantiva en códigos o leyes adjetivas las conductas que en lo adelante se entenderían como delitos especiales.

Tabla No. 1. Derecho penal sustantivo.

Derecho Penal Sustantivo	Delitos
Título 1 Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.	Artículo 2 Acceso ilícito
	Artículo 3 Interceptación ilícita

	Artículo 4 Atentados contra la integridad de los datos
	Artículo 5 Atentados contra la integridad del sistema
	Artículo 6 Abuso de equipos e instrumentos técnicos
Título 2 Infracciones informáticas	Artículo 7 Falsedad informática
	Artículo 8 Estafa informática
Título 3 Infracciones relativas al contenido	Artículo 9 Infracciones relativas a la pornografía infantil
Título 4 Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines	Artículo 10 Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

Fuente: Elaboración propia, a partir del Convenio Sobre la Ciberdelincuencia del Consejo de Europa, celebrado en Budapest, el 23 de noviembre del año 2001.

El quinto título del convenio sobre ciberdelincuencia se compone de tres artículos, en los cuales se hace alusión a la tentativa, la complicidad, la responsabilidad de las personas jurídicas y sus respectivas sanciones y medidas.

El tercer capítulo contiene un apartado completo sobre la cooperación internacional enunciando de forma explícita los principios generales relativos dicha cooperación. El art. 23 del convenio enuncia lo siguiente:

> Las partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.

Como se puede apreciar este convenio obliga a que los Estado participantes en el mismo adopten de forma activa medidas contra los delitos informáticos y la ciberdelincuencia, sin embargo no todos los países poseen un marco legislativo nacional con el derecho penal sustantivo indicado en el convenio.

El 28 de enero del año 2003, en la ciudad de Estrasburgo, los Estados Miembros del Consejo de Europa y los demás Estados partes del convenio sobre

ciberdelincuencia de Budapest presentaron un protocolo complementario relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. Sobre la base de la cooperación internacional y la finalidad de unidad entre los Estados, se busca adicionar de forma integral diferentes mecanismos que permitan a los mismos la lucha efectiva contra la propaganda racista y xenófoba existente. El derecho a la libertad de expresión y el abuso de los sistemas informáticos como canales o medios para la realización de actos de índole racista y discriminatoria, son parte de las consideraciones que los Estados ponderaron al momento de estructurar el protocolo adicional.

Es importante destacar que la intención o finalidad del protocolo no es limitar o menoscabar el derecho a la libre expresión que existe, sino crear compromisos con los Estados miembros para que estos encaminen políticas penales a la erradicación del mal uso de los sistemas informáticos. El art. 1 del protocolo establece la finalidad del mismo al reconocer que:

> La finalidad del presente Protocolo es completar, entre las Partes en el Protocolo, las disposiciones del Convenio sobre la Ciberdelincuencia, abierto a la firma en Budapest el 23 de noviembre de 2001 (en lo sucesivo denominado “el Convenio”), por lo que respecta a la tipificación penal de los actos de índole racista y xenófoba cometidos mediante sistemas informáticos.

El convenio sobre ciberdelincuencia firmado en Budapest no contempla de forma específica los actos de racistas o de xenofobia. En atención a esto el art. 2 del convenio establece lo que debe entenderse por “material racista y xenófobo” explicando que:

> Todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que propugne, promueva o incite al odio, la discriminación o la violencia, contra cualquier persona o grupo de personas, por razón de la raza, el calor, la ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores.

De igual forma este protocolo establece en sus capítulos subsiguientes las medidas que los Estados suscribiente debe tomar a nivel interno en torno acciones como:

- Difusión de material racista y xenófobo mediante sistemas informáticos.
- Amenazas con motivación racista y xenófoba.
- Insultos con motivación racista y xenófoba.
- Negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.
- Cooperación y complicidad.

Todas estas acciones tienen como factor común el racismo y la xenofobia, la cual constituye la causa y motor de las mismas. En estas acciones se utiliza como medio o canal los sistemas informáticos con el objeto de difundir, propagar o encubrir actitudes de racismo y xenofobia.

El capítulo III del protocolo establece la relación que el mismo guarda con el convenio sobre ciberdelincuencia de Budapest, señalando los artículos que deben ser adaptados. El art. 8 dispone que: "Los artículos 1, 12, 13, 22, 41, 44, 45 y 46 del Convenio se aplicarán, *mutatis mutandis*[3], al presente Protocolo". Esta disposición permite cambiar los aspectos necesarios en los artículos que se señalan a fin de que los mismos formen parte integral del convenio y pueda interpretarse de esta forma.

[3] Cambiando lo que se deba cambiar. *Diccionario de la lengua española* (*DRAE*), 23ª, 2014. Consultado en fecha 28 del mes de octubre del año 2014 en: http://lema.rae.es/drae/?val=mutatis+mutandis

Tabla No. 2. Legislación internacional en materia de delito de alta tecnología.

País	Legislación
Estados Unidos	Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986
Alemania	Ley contra la Criminalidad Económica del 15 de mayo del año 1986
Gran Bretaña	Computer Misuse Act (Ley de Abusos Informáticos)
Argentina	No existe una legislación especifica
Holanda	Ley de Delitos Informáticos, de fecha 1ro de marzo del año 1993
Francia	Ley relativa al fraude informático de enero de 1988
España	Código penal español
Chile	Ley contra delitos informáticos del 7 de junio del 1993
Perú	Ley N° 27.309, promulgada el 15 de julio de 2000 y publicada el 17 de julio de 2000, se incorporaron los delitos informáticos al Código Penal.

Fuente: Elaboración propia, a partir de la legislación vigente en los países listados.

1.3TRATAMIENTO DE LOS DELITOS TECNOLÓGICOS EN LA LEY NO. 53-07, SOBRE CRÍMENES Y DELITOS DE ALTA TECNOLOGÍA (LCDAT).

La Constitución de la República Dominicana como ley sustantiva define la función primaria del Estado y el marco dentro del cual debe desarrollarse la misma. El artículo 8 de la Constitución enuncia que:

> Es función esencial del Estado, la protección efectiva de los derechos de la persona, el respeto de su dignidad y la obtención de los medios que le permitan perfeccionarse de forma igualitaria, equitativa y progresiva, dentro de un marco de libertad individual y de justicia social, compatibles con el orden público, el bienestar general y los derechos de todos y todas.

El párrafo anterior deja claramente establecido el deber de garantía que tiene el Estado dominicano sobre aquellos derechos fundamentales listados a partir del art. 37 de nuestra Carta Magna. Dentro de los derechos fundamentales a ser protegidos se encuentran: el derecho a la vida, el derecho a la dignidad humana, derecho a la igualdad, derecho a la libertad y seguridad personal, entre otros. Tomando en consideración estos derechos el Estado dominicano se ve en la necesidad de asegurar el disfrute efectivo de los mismos y en consecuencia buscar los mecanismos y herramientas adecuadas para dicha protección.

La tecnología, los sistemas de información y comunicación han servido como medio para la vulneración de ciertos derechos fundamentales, por lo cual el Estado ha debido legislar en ese sentido.

La Ley General de Telecomunicaciones No. 153-98, del 27 de mayo del año 1998, constituyó la primera normativa a nivel nacional que trataba de forma directa los ilícitos en el ámbito de la tecnología. Dentro del objeto de esta ley puede evidenciarse, en su artículo 3ro, el establecimiento a groso modo de la prohibición del mal uso de las telecomunicaciones. La ley operó de manera uniforme en todo el territorio nacional, siendo el marco referencial jurídico para los ilícitos en materia de telecomunicaciones. Sin embargo, tal y como su objeto lo indica, el carácter comunicacional de ésta ley es predominante.

El artículo 2 de la ley 153-98 establece el alcance de la misma:

> La presente Ley constituye el marco regulatorio básico que se ha de aplicar en todo el territorio nacional, para regular la instalación, mantenimiento y operación de redes, la prestación de servicios y la provisión de equipos de telecomunicaciones. La misma deberá ser interpretada de conformidad con los convenios internacionales ratificados por la República Dominicana y se complementará con los reglamentos dictados por las autoridades competentes.

Como puede observarse en la parte infine de este articulo los convenios internacionales ratificados por la República Dominicana y los reglamentos dictados por las autoridades competentes cubrían de forma magistral aquellos vacios o ambigüedades que contenía la ley.

A partir del capítulo III de la ley se establecen los principios generales de la misma, dentro de los cuales resaltan:

> Art. 5. Secreto e inviolabilidad de las telecomunicaciones. Las comunicaciones y las informaciones y datos emitidos por medio de servicios de telecomunicaciones son secretos e inviolables, con excepción de la intervención judicial de acuerdo al derecho común y a lo dispuesto por las leyes especiales. Los prestadores de servicios públicos de telecomunicaciones deberán velar por dicha inviolabilidad, y no serán responsables de las violaciones cometidas por usuarios o terceros sin su participación, culpa o falta.
>
> Art. 6. Uso indebido de las telecomunicaciones. Se prohíbe el uso de las telecomunicaciones contrario a las leyes o que tenga por objeto cometer delitos o entorpecer la acción de la Justicia.

Ambos artículos reseñan conductas punibles y pasibles de sanción penal. En atención a estas situaciones se establece dentro de la misma normativa en el capitulo XIII las faltas y sanciones para en materia de telecomunicaciones. Las faltas que la ley tipifica y reconoce fueron clasificadas en: Faltas muy graves, faltas graves y faltas leves.

Asimismo, la ley establece de forma genérica cuales son los sujetos responsables de las faltas que la misma indica posteriormente y los hechos punibles en cada caso. De este modo el artículo 103 expresa lo siguiente:

> a. Quienes realicen actividades reguladas por las disposiciones legales vigentes en materia de telecomunicaciones sin poseer la concesión o licencia respectiva;
>
> b. Quienes, aún contando con la respectiva concesión o licencia, realicen actividades en contra de lo dispuesto en la presente Ley;
>
> c. El usuario de los servicios de telecomunicaciones, por la mala utilización de dichos servicios, así como por su empleo en perjuicio de terceros.

Los títulos III y IV de la ley disponen las sanciones y las medidas precautorias que deben aplicarse a las faltas establecidas.

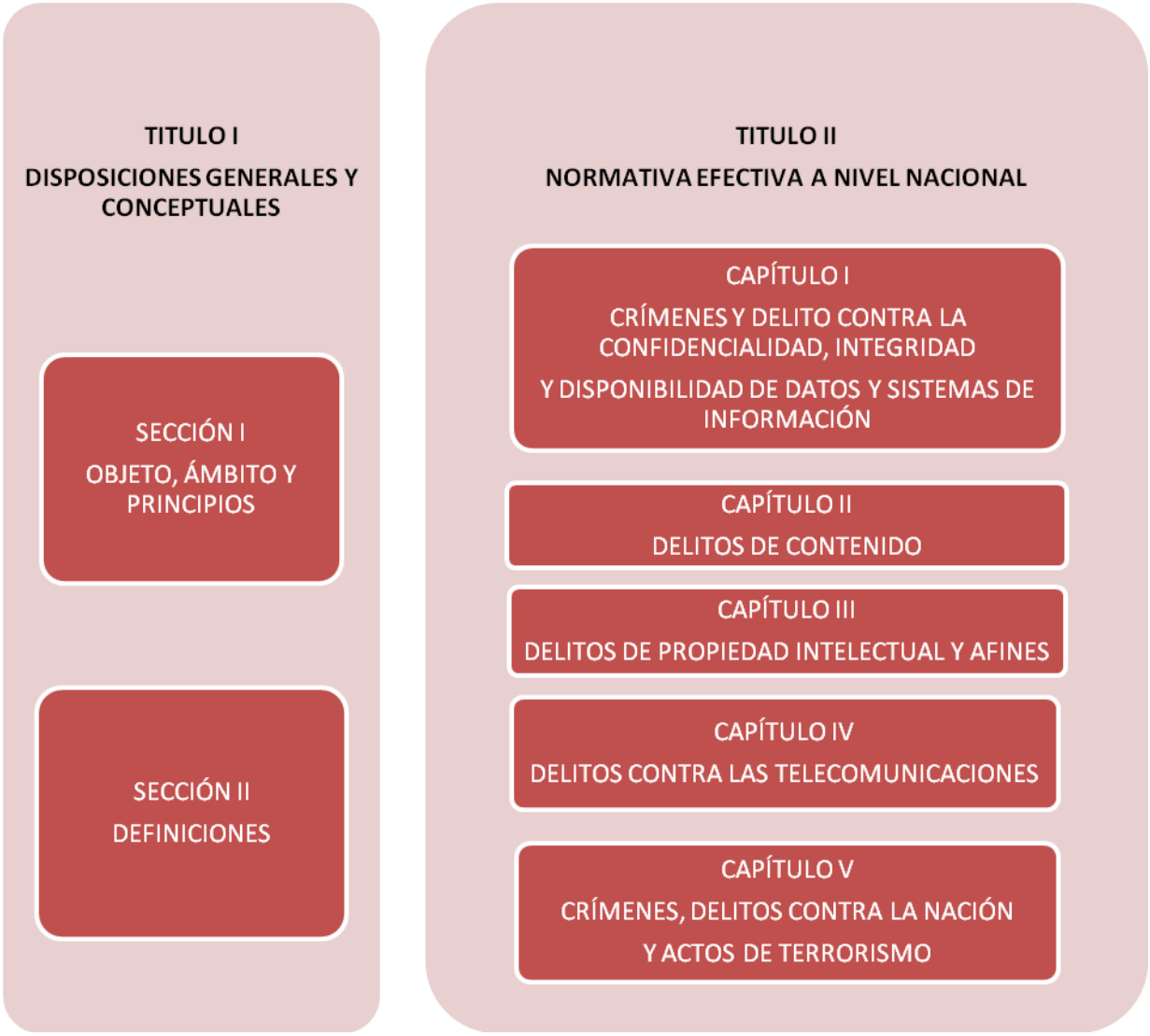
La ley 153-98, ley general de telecomunicaciones es un marco regulatorio que, como su nombre lo indica, fue concebida por el legislador para regular los aspectos que se relacionaban con el ámbito de las telecomunicaciones y la tecnología, sin embargo la misma no abarca ni trata otra clase de delitos de alta tecnología por lo cual surge la siguiente interrogante: ¿Hasta qué punto la globalización y los nuevos avances tecnológicos permitirían que nuestra legislación en esta materia permaneciera intacta?

El avance vertiginoso e impresionante de la tecnología, la globalización, y el acceso a la información que predomina en esta era han contribuido de forma sustancial al desarrollo de nuevas conductas ilícitas en el ámbito de la tecnología y los sistemas de información. Los crímenes y delitos de alta tecnología son el producto directo de un nuevo cambio en el medio de comisión de los delitos.

Ante esta situación surge en nuestro ordenamiento jurídico la necesidad de un marco legal que abarcara los nuevos crímenes y delitos relacionados a las nuevas tecnologías que no estaban considerados en la antigua ley No. 153-98.

Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, de fecha 23 del mes de abril del año 2007, es la norma que tiene por objeto la protección integral de los sistemas que utilicen tecnología de la información y comunicación. A nivel estructural esta ley se compone de 67 artículos agrupados en tres (03) títulos que a su vez se subdividen en varias secciones y capítulos.

Figura No. 1. Estructura y organización de los delitos de alta tecnologia en la ley No. 53-07.



Fuente: Elaboración propia, a partir de la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, de fecha 23 del mes de abril del año 2007.

El primer título contiene las disposiciones generales y conceptuales, abarcando de forma general el objeto, ámbito y principios normativos de dicha ley. El art. 1 de la ley 53-07 plantea lo siguiente sobre el objeto de la misma:

> La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos.

La ley No. 53-07 en su art.2 extiende su ámbito de aplicación a todo el territorio nacional y sobre toda persona física o moral ya sea nacional o extranjera que viole las disposiciones que la misma enumera. De forma textual este articulo reseña las siguientes situaciones:

> a) Cuando el sujeto activo origina u ordena la acción delictiva dentro del territorio nacional;
>
> b) Cuando el sujeto activo origina u ordena la acción delictiva desde el extranjero, produciendo efectos en el territorio dominicano;
>
> c) Cuando el origen o los efectos de la acción se produzcan en el extranjero, utilizando medios que se encuentran en el territorio nacional;
>
> d) Cuando se caracterice cualquier tipo de complicidad desde el territorio dominicano.

A partir del art. 4 de la (LCDAT) se presenta un glosario con los principales conceptos que se abordan en la ley y la definición entorno a la cual deberán entenderse los mismos. Dentro de los conceptos que la ley recoge se encuentran: Acceso ilícito, afectar, clonación, código de acceso, código de identificación,

código malicioso, computadora, datos, delito de alta tecnología, dispositivo, internet, red informática, sistema de telecomunicaciones, entre otros.

El segundo título de la (LCDAT) establece la normativa efectiva a nivel nacional, en materia de delitos de alta tecnología, planteando el derecho penal sustantivo a aplicar en el territorio nacional. Este se compone de cinco capítulos dentro de los cuales se agrupan de forma general las conductas que sanciona esta ley.

El Primer capítulo abarca los crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información. Dentro de este capítulo se tipifican aquellas conductas que atentan contra la seguridad de la información y los sistemas que tienen que ver con la misma.

Tabla No. 3. Crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información.

Articulo	Delito	Definición
5.	Códigos de acceso	El hecho de divulgar, generar, copiar, grabar, capturar, utilizar, alterar, traficar, desencriptar, decodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares, a través de los cuales se logra acceso ilícito a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, o falsificar cualquier tipo de dispositivo de acceso al mismo, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo.

6.	Acceso ilícito	El hecho de acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de tres meses a un año de prisión y multa desde una vez a doscientas veces el salario mínimo.
7	Acceso ilícito para servicios a terceros	El hecho de utilizar un programa, equipo, material o dispositivo para obtener acceso a un sistema electrónico, informático, telemático o de telecomunicaciones, o a cualquiera de sus componentes, para ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, se sancionará con la pena de tres meses a un año de prisión y multa desde tres a quinientas veces el salario mínimo.
8	Dispositivos fraudulentos	El hecho de producir usar, poseer, traficar o distribuir, sin autoridad o causa legítima, programas informáticos, equipos, materiales o dispositivos cuyo único uso o uso fundamental sea el de emplearse como herramienta para cometer crímenes y delitos de alta tecnología, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo.

9	Interceptación e intervención de datos o señales	El hecho de interceptar, intervenir, injerir, detener, espiar, escuchar, desviar, grabar u observar, en cualquier forma, un dato, una señal o una transmisión de datos o señales, perteneciente a otra persona por propia cuenta o por encargo de otro, sin autorización previa de un juez competente, desde, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones, o de las emisiones originadas por éstos, materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas físicas o morales, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo, sin perjuicio de las sanciones administrativas que puedan resultar de leyes y reglamentos especiales.
10	Daño o alteración de datos	El hecho de borrar, afectar, introducir, copiar, mutilar, editar, alterar o eliminar datos y componentes presentes en sistemas electrónicos, informáticos, telemáticos, o de telecomunicaciones, o transmitidos a través de uno de éstos, con fines fraudulentos, se sancionará con penas de tres meses a un año de prisión y multa desde tres hasta quinientas veces el salario mínimo.
11	Sabotaje	El hecho de alterar, maltratar, trabar, inutilizar, causar mal funcionamiento, dañar o destruir un

		sistema electrónico, informático, telemático o de telecomunicaciones, o de los programas y operaciones lógicas que lo rigen, se sancionará con las penas de tres meses a dos años de prisión y multa desde tres hasta quinientas veces el salario mínimo.

Fuente: Elaboración propia, a partir de la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, de fecha 23 del mes de abril del año 2007.

Como puede observarse todos los crímenes y delitos que la ley reconoce en este capítulo se relacionan con la confidencialidad, integridad, los datos y los sistemas de información. Estos delitos prevén el acceso de una forma no autorizada, ya sea intencional o no a los datos que se encuentran resguardados en sistemas informáticos, electrónicos o mecanismos análogos. De igual forma la vulneración de los sistemas electrónicos, informáticos o de telecomunicaciones, a los fines de extraer información es penado por esta ley.

El segundo capítulo de la (LCDAT) presenta los delitos de contenido. Dentro de los delitos de contenido que tipifica la (LCDTA) es el más extenso de los capitulo y en el mismo se presentan aquellos delitos comúnmente conocidos pero que nos perpetrados con ayuda de la tecnología.

Tabla No. 4. Delitos de contenido.

Articulo	Delito	Definición
12.	Atentado contra la vida de la persona	Se sancionará con las mismas penas del homicidio intencional o inintencional, el atentado contra la vida, o la provocación de la muerte de una persona cometido

		utilizando sistemas de carácter electrónico, informático, telemático o de telecomunicaciones, o sus componentes.
13.	Robo mediante la utilización de alta tecnología	El robo, cuando se comete por medio de la utilización de sistemas o dispositivos electrónicos, informáticos, telemáticos o de telecomunicaciones, para inhabilitar o inhibir los mecanismos de alarma o guarda, u otros semejantes; o cuando para tener acceso a casas, locales o muebles, se utilizan los mismos medios o medios distintos de los destinados por su propietario para tales fines; o por el uso de tarjetas, magnéticas o perforadas, o de mandos, o instrumentos para apertura a distancia o cualquier otro mecanismo o herramienta que utilice alta tecnología, se sancionará con la pena de dos a cinco años de prisión y multa de veinte a quinientas veces el salario mínimo.
14.	Obtención ilícita de fondos	El hecho de obtener fondos, créditos o valores a través del constreñimiento del usuario legítimo de un servicio financiero informático, electrónico, telemático o de telecomunicaciones, se sancionará con la pena de tres a diez años de prisión y multa de cien a quinientas veces el salario mínimo.
15.	Estafa	La estafa realizada a través del empleo de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con la pena de

		tres meses a siete años de prisión y multa de diez a quinientas veces el salario mínimo.
16.	Chantaje	El chantaje realizado a través del uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de sus componentes, y/o con el propósito de obtener fondos, valores, la firma, entrega de algún documento, sean digitales o no, o de un código de acceso o algún otro componente de los sistemas de información, se sancionará con la pena de uno a cinco años de prisión y multa de diez a doscientas veces el salario mínimo.
17.	Robo de identidad	El hecho de una persona valerse de una identidad ajena a la suya, a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con penas de tres meses a siete años de prisión y multa de dos a doscientas veces el salario mínimo.
18.	De la falsedad de documentos y firmas	Todo aquel que falsifique, desencripte, decodifique o de cualquier modo descifre, divulgue o trafique, con documentos, firmas, certificados, sean digitales o electrónicos, será castigado con la pena de uno a tres años de prisión y multa de cincuenta a doscientas veces el salario mínimo.

19.	Uso de equipos para invasión de privacidad	El uso, sin causa legítima o autorización de la entidad legalmente competente, de sistemas electrónicos, informáticos, telemáticos, de telecomunicaciones, o dispositivos que puedan servir para realizar operaciones que atenten contra la privacidad en cualquiera de sus formas, se sancionará con la pena de seis meses a dos años de prisión y multa de cinco a quinientas veces el salario mínimo.
20.	Comercio ilícito de bienes y servicios	La comercialización no autorizada o ilícita de bienes y servicios, a través del Internet o de cualquiera de los componentes de un sistema de información, se castigará con la pena de tres meses a cinco años de prisión y multa de cinco a quinientas veces el salario mínimo.
21.	Difamación	La difamación cometida a través de medios electrónicos, informáticos, telemáticos, de telecomunicaciones o audiovisuales, se sancionará con la pena de tres meses a un año de prisión y multa de cinco a quinientas veces el salario mínimo.
22.	Injuria pública	La injuria pública cometida a través de medios electrónicos, informáticos, telemáticos, de telecomunicaciones, o audiovisuales, se sancionará con la pena de tres meses a un año de prisión y multa de cinco a quinientas veces el salario mínimo.

23.	Atentado sexual.	El hecho de ejercer un atentado sexual contra un niño, niña, adolescente, incapacitado o enajenado mental, mediante la utilización de un sistema de información o cualquiera de sus componentes, se sancionará con las penas de tres a diez años de prisión y multa desde cinco a doscientas veces el salario mínimo.
24.	Pornografía infantil	La producción, difusión, venta y cualquier tipo de comercialización de imágenes y representaciones de un niño, niña o adolescente con carácter pornográfico en los términos definidos en la presente ley, se sancionará con penas de dos a cuatro años de prisión y multa de diez a quinientas veces el salario mínimo.

Fuente: Elaboración propia, a partir de la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, de fecha 23 del mes de abril del año 2007.

Los denominados delitos de contenido son aquellos ilícitos tradicionales, reconocidos en el código penal dominicano, en los cuales se utiliza como medio de comisión los sistemas electrónicos, informáticos, de telecomunicaciones o similares. Estos delitos presentan como elemento común el empleo de la tecnología y los componentes de la misma. El bien jurídico protegido en estos casos dependerá del delito base, por ejemplo, el art. 12 sanciona el atentado contra la vida de la persona al establecer que se sanciona con la misma pena del homicidio.

El tercer capítulo se enfoca en los delitos de propiedad intelectual y afines. En este capítulo la ley remite de forma directa a legislaciones especializadas sobre derecho de autor y propiedad intelectual. El art. 25 de la (LCDAT) explica que:

> Cuando las infracciones establecidas en la Ley No.20-00, del 8 de mayo del año 2000, sobre Propiedad Industrial, y la Ley No.65-00, del 21 de agosto del año 2000, sobre Derecho de Autor, se cometan a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de cualquiera de sus componentes, se sancionará con las penas establecidas en las respectivas legislaciones para estos actos ilícitos.

El cuarto capítulo trata aquellos delitos que van en contra de las telecomunicaciones. El art. 26 y siguiente de la ley No. 53-07, enumera los hechos que constituyen ilícitos en el ámbito de las telecomunicaciones.

Tabla No. 5. Delitos en contra de las telecomunicaciones.

DELITO	DEFINICIÓN
Llamada de retorno de tipo fraudulento	La generación de tráfico internacional en sentido inverso al normal, con fines comerciales, mediante mecanismos y sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones. Este hecho incluye, pero no se limita, a cualquier tipo de retorno de llamada a través de código, asistencia de operador, vía un sistema informático, dependiendo del mecanismo o sistema mediante el cual se transmita la señal de disparo;
Fraude de proveedores de servicio de información líneas tipo 1-976	La autogeneración de llamadas por parte del proveedor de servicio de información de líneas tipo 1-976, con el propósito de que la prestadora que le ofrece el servicio de telefonía tenga que pagarle las comisiones de estas llamadas será considerada un fraude, constituyendo un agravante, cuando los autores del delito se valgan de medios publicitarios o de cualquier otro tipo y precios reducidos, o de

	números telefónicos ordinarios para su redireccionamiento hacia líneas de servicio de información, u otros medios similares;
Redireccionamiento de llamadas de larga distancia	El fraude en el desvío o redirección del tráfico de larga distancia de la ruta utilizada por parte de las compañías portadoras de señal de larga distancia, para evadir el costo real de la misma, a través de conmutadores colocados en lugares distintos al de origen de la llamada;
Robo de línea	El uso de una línea existente, alámbrica o inalámbrica, de un cliente legítimo, para establecer cualquier tipo de llamadas mediante una conexión clandestina, física o de otra índole, en cualquier punto de la red;
Desvío de tráfico	El desvío de tráfico a través de rutas no autorizadas con el objeto de evitar o disminuir los pagos que corresponden a la naturaleza del tráfico desviado, ya sea un desvío de servicios, desvío de facilidades contratadas, o cualquier otro tipo de desvío ilícito;
Manipulación ilícita de equipos de telecomunicaciones	El hecho de manipular ilícitamente, de cualquier forma, las centrales telefónicas u otros componentes de las redes de telecomunicaciones, con el objetivo de hacer uso de los servicios sin incurrir en los cargos correspondientes;
Intervención de centrales privadas	La utilización de medios para penetrar centrales privadas a través de los puertos de mantenimiento o especiales del contestador automático o cualquier otro medio, que conlleven la realización de llamadas no autorizadas en perjuicio del propietario de la central intervenida.

Fuente: Elaboración propia, a partir de la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, de fecha 23 del mes de abril del año 2007.

El quinto capítulo enuncia los crímenes, delitos contra la nación y los actos de terrorismo. Los artículos 27 y 28 enuncian los crímenes y delitos contra la nación y los actos de terrorismo respectivamente.

El artículo 27 trata los Crímenes y Delitos contra la Nación, explicando que:

> Los actos que se realicen a través de un sistema informático, electrónico, telemático o de telecomunicaciones, que atenten contra los intereses fundamentales y seguridad de la Nación, tales como el sabotaje, el espionaje o el suministro de informaciones, serán castigados con penas de quince a treinta años de reclusión y multa de trescientas a dos mil veces el salario mínimo.

De igual forma el artículo 28 de la ley refiere sobre los actos de terrorismo lo siguiente:

> Todo aquel que con el uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, ejerza actos de terrorismo, será castigado con pena de veinte a treinta años de reclusión y multa de trescientos a mil salarios mínimos, del sector público. Asimismo, se podrá ordenar la confiscación y destrucción del sistema de información o sus componentes, propiedad del sujeto pasivo utilizado para cometer el crimen.

El tratamiento de los delitos tecnológicos en la ley No. 53-07, sobre Crímenes y Delitos de Alta Tecnología, no es el único marco legal a nivel interno para la regulación de esta clase de delitos. En atención a los crecientes cambios y a los nuevos desafíos en el ámbito de la tecnología ha sido necesario crear leyes adjetivas que cubran o complementen el marco general que se ha dispuesto. Un motor interesante para la creación de nuevas leyes es la casuística, es decir disposiciones especiales que nacen para casos especiales y cuya aplicación genérica es limitativa.

Uno de los casos especiales detectados en nuestra sociedad con los denominados correos basura o spam. Larios Escamilla, J. A., & Sánchez González, R. J. (2014) define spam como los mensajes no solicitados, no deseados o de remitentes desconocidos. Este autor, dentro de su tesis, señala el

alto porcentaje de correos basura que diariamente recibe un usuario en su email. Asimismo destaca diversas acepciones del término al establecer que:

> También se llama correo no deseado a los virus sueltos en la red y páginas filtradas (casinos, sorteos, premios, viajes, drogas, software y pornografía), se activa mediante el ingreso a páginas de comunidad eso grupos o acceder a enlaces en diversas páginas o inclusive sin antes acceder a ningún tipo de páginas de publicidad.

Este autor reseña nuevas consideraciones sobre lo que podría considerarse como spam, llegando a considerarlo dentro de los foros o chats. De este modo cuando un usuario, repetida y deliberadamente, realiza publicaciones en un foro que no van orientados al tema y resultan inútiles sobre la conversación iniciada podría considerarse como spam. Asimismo identifica como spam aquellos casos donde se realizan publicaciones inútiles en foros si la información presentada resulta inútil para los demás participantes del mismo.

El 8 de agosto del presente año 2014, fue promulgada en la ciudad de Santo Domingo, Distrito Nacional, la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam). Esta herramienta legal nace a raíz del incremento de correos electrónicos no solicitados por los usuarios y tomando en consideración el impacto negativo que esto representa para dichos usuarios. El legislador dominicano reconoce el carácter personal y privado de los correos electrónicos o e-mails y en consecuencia los asemeja a un patrimonio personal y por ende a un derecho de todo usuario. El art. 1 de la ley 310-14 establece la finalidad de la misma al explicar que:

> Esta ley tiene como objeto regular el envío de comunicaciones comerciales, publicitaria o promocionales no solicitadas, realizadas vía correos electrónicos, sin perjuicio de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor.

Esta ley, al igual que muchas otras, contiene a partir del art. 3 diferentes conceptos y la forma en que los mismos deberán interpretarse dentro de la misma De este modo términos como: Destinatario, intermediario, campo del asunto, proveedores de servicios, nombre del dominio, son definidos ubicándolos en el contexto acorde a la ley. Uno de los conceptos fundamentales de esta ley es el de "spam". El art. 2, numeral 2 de la ley define spam como:

> Comunicaciones comerciales no solicitadas y/o Spam es todo mensaje de datos enviado a un número indiscriminado de personas, sin su debida autorización, dirigido a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial industrial, artesanal o profesional.

Este concepto inicia con la expresión "comunicaciones comerciales no solicitadas" y la equipara al vocablo o termino de spam. Bien podríamos señalar que el punto común en las definiciones y conceptualización es la no solicitud y la molestia que esta recepción ocasiona a los usuarios que las reciben.

El segundo capítulo de esta ley trata del envío de comunicaciones comerciales estableciendo las condiciones de las comunicaciones comerciales y los requisitos para el envío de la misma. A partir del art. 4 de este capítulo se establece que: "Toda comunicación comercial electrónica debe contener el señalamiento publicidad en el campo del asunto de cada mensaje". El primer párrafo de este artículo exige la identificación de la publicidad cuando sea para mayores de edad con la etiqueta "publicidad para adultos". Con esta disposición se obliga a la identificación del mensaje a los fines de que el destinatario pueda tener conocimiento de lo que recibe.

Sin embargo, la ley no solo dispone la identificación del contenido, sino que va más allá y establece los requisitos para el envío de las comunicaciones comerciales a partir del art. 5, los cuales consisten en la identificación adecuada de datos esenciales del iniciador y cualidades del mensaje. Dentro de los

requisitos exigidos están en primer lugar el nombre o razón social, domicilio y correo de quien inicia el mensaje. Asimismo se exige la inclusión de una dirección para que el destinatario pueda notificar su deseo de recibir o no comunicaciones de esta especie. En el caso de que el mensaje se mediante un móvil, se requiere el señalamiento del numero del iniciador y la inclusión de un numero para dar respuesta sobre el mensaje la conformidad con el mismo.

El tercer capítulo abarca las prohibiciones y las excepciones que la ley marca. De forma textual el art. 7 de este capítulo reseña lo siguiente: “Queda prohibida la remisión, directa o indirecta, de comunicaciones comerciales cuya recepción no haya sido solicitada o consentida por el interesado receptor de la misma”. Esta prohibición presenta una serie de excepciones donde el envío de esta clase de comunicaciones son permitida no pudiendo darse lugar a las sanciones que la misma ley prevé en estos casos. Constituyen excepciones a la prohibición los casos en que, previo a la recepción por parte del destinatario de un mensaje no solicitado, este haya tenido algún tipo de relación comercial con el iniciador de dicho mensaje o cuando haya dado su consentimiento expreso. Cabe aclarar que entre la relación comercial iniciada y la recepción del mensaje por parte del destinatario no debe haber existido ninguna notificación expresa donde el destinatario declare el deseo de no recibir mensajes de esta especie.

Esta misma ley establece cuando una comunicación comercial puede considerarse como ilegal, y en consecuencia dar lugar a las sanciones que la misma ley dispone en cada caso. El art. 7 de la ley establece los casos en los cuales las comunicaciones comerciales pueden considerase ilegales:

> 1) Se remita, directa o indirectamente sin haber sido solicitada o consentida expresamente por el interesado receptor de la misma;
>
> 2) Contenga información falsa o engañosa en el campo del asunto, que no coincida con el contenido del mensaje esta información incluye toda información de cabecera, según lo dispone el numeral 6) del artículo 3, de esta ley;

> 3) Imposibilite o entorpezca los esfuerzos del destinatario, de los proveedores de servicios o de las autoridades del Estado, para identificar, localizar o responder a la persona que inició o emitió la comunicación comercial, o de investigar la presunta violación de esta ley;
>
> 4) Se envíe o transmita después de pasados cinco (5) días calendarios desde que el destinatario haya formulado el pedido para que no se envíe dicha publicidad.

El capítulo cuarto de la ley enuncia los derechos del destinatario. El art. 10 dispone que los destinatarios tienen derecho a:

> 1) No recibir comunicaciones comerciales no solicitadas;
>
> 2) Rechazar de forma expresa la recepción de las comunicaciones comerciales no solicitadas utilizando un mecanismo válido y activo de respuesta. El simple reenvío de la comunicación comercial ni iniciador constituirá rechazo expreso;
>
> 3) Revocar en cualquier momento el consentimiento otorgado para la recepción de comunicaciones comerciales. El simple reenvío de la comunicación comercial al iniciador constituirá revocación expresa.

Las infracciones y sanciones son establecidas en la ley a partir del capítulo quinto. El art. 13 de la ley sanciona y presenta cuales son los delitos informáticos listando infracciones como:

> 1) Acceder a un sistema informático sin autorización e intencionalmente iniciar la transmisión de comunicaciones comerciales desde o a través de dicho sistema;
>
> 2) Acceder a un sistema informático para reenviar o retransmitir comunicaciones comerciales con la intención de engañar a los destinatarios sobre el origen de las mismas;
>
> 3) Falsificar el campo del asunto de un mensaje de datos que contenga una comunicación comercial e intencionalmente iniciar la transmisión del mismo:

> 4) Registrar y recolectar, fraudulenta o maliciosamente, usando información falsa, la identidad del registrante de una cuenta de correo electrónico o direcciones de correo electrónico de sitios de acceso público, tales como sitios de charla, directorios públicos, grupos receptores de noticias, servicios de perfiles en línea, redes sociales y cualquier otro medio masivo que agrupe direcciones electrónicas, o de un nombre de dominio e iniciar intencionalmente la transmisión de múltiples comunicaciones comerciales desde cualquier combinación de tales cuentas o dominios sin la autorización del titular del correo electrónico o del operador del sitio de acceso;
>
> 5) Ofrecer la venta de bases de datos con direcciones de correos electrónicos sin el consentimiento expreso de los propietarios de los mismos, con el objetivo de generar comunicaciones comerciales no solicitadas conforme a la presente ley.

Resulta interesante señalar que estas infracciones pueden dar lugar a que el destinatario afectado por los mismos solicita el resarcimiento por daños y perjuicios, explicando los daños y lesiones que el mensaje le ocasiono. El art. 11 resalta la competencia de los juzgados ordinarios para conocer de esta acción.

CAPÍTULO II-

CATEGORIZACIÓN DE LOS DELITOS DE ALTA TECNOLOGÍA.

2.1 CRITERIOS INTERNACIONALES APLICABLES A LA REPÚBLICA DOMINICANA.

El Diccionario de la Real Academia de la Lengua Española (2014) define la palabra criterio como: “Norma para conocer la verdad” o “juicio o discernimiento”. La palabra “juicio” empleado en la última definición revela el origen de la palabra misma. El término “criterio” suele asemejarse al concepto de opinión o posición, entendidos estos dos en un sentido estricto, como la postura que se adopta frente a una persona, situación u objeto.

El criterio es un juicio subjetivo que se hace sobre algo en particular y que se sustenta en una norma fija, es decir que no varía, y que nos permite discernir la mejor opción ante escenarios comunes. Frecuentemente escuchamos frases como: “Según mi criterio…”, “El criterio de la empresa es…”, “No tienes criterio para…”, etc. Todas ellas evidencian un trasfondo subjetivo acorde al cual se hace una distinción en una situación concreta.

A lo largo del primer capítulo de este trabajo final se presenta el concepto y los antecedentes de los delitos de alta tecnología. De igual forma se abordan desde la perspectiva legislativa los sujetos de estos delitos y el tratamiento nacional e internacional que se le da a los mismos. Dentro del apartado sobre el tratamiento de los delitos de alta tecnología se detallan cuales de estos delitos han sido tipificados en nuestra legislación y la forma en que los mismos son clasificados en ella. Sin embargo, no se plantea en la legislación o la doctrina el criterio específico con el cual se tipifica esta clase de delitos en nuestros marcos legales. En atención a esto debemos cuestionar ¿Cuál es el término adecuado para referirse a esta clase de delitos? ¿Cómo se identifican estos ilícitos? ¿Cuáles

elementos conforman estos tipos penales? ¿Qué es lo que permite reconocer la especialidad de los mismos?

Con el objeto identificar una definición precisa sobre nuestro objeto de estudio, es decir las conductas ilícitas abordadas en nuestro primer capítulo, decidimos aplicar una pequeña entrevista focalizada a diferentes profesionales del área de la informática, la tecnología y el derecho. Dentro de las preguntas que componen la entrevista están:

1. ¿Qué considera usted como alta tecnología?
2. ¿Qué diferencia existe entre los siguientes términos: Delito informático, delito de alta tecnología y delito cibernético?
3. ¿Cómo podría definir delitos de alta tecnología?
4. ¿Cuáles conductas denominadas como delitos de alta tecnología conoce?
5. ¿Conoce usted la ley 53-07 sobre crímenes y delitos de alta tecnología? En caso de conocerla ¿Cuál es su opinión sobre ella?
6. ¿Cuáles delitos de alta tecnología se presentan en el desarrollo de su trabajo?
7. ¿Cuáles conductas, según su criterio, podrían constituir delitos de esta especie?

Cada una de estas o preguntas fue cuidadosamente estructurada con el objeto de recolectar información de calidad en relación a nuestro problema de investigación y con la finalidad de dar respuesta al mismo. Sin embargo los resultados obtenidos a partir de las mismas no fueron concluyentes y carecen de relevancia para nuestra investigación en el sentido de que el nivel teórico y práctico que evidenciaron los sujetos a los cueles se aplico está por debajo de los niveles técnicos y especializados necesarios. En atención a esta situación la información recogida no fue tomada en consideración para esta investigación.

No obstante esta aclaración, no podemos dejar subsistir las ambigüedades y vacios detectados en nuestras leyes y doctrina, por lo cual se ha tomado como referencia las opiniones y conceptos ofertados por investigadores especializados en nuestra área de investigación, para con apoyo de sus aportes se pueda dar respuesta a las interrogantes planteadas.

La doctrina se ha encargado de establecer de forma precisa diferentes criterios para la división de los delitos de alta tecnología. Establecer estos criterios de identificación permite clasificar estos delitos y agrupar a aquellos que presentan características comunes. De este modo la doctrina ha llenado el vacio que los códigos y las leyes sustantivas y adjetivas han dejado.

2.1.1 CRITERIO NO. 1: TIPOS DE DELITOS INFORMÁTICOS SEGÚN TÉLLEZ VALDEZ.

La primera clasificación que vamos a abordar es la utilizada por Téllez Valdez, en la cual se agrupan en dos grandes segmentos los delitos de alta tecnología. Esta clasificación es una de las más generales y abarcativas pues dentro de la misma pueden encasillarse cualquier delito de esta especie.

Tabla No. 6. Clasificación de los delitos de alta tecnología según Téllez Valdez.

Criterio de clasificación	Crímenes y delitos
1. Como instrumento o medio: son conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito	a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.) b) Variación de los activos y pasivos en la situación contable de las empresas. c) Planeamiento y simulación de delito convencionales (robo, homicidio, fraude, etc.) d) Lectura, sustracción o copiado de

	información confidencial. e) Modificación de datos tanto en la entrada como en la salida. f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas. g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa. h) Uso no autorizado de programas de cómputo. i) Introducción de Instrucciones que provocan "interrupciones" en la lógica interna de los programas. j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos. k) Obtención de información residual impresa en papel luego de la ejecución de trabajos. l) Acceso a áreas informatizadas en forma no autorizada. m) Intervención en las líneas de comunicación de datos o teleproceso.
2. Como fin u objeto: conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física	a) Programación de instrucciones que producen un bloqueo total al sistema. b) Destrucción de programas por cualquier método. c) Daño a la memoria. d) Atentado físico contra la máquina o sus accesorios. e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados. f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)

Fuente: Elaboración propia, a partir de la clasificación realizada por Téllez Valdez.

Los dos criterios presentados por Téllez Valdez giran en torno a si el delito en cuestión es el medio o el fin en sí mismo. Sin duda alguna este autor pudo visualizar de forma clara la diferencia precisa que existe en ambos móviles, pues agrupa en estas dos categorías delitos diferentes, sin limitar el número que dentro de dichas clasificaciones pueda incluirse. Valdivia, I. G., & Rubí, A. (2011). Abordan el tema en ese mismo sentido, Sin embargo estos sustituyen el término "criterio" por "vertiente", para con ello poder identificar las modalidades en las cuales se presentan esta clase de delitos.

En la clasificación realizada por Téllez Valdez, presentada en la tabla No.7, el primer grupo corresponde a: Cuando el delito es el medio o instrumento. En este apartado se incluyen aquellas acciones ilícitas que se sirven de la tecnología y los medios electrónicos propiamente dichos para la comisión de otro delito. Tomando como ejemplo la falsificación de documentos vía computarizada (tarjetas de créditos, cheques, documentos de identidad, etc.), que es el primer ilícito que aparece en nuestra tabla podemos deducir que:

1. La expresión "vía computarizada" indica que te tecnología es una herramienta o auxiliar al momento de la comisión del mismo.
2. El delito de falsificación de documentos es un ilícito que se encuentra tipificado en nuestra legislación.
3. En consecuencia el delito base de "falsificación" puede configurarse en ausencia o presencia de la tecnología.

El segundo grupo de la tabla presenta aquellas conductas donde la tecnología es el fin u objeto del delito mismo. Esta clase de delitos van dirigidos a afectar principalmente la tecnología de la cual se sirven. Dentro de este grupo puede mencionarse cualquier programa que genere a priori la destrucción de programas por cualquier método. De este grupo podemos señalar que el objeto o bien jurídico afecto es la tecnología o medio electrónico en sí mismo.

La clasificación realizada en torno a estos dos criterios, tal y como señalamos anteriormente, resulta tan general que ubica a delitos de diferentes naturalezas bajo una misma especie. Delitos que utilizan la tecnología como medio o fin bien pueden obedecer a causas diferentes. Ocurre de igual manera con respecto a la clasificación realizada atendiendo al objeto, debido a que dicho objeto puede ramificarse y dirigirse a diferentes campos dependiendo de la causa que lo impulse.

2.1.2 CRITERIO NO. 2: TIPOS DE DELITOS INFORMÁTICOS SEGÚN EL OBJETIVO.

Determinar el objeto de un delito permite conocer la finalidad y naturaleza del mismo. El segundo criterio de clasificación está estructurado tomando como punto focal el objetivo del delito de alta tecnología.

Tabla No. 7. Clasificación de los delitos informáticos según el objetivo.

Categoría	Delito	Tipos
Ciberdelincuencia económica	Malware	Virus
		Ransomware
		Gusanos
		Troyanos
		Spyware
		Adware
		Scareware/Rogue
	Spam	
	Phishing	Smishing
		Pharming
		Pharming local
		Vishing
	Scam	Citas online fraudulentas

		Fraude nigeriano A precio de chollo por motivos personales
	Ataques DoS y DDoS	Ataques por Volumen
		Ataques por protocolo
		Ataques de capa de aplicación
	Defacement	
	Ciberespionaje y ciberguerra	
Ciberdelincuencia social	Ciberacoso	Ciberbullying
		Cyberstalking
		Cybergrooming
Ciberdelincuencia ideológica	Ciberterrorismo y Hacktivismo	Anonymous
		LulzSec

Fuente: Elaboración propia a partir de la tipificación del delito informático que realiza Mateos Pascual, I. (2013) en su proyecto Ciberdelincuencia: desarrollo y persecución tecnológica.

La tabla No. 7 agrupa de una forma diferente los delitos electrónicos, pues en este caso no se trata de si la tecnología es el medio o el fin, sino del objeto que se persigue al momento de cometer el mismo. La primera categoría agrupa la ciberdelincuencia económica. Esta clase de delitos persiguen una remuneración económica.

El segundo grupo contiene los delitos electrónicos de corte social. En este caso no se trata de una afectación de carácter económico, sino más bien de de ilícitos que atañen a grupos sociales y los cuales lesionan elementos patrimoniales como la imagen, el nombre y la intimidad de los mismos.

El tercer renglón agrupa los delitos de alta tecnología con base ideológica. Bajo esta categoría se presentan aquellos cuyo motor principal es el cumplimiento o fidelidad a una ideología concreta. En este caso la ideología que se persigue motiva por completo las acciones que se emprenden y que configuran este tipo de delitos.

El criterio de clasificación empleado para la estructura de la tabla No. 7, parecería ser el más idóneo para la clasificación de esta especie de delitos, sin embargo la misma deja a un lado conductas que ya están en nuestra legislación.

2.1.3 CRITERIO NO. 3. TIPOS DE DELITOS INFORMATICOS SEGÚN LAS NACIONES UNIDAS (ONU).

El Foro de Profesionales Latinoamericanos de Seguridad, según Hall, A. (s.f.), publicó los tipos de delitos informáticos reconocidos por la Organización de las Naciones Unidas (ONU).

Tabla No. 8. Tipos de delitos informáticos reconocidos por la Organización de las Naciones Unidas (ONU).

Tipo	Delito
Fraudes cometidos mediante manipulación de computadoras	- Manipulación de datos de entrada - Manipulación de programas - Manipulación de los datos de salida - Fraude efectuado por manipulación informática
Manipulación de datos de entrada	- Como objeto - Como instrumento
Daños o modificaciones de programas o datos computarizados	- Sabotaje informático - Virus - Gusanos - Bombas lógicas o cronológicas
Acceso no autorizado a servicios y sistemas informáticos	- Piratas informáticos o hackers - Reproducción no autorizada de programas informáticos de la protección legal

Fuente: Elaboración propia, a partir de la clasificación de los delitos informáticos reconocidos por la ONU.

La tabla No. 8 presenta la clasificación realizada por la Organización de las Naciones Unidas. Esta organización agrupa en solo cuatro grandes categorías los delitos informáticos a sancionar, sin embargo, al igual que muchas normas

internacionales, esta no señala de forma clara el criterio a establecer. La primera categoría es denominada como fraudes por medio de la manipulación de las computadoras, abarcando únicamente el tipo delictual de fraude con la variante del medio a utilizar. La segunda clase describe las manipulaciones de datos y las divide según el uso, es decir si las mismas son usadas como objeto o como instrumento propiamente dicho. Este criterio es similar al que presenta Téllez Valdez en su clasificación, a pesar de que en este caso solo se ha limitado al uso de los datos.

El tercer reglón recoge los daños o modificaciones realizadas a programas o datos, señalando los casos de sabotaje, virus o gusanos que puedan ocasionar este efecto. El acceso no autorizado ha sido separado en una última categoría, ya sea a servicios o sistemas informáticos.

Todos estos renglones conforman la clasificación generalizada que presenta la ONU en materia de delitos de alta tecnología, sin embargo podemos verificar que los reglones no son tan cerrados como deberían y en ocasiones se plantean en categorías diferentes acciones o conductas similares. En esta clasificación la manipulación de datos se ve como medio y como instrumento, sin embargo la tercera categoría contiene las modificaciones de datos computarizados, lo cual nos indica que en ambos casos estos delitos describen las mismas acciones pese a que son recogidas en grupos diferentes.

En consecuencia la división por tipo que se presenta en la tabla No. 8 resultaría confusa o ambigua al momento de encasillar una determinada conducta, en atención a que no podría determinarse si la acción de extracción y uso de determinados datos realizados por un sujeto obedece al segundo o tercer grupo. Es necesario especificar de forma clara la conducta a juzgar y sobre todo el objeto de la misma, ya que bajo ningún concepto son equivalentes la manipulación de datos y el daño de los mismos.

2.2 TIPIFICACIÓN DE NUEVOS DELITOS DE ALTA TECNOLOGÍA EN EL MARCO DE LA LCDAT.

Larios Escamilla, J. A., & Sánchez González, R. J. (2014). Presentan en su tesis "ciberdelito" una serie interesante de nuevos ilícitos y variaciones de los ya existentes. Esta tesis es desarrollada por ingenieros en telecomunicaciones, por lo cual se debe analizar minuciosamente si los crímenes y delitos allí expuestos realmente se constituyen como tales. Este autor no solamente reseña nuevas conductas, sino que también presenta nuevos sujetos y el perfil que integra cada uno.

La teoría del delito aplicada a los delitos de alta tecnología.

La teoría del delito es el sistema que nos permite identificar elementos comunes a todos los delitos y que facilitan el reconocimiento del mismo. Estos elementos van más allá de la simple revelación de la naturaleza ilícita de una conducta, pues los mismos permiten comprobar cuando estamos en presencia de un delito consumado y cuando no.

La Escuela Nacional de la Judicatura en su libro "Teoría del Delito", publicado en el año 2007, presenta el concepto de "teoría jurídica del delito", explicando que:

> La teoría jurídica del delito es la sistematización de los diversos elementos que, partiendo del Derecho penal positivo, pueden entenderse comunes a todos los ilícitos penales o a un grupos significativo de ellos. Esta labor de sistematización es obra de la doctrina penal y resultado de una elaboración dogmática.

Los delitos de alta tecnología para ser considerados como deben contener los elementos a los cuales hace referencia la teoría del delito. No se trata de agrupar técnicas no permitidas o no contempladas en la ley, sino de la efectiva tipificación de conductas pasibles de sanción penal. El tipo, como parte de la teoría del delito cumple con tres funciones principales. La primera función del tipo es la de garantía, esto es acorde al principio de legalidad, el cual exige que ninguna

conducta ilícita puede sancionarse sin que la misma este consagrada en una ley promulgada con anterioridad a la comisión de la misma. La segunda función obedece a la motivación, es decir disuadir mediante la advertencia de imposición de una pena, a los posibles sujetos activos, de la comisión de las conductas identificadas. La tercera y última función es la de indicación, a través de la cual se advierte el carácter ilícito de la conducta tipificada en atención a la protección del bien jurídico que se protege.

La Escuela Nacional de la Judicatura. (2007) presenta la estructura y los elementos que debe contener el tipo. En esencia la estructura se compone de dos partes: una parte objetiva que obedece a factores externos y una parte subjetiva que obedece a factores internos. La parte objetiva se compone de: la conducta, los sujetos y el objeto; en cambio la parte subjetiva se compone de elementos internos como el dolo o la imprudencia.

Figura No. 2. Elementos de la tipicidad en la teoría del delito.

Fuente: Elaboración propia, a partir del libro Teoría del Delito de la Escuela Nacional de la Judicatura. (2007).

Lo significativo de la teoría del delito es que puede aplicarse a cualquier conducta para determinar si puede o no constituir un delito. Ambas partes, tanto la objetiva y como la subjetiva deben estar presente en las conductas que pretendan ser catalogadas como delitos.

2.2.1. IDENTIFICACIÓN DE NUEVOS PERFILES DE LOS SUJETOS EN LOS DELITOS DE ALTA TECNOLOGÍA.

La identificación de nuevas conductas delictivas, en el campo de los delitos de alta tecnología, trae consigo el reconocimiento de nuevos sujetos o actores que intervienen en los mismos. Inicialmente se había mostrado en el capitulo anterior los sujetos que la ley No. 53-07 reconoce y la forma en que los mismos entran en contacto.

Figura No. 3. Sujetos de los delitos de alta tecnología.

Fuente: Elaboración propia, a partir de la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007.

La figura No. 3 es una representación gráfica de los sujetos que la ley 53-07, sobre crímenes y delitos de alta tecnología, ha previsto que intervienen en esta clase de delitos. Acorde a la identificación y clasificación de delitos que presenta esta ley es general y poco específica, lo cual en consecuencia se tradujo en la identificación simplificada de los sujetos que en ella aparecen.

El desarrollo tecnológico y la evolución de los instrumentos electrónicos han incrementado y especializado de forma proporcional los ilícitos que en esta área aparecen. Todo esto ha traído como consecuencia la aparición de nuevos perfiles de los sujetos activos, es decir aquellos que realizan la acción delictual. No se trata de la aparición de nuevos sujetos como tal sino, de nuevos perfiles que el sujeto activo puede adoptar.

En el ámbito popular el sujeto activo es comúnmente identificado con el sustantivo de “hacker”, por lo cual el término se usa indistintamente para denominar a quien comete un delito de alta tecnología, sin importar el tipo cometido. De este modo se identifica con el mismo nombre conductas técnicas y muy específicas que podrían conducir al error o a una identificación incorrecta. Resulta ambiguo catalogar bajo el mismo término a sujetos que cometen delitos de naturaleza u objetivos distintos dentro de esta materia. La doctrina ha considerado indispensable separar o dividir técnicamente los delitos de alta tecnología, lo cual en consecuencia se ha traducido en la identificación de nuevos perfiles de sujetos activos para cada uno de los delitos identificados.

Tabla No. 9. Tipos de hackers y sus perfiles.

Criterio de clasificación	Sujeto	Perfil
Filosofía	*Black Hat Hacker*	(Del inglés, Hacker de sombrero negro) Son aquellos a los que normalmente se les refiere como simple Hacker. Son identificados por no seguir ningún tipo de ética de comunidad, y por buscar a

		menudo el beneficio personal o económico. El Hacker negro se dedica a buscar la forma de colapsar servidores, entrar en zonas restringidas o tomar el control de sistemas y redes. Se siente orgulloso de demostrar sus habilidades y su grado de autorrealización es mayor cuanto mayor sea el impacto del perjuicio provocado.
	White Hat Hacker	Conocidos también como los Hacker éticos o Hacker tradicionales, acerca de los cuales se ha comentado con anterioridad. Su mayor fechoría era la de dejar una tarjeta de visita informando al administrador del sistema las vulnerabilidades o fallos encontrados tras una incursión en su sistema, y/o realizando, en el peor de los casos, como únicas modificaciones, aquellas estrictamente necesarias para mantener su anonimato. En ocasiones los Hacker Blancos, son sujetos que han formado parte de los Hacker Negros, y que han decidido cambiar sus propósitos maliciosos por el apoyo a los administradores de los sistemas de seguridad y a la lucha contra el Cibercrimen, utilizando los mismos conocimientos para luchar contra estos.
	Grey Hat Hacker	Conocidos también como Hacker de sombrero Gris. Sujetos cuya ética es ambigua, los cuales poseen conocimientos comparables a los de un Black Hat Hacker pero que sin embargo utilizan para encontrar vulnerabilidades o fallos de seguridad que posteriormente se ofrecen a solventar bajo un acuerdo económico.

Tipos	*Cracker*	Podrían incluirse dentro del grupo de los Hacker de sombrero Negro. Son considerados el grupo más agresivo y su único objetivo es, utilizando la expresión comúnmente usada por este colectivo, “reventar sistemas” ya sean informáticos o electrónicos. Los cracker son expertos programadores que utilizan sus conocimientos para modificar el comportamiento de sistemas y redes explotando cualquier vulnerabilidad encontrada, actuando de manera obsesiva e insaciable guiados por su afán destructivo y ególatra.
	Phreaker	Colectivo enfocado mayormente al mundo de los sistemas telefónicos, incluyendo también la telefonía móvil y Voz sobre IP (VoIP). Conocen el funcionamiento de dichas tecnologías así como sus protocolos de comunicación y se dedican a alterar el comportamiento de dichos sistemas por placer y en ocasiones con fines económicos.
	Lammer	Repudiados dentro del colectivo Hacker, son aquellos internautas que se dedican a recopilar información y ejecutar códigos maliciosos buscando el reconocimiento social como Hacker sin tener un conocimiento real del impacto de sus acciones, ni del funcionamiento del código ejecutado. En ocasiones son realmente molestos aunque sus acciones no suelen provocar grandes daños.
	Scriptkiddie	Son simples usuarios de internet con afición a los

		temas de Hacking aunque sin demasiados conocimientos al respecto. Suelen utilizar programas o malware que encuentran por la red que ejecutan sin mayor estudio, llegando a infectar sus propios sistemas en multitud de ocasiones.
	Newbie	Conocidos como los aprendices de Hacker. Son aquellos novatos que comienzan a leer y experimentar con la información encontrada y que en ocasiones perpetran intrusiones en sistemas débiles aunque sin mayor trascendencia dados sus escasos conocimientos. Su único objetivo es el de aprender.
	Wannaber	Son aquellos que “quieren ser”. Aspirantes a Hacker con poca perseverancia y capacidad técnica, en su gran mayoría inofensivos, que utilizan sus escasos conocimientos para obtener el reconocimiento social fuera de la red.
	Piratas informáticos	Pese a que a menudo se confunde esta denominación con la del término Hacker, los piratas informáticos únicamente se dedican a la copia y distribución de software, música, juegos y un largo etc. de contenidos de manera ilegal, atentando contra la propiedad intelectual y los derechos de sus propietarios.

	Bucaneros	Hacen el papel de comerciantes en la red. Se dedican a comprar y vender material ilegal obtenido por medio de otros, tales como identidades, tarjetas de control de acceso, software crackeado, etc.

Fuente: Elaboración propia a partir de la lista presentada por Mateos Pascual, I. (2013) en su proyecto Ciberdelincuencia: desarrollo y persecución tecnológica.

La tabla No. 9 presenta los tipos de hackers y los perfiles que los mismos pueden identificar. Los criterios de división en este caso son: la filosofía y el tipo. Cuando se hace referencia a la filosofía como criterio para clasificar a los hackers, estamos hablando de la ética con la cual estos operan. Tal y como se reseña en la tabla, el objeto y por ende el tipo de delito en la cual se encausan cada uno obedece a su ética o principios. Un hacker propiamente dicho o *"Black Hat Hacker"* es propenso a la comisión de delitos de alta tecnología contra sistemas informáticos y electrónicos a cambio de la obtención de beneficios económicos. En cambio un *"White Hat Hacker"* asume una postura más conservadora o tradicionalista, siendo de un carácter diferente al concepto antiguo de hacker que se tiene. Resulta interesante destacar que esta la intensión que orienta al sujeto activo puede ser estudiada a partir del elemento subjetivo que compone la teoría del delito.

La intensión con la cual un determinado sujeto comete una acción influye de forma determinante en el tipo que comete. Determinar si el sujeto actúa con dolo, por imprudencia o por error es vital al momento de calificar una determinada conducta y en consecuencia juzgarla.

Si aplicamos la parte subjetiva a los tres tipos de hackers identificados según su filosofía en la tabla No. 9 observamos lo siguiente:

- Los "Black Hat Hackers": Son sujetos de carácter activo que actúan con conocimiento de causa, intensión o solo. El elemento de la intención se

encuentra claramente presente en estos al momento de la comisión de un delito de alta tecnología. Estos tienen un claro conocimiento de la conducta prohibida y en ocasiones de las consecuencias precisas que la misma. La intención o voluntad de estos sujetos es ejecutar un tipo daño o perjuicio a un sistema informático, a un equipo electrónico o medio tecnológico.

- Los “White Hat Hacker”: Son sujeto que, al igual que los anteriores, intervienen de forma activa en la comisión de los delitos de alta tecnología. Sin embargo es preciso marcar que una diferencia en el elemento volitivo de las acciones de los mismos. Estos a diferencia de los sujetos anteriores se orientan hacia la detección de fallas de seguridad e incursión en sistemas de acceso no autorizado, evitando el daño o colapso de las mismas. Su intención es más accesar o violar un sistema que destruirlo o dañarlo.
- Los “Grey Hat Hacker”: Constituyen otro tipo de sujetos activos. Estos representan un tercer tipo de sujeto cuyo objeto no es ocasionar un daño ni detectar fallas de seguridad, sino que sus acciones van encaminadas hacia la provocación de situaciones de esta especie con la finalidad de obtener una remuneración económica.

Como ha podido observarse, pese a que las acciones pueden ser similares entre uno y otro sujeto, la intensión o móvil determina gran parte de la selección del delito a cometer y debe considerarse al momento del estudio de los delitos de alta tecnología. Las circunstancias y el elemento subjetivo que representa y mueve a cada uno de estos sujetos marcan la diferencia en sus acciones y en su proceder.

La filosofía que persiguen los sujetos activos no es el único medio para catalogarlos, sino que la especificación técnica del delito cometido también nos permite diferenciar a estos sujetos. La tabla No. 9 en su parte infine presenta ocho (08) tipos de hackers y el perfil que cada uno de ellos adopta al momento de la comisión de un delito de alta tecnología. De este modo podríamos identifican: los Crackers, Phreakers, Lammers, Scriptkiddies, Newbies, Wannabe, Piratas informáticos y los Bucaneros. Todos estos están agrupados bajo la categoría de

hakers, sin embargo no todos ellos realizan las mismas acciones lo cual hace deducir que sus móviles y características son particulares.

La tabla No. 9 define de forma clara y precisa el perfil de cada uno de estos sujetos. La utilidad de estos perfiles es innegable en el estudio y comprensión de de los delitos de alta tecnología. La comprensión de estos perfiles es básica para el juzgamiento de estos delitos, pues permiten reconocer no solo la intención del agente activo, sino que también permite establecer su naturaleza. Tomando como ejemplo el perfil de un “cracker”, el cual contiene uno de los perfiles más preciso y cuyas acciones pueden encajarse dentro de los crímenes más agresivos en esta categoría y comparándolo con un “pirata informático”, cuyo objeto no es más que la copia y distribución de materiales informáticos no autorizados, reconocemos la diferencia abismal que los separa. En definitiva los delitos cometidos por un “*Phreaker”, el cual se enfoca en sistemas telefónicos, no podrían ser atribuidos a un “Newbie”, que representa un aprendiz o novato en el área, acorde a sus perfiles.*

La tabla No. 9 presenta la clasificación de lo que se considera con hackers acorde a su filosofía y tipo, sin embargo estos no son los únicos perfiles que la doctrina ha identificado y aportado. A continuación se presenta la tabla No. 9 que describe una serie de sujetos activos y los perfiles que los mismos integran.

Tabla No. 10. Perfiles adicionales.

Sujeto	Perfil
Instaladores de Bots	*Son* aquellos cuya intención es la de conseguir el control de un equipo remoto a través de la instalación de software malicioso. Para conseguir dichos fines se valen de malware pre-programado, el cual es embebido de manera oculta en todo tipo de interacciones que el usuario realiza mientras navega por la web.
Carders	

	Este tipo de ciberdelincuentes se centran exclusivamente en el robo de identidad y en la consecución de fraudes mediante tarjetas de crédito en la Red. Podemos considerar a los Carders como la evolución natural de los tradicionales carteristas. Una vez conseguida la información necesaria, pueden realizar transacciones y compras online encubriendo su identidad y cargando el coste a su víctima.
Ciberpunks	Sin llegar a tener un objetivo lucrativo en sus actos, los Ciberpunks, término surgido del movimiento literario con el mismo nombre, pueden llegar a suponer grandes pérdidas a sus víctimas, tanto económicas como de imagen. Considerado como el ciberdelincuente travieso, el ciberpunk se dedica a alterar sistemas públicos, como pueden ser una página Web, con objeto de mofarse y ridiculizar a aquellos que considere sus víctimas.
Insiders	Empleados o ex-empleados que actúan desde dentro de las propias compañías utilizando su experiencia y conocimiento de los sistemas “desde dentro”, para acceder, distribuir información confidencial o perjudicar de algún modo a sus empresas. Sus motivaciones suelen ser tanto económicas como personales incluso con fines de venganza.
Phisher, Spammer	Especializados en utilizar el correo electrónico como forma o vía de comunicación con sus víctimas. Buscan el beneficio económico a través de engaños y señuelos que llevan a confusión al cibernauta despistado mostrándose como fuentes aparentemente confiables.

Fuente: Elaboración propia a partir de la lista presentada por Mateos Pascual, I. (2013) en su proyecto Ciberdelincuencia: desarrollo y persecución tecnológica.

Hasta ahora hemos visto perfiles aislados de sujetos que cometen delitos informáticos y que pueden o no relacionarse los unos con los otros. Sin embargo, la doctrina ha pensado en cómo estos perfiles interactúan entre si y la forma en que los mismos podrían organizarse en una estructura continua que delito las funciones de cada sujeto. El crimen organizado, en el ámbito de los delitos de alta tecnología, es el espacio idóneo para la visualización de estas relaciones y el reconocimiento de la conducta que en el mismo se advierten.

Tabla No. 11. Roles en el crimen organizado.

Sujetos	Perfil
Programadores	Desarrollan los exploits y malware que se utiliza para cometer los cibercrimenes.
Distribuidores	Recopilan y venden los datos robados. Actúan como intermediarios.
Técnicos expertos	Mantienen la infraestructura de la “compañía Criminal”, incluyendo servidores, tecnologías de cifrado, base de datos, etc.
Hackers	Buscan aplicaciones de explits y vulnerabilidades de sistemas y redes.
Defraudadores	Crean técnicas de ingeniería social y despliegan diferentes ataques de phising o spam, entre otros.
Proveedores de hosting	Ofrecen un entorno seguro para alojar contenido ilícito en servidores y paginas.

Vendedores	Controlan las cuentas y los nombres de las víctimas y las proveen a otros criminales mediante pago.
Muleros	Realizan las transferencias bancarias entre cuentas de bancos.
Blanqueadores	Se ocupan del blanqueo de los beneficios.
Líderes de la organización	Frecuentemente, personas normal sin conocimientos técnicos que crean el equipo y defienden los objetivos.

Fuente: Elaboración propia a partir de la lista presentada por Mateos Pascual, I. (2013) en su proyecto Ciberdelincuencia: desarrollo y persecución tecnológica.

La tabla No. 11 plasma de forma ordenada el papel que juega un determinado sujeto activo dentro de una organización de carácter criminal. Básicamente la interacción y coordinación es prácticamente una obligación de los individuos en cualquier sociedad, y en consecuencia de las organizaciones que dentro de la misma se desarrollan. El rol o la función representada va acorde al conocimiento técnico y al objeto que busca un determinado sujeto. La interacción de los sujetos de los sujetos en esta clase de organizaciones es similar a la que aparece dentro de cualquier empresa organizada. Las funciones de los integrantes de este tipo de sociedades dependen la una de la otra. La labor de los hackers y de los técnicos expertos es prioritaria para las acciones subsiguientes que realizadas por los distribuidores, vendedores y los blanqueadores. Es importante destacar que como cualquier organización, frecuentemente aparecen líderes que guían, defienden y en ocasiones reúnen el equipo de trabajo.

Tabla No. 12. Técnicas empleadas por los sujetos activos de los delitos de alta tecnología.

Técnica	Descripción
Botnets	Las llamadas Botnets o redes de Bots, diminutivo de la palabra robot, son redes o grupos de ordenadores infectados, que pueden ser controladas de manera remota por el propietario del malware de control o bot, instalado en los equipos. El fin de estas redes es el de contar con todo un ejército de equipos anónimos, los cuales pueden recibir órdenes como la distribución del malware, el envío de Spam o la ejecución de ataques de denegación de servicio (DDoS).
Spoofing	El término Spoofing se refiere al uso de técnicas de suplantación de identidad con objeto de interceptar, alterar o conseguir establecer una comunicación.
Ataques Brute Force	Los ataques Brute Forte, del inglés, ataques por Fuerza Bruta, suelen estar destinados a la superación de sistemas criptográficos o protegidos por contraseñas. Se denominan ataques de fuerza bruta, a aquellos cuyo método empleado, para conseguir el acceso a un sistema restringido, consiste en recorrer todas y cada una de las posibilidades existentes dentro de un algoritmo de posibilidades de composición (como son el número de caracteres mínimo y máximo u otros requerimientos de complejidad) de credenciales de acceso, hasta conseguir obtener el resultado correcto, que permita la intrusión no autorizada.
Ataques JavaScript	Con la popularidad del desarrollo de las web 2.0 (término empleado para aludir a la nueva modalidad de sitios web, diseñados para facilitar la interoperabilidad y la participación de los usuarios),

	JavaScript se ha convertido en uno de los lenguajes de programación web más populares de Internet. Al contrario que el tradicional código HTML, orientado principalmente a la lectura de contenidos, este lenguaje es empleado principalmente para la creación de pequeñas aplicaciones que se ejecutan en el lado cliente, a través principalmente del navegador web, y que permiten al usuario actuar directamente sobre la interfaz, el formato y contenido del sitio.
SQL Injection	El funcionamiento de los ataques mediante SQL Injection se basa en la introducción de código SQL adicional a un aplicativo, generalmente a través de un formulario de login (donde es requerido un usuario y una contraseña de acceso) con el cual se pretende alterar el funcionamiento del entorno programado para realizar las consultas a la base de datos, de modo que sea posible conseguir, modificar o acceder a la información restringida contenida en esta.
Rootkits	Se denominan de este modo al conjunto de herramientas que permiten, a una determinada aplicación diseñada por un tercero (con fines habitualmente dañinos) la ejecución de procesos y modificación de archivos del sistema, cuyo acceso se encuentra restringido a exclusivamente a usuarios con privilegios de administrador o superusuario, también conocido como usuario “root”.

Fuente: Elaboración propia a partir de la lista presentada por Mateos Pascual, I. (2013) en su proyecto Ciberdelincuencia: desarrollo y persecución tecnológica.

2.2.2 IDENTIFICACIÓN DE NUEVOS DELITOS DE ALTA TECNOLOGÍA.

Hasta el momento hemos presentado y desglosado tres criterios para la clasificación de los delitos de alta tecnología, explicando en cada uno de ellos los parámetros utilizados para la división realizada. Sin embargo, entendemos que estos criterios, doctrinales y legislativos, no satisfacen la necesidad concreta que en la actualidad se nos plantea. En virtud de estos hemos realizado una nueva propuesta de categorización de los delitos de alta tecnología, en la cual se recoge lo mejor de los tres criterios antes expuestos, potencializando las fortalezas de los mismo y eliminando las debilidades encontradas.

Tabla No. 13. Categorización de los delitos de alta tecnología según la naturaleza de la acción.

Grupo	Delitos	Variaciones
Delitos contra sistemas informáticos	Delitos contra los sistemas informáticos	Sabotaje, daño y/o alteración de sistemas informáticos
	Delitos contra sistemas electrónicos	Sabotaje, daño y/o alteración de equipos electrónicos
Delitos con auxilio de sistemas informáticos y/o electrónicos	Crímenes y delitos contra la integridad, confidencialidad y privacidad.	- Acceso ilícito - Obtención, uso, clonación y/o divulgación de códigos de acceso. - Interceptación de datos o señales
	Delitos de contenido por medio de sistemas informáticos y/o electrónicos	- Atentado contra la vida de una persona - Atentado sexual - Robo

		- Obtención ilícita de fondos - Transferencia ilícita de fondos - Estafa - Chantaje - Robo de identidad - Falsificación de documentos y/o firmas - Grabación, producción, distribución, adquirían y posesión de pornografía infantil
	Delitos de propiedad intelectual	Delitos contenidos en la ley No.65-00, del 21 de agosto del año 2000, sobre Derecho de Autor
	Delitos contra la propiedad industrial	Delitos contenidos en la ley No.20-00, del 8 de mayo del año 2000, sobre Propiedad Industrial
	Delitos contra las telecomunicaciones	- Llamada de retorno de tipo fraudulento - Fraude de proveedores de servicios de información de líneas tipo 1-976 - Redireccionamiento de llamadas de larga distancia - Robo de línea

		- Desvío de trafico - Manipulación ilícita de equipos de telecomunicaciones - Intervención de centrales privadas
	Delitos contra la nación y actos de terrorismo	- Ciberdelincuencia ideológica: Anonymous, Lulzsec - Ciberterrorismo
	Ciberdelincuencia económica	- Malware - Spam - Phising - Scam - Ataques Dos y Ddos - Defacement
	Ciberdelincuencia social	- Ciberacoso: ciberbullying, cyberstalking y cibergrooming

Fuente: Elaboración propia.

La tabla No. 13 presenta de forma ordenada, una nueva clasificación de los delitos de alta tecnología. Este criterio gira en torno a la división realizada por Téllez Valdez pues parte de la premisa de que todo delito obedece a una de las dos naturalezas presentadas. El primer grupo reúne a aquellos delitos cuyo objeto es atentar contra sistemas informáticos. El segundo grupo en cambio va más allá, ya que estos delitos se auxilian de forma técnica de la tecnología para la comisión de ilícitos.

Esta tabla, contentiva de la categorización de los delitos de alta tecnología según la naturaleza de la acción, presenta conductas y acciones que no están tipificadas en nuestra legislación lo cual implica que no pueden ser perseguidas de forma efectiva. Estas acciones están surgiendo en nuestra sociedad lo cual implica que debemos empezar a preocuparnos por observar estas conductas y ver cuales características presentan, con el objeto de que las mismas sean insertadas en nuestra legislación.

Como bien señalamos esta propuesta contiene elementos que ya hemos definido, tal es el caso del grupo de los delitos contra sistemas informáticos, tanto los delitos contra sistemas informáticos como aquellos que se cometen contra sistemas electrónicos. Sin embargo, el caso de los delitos de alta tecnología con auxilio de de sistemas informáticos y/o electrónicos es más complejo, esto debido a que grupos como la ciberdelincuencia económica y la ciberdelincuencia social no están previstos de esta forma en nuestra ley.

A raíz de esta necesidad y siempre con miras a arrojar luz sobre este aspecto, hemos decidido analizar ambos tipos de delitos. El nivel técnico que presentan estas categorías puede resultar difícil de manejar en el ámbito jurídico, sin embargo, debemos recordar que como cualquier conducta ilícita (delito) puede aplicarse a los mismos la teoría del delito y ver si estas se corresponden con la misma.

2.2.2.1 Ciberdelincuencia económica.

La ciberdelincuencia económica, tal y como su nombre lo indica, es aquella que persigue un objetivo de carácter económico. Dentro de esta categoría de delitos se encuentran: Malware, Spam, Phising, Scam, Ataques Dos y Ddos, Defacement.

Malware:

Mateos Pascual, I. (2013) señala que el termino malware proviene de la combinación de dos términos en ingles, “malicious” y “software”, lo cual se traduce como software malicioso.

Tabla No. 14. Tipos de malware.

	Tipo	Descripción
Tipos de malware	Virus	El principal objetivo de los virus es el de servir como método de propagación a otro malware o modificar archivos del sistema para alterar su estabilidad.
	Ransomware	Esta nueva modalidad, a su vez situada entre las más lucrativas para sus autores, se trata del tipo de malware más cercano a un delito convencional: el secuestro.
	Gusanos	También llamados “Worm”, por su traducción en inglés, son un tipo de malware capaz de duplicarse por sí mismo. A diferencia de los Virus, no necesitan de la ejecución por parte del usuario sino que utilizan los propios procesos de ejecución de los sistemas.
	Troyanos	Basados en conocida la historia del caballo de Troya, esta clase de programas, sin duda el tipo de malware más abundante en la red, se presentan generalmente en forma de algún tipo de software confiable que el usuario instala de manera consciente.
	Spyware:	También conocido como software espía. Al igual que los troyanos, su comportamiento se basa en la recopilación de información del usuario de manera no permitida.
	Adware	Generalmente embebido en la descarga e instalación de software gratuito, este tipo de malware se instala in autorización por parte del usuario en su sistema y su función principal es la de mostrar y/o descargar anuncios publicitarios en la pantalla de la víctima.
	Scareware/Rogue	En ocasiones conocidos simplemente como falso software, se trata de un modo de malware que simula ser una aplicación anti-malware o de seguridad, la cual es justamente lo contrario.

Fuente: Elaboración propia, a partir de la información obtenida de Mateos Pascual, I. (2013). Ciberdelincuencia: desarrollo y persecución tecnológica.

Spam:

El 8 de agosto del presente año 2014, fue promulgada en la ciudad de Santo Domingo, Distrito Nacional, la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam). Como puede observarse, diferencia de los demás ciberdelitos económicos, el spam, está contemplado dentro de la legislación dominicana.

De acuerdo a la definición otorgada por la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), del 8 de agosto del año 2014, en su art. 2, numeral 2, spam es:

> Comunicaciones comerciales no solicitadas y/o Spam es todo mensaje de datos enviado a un número indiscriminado de personas, sin su debida autorización, dirigido a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial industrial, artesanal o profesional.

Phising:

Mateos Pascual, I. (2013) explica que esta técnica va orientada hacia la extracción de información personal de un usuario, mediante la creación de una interfaz que haga que el mismo suministre información básica y confidencial.

Tabla No. 15. Tipos de Phishing.

	Tipo	Descripción
Tipos de Phising	Smishing	La variación respecto al Phishing es que el contacto con el usuario se realiza vía sms. El usuario recibe un mensaje de texto donde se le insta a verificar sus datos o acceder a su cuenta a través de un enlace que le redirige al sitio web falsificado.
	Pharming	Al igual que el Phishing, esta técnica redirige al usuario hacia uno o varios sitios web falsos, los cuales simulan ser los auténticos.
	Pharming local	Al igual que en el caso anterior, esta técnica se basa en modificar el sistema de resolución de nombres (DNS) del usuario. La diferencia en este caso es que esta modificación se realiza únicamente de manera local en el PC de la víctima, a través de la alteración del archivo “host”.
	Vishing	Aunque podríamos considerar está técnica dentro del Phreaking, por el hecho de que el medio de contacto con el usuario sea a través del teléfono, dado que la línea de comunicación sigue siendo la red de datos se ha decidido incluirla en este punto.

Fuente: Elaboración propia, a partir de la información obtenida de Mateos Pascual, I. (2013). Ciberdelincuencia: desarrollo y persecución tecnológica.

Scam:

El término Scam es el utilizado para las estafas y los engaños realizados por medios tecnológicos. Mateos Pascual, I. (2013) señala que:

> Este tipo de estafas, no requieren de una técnica especial ni conocimientos avanzados de informática, sino que su principal arma es la ingeniería social. En ellas los delincuentes llegan a sus víctimas a través del correo ofreciendo grandes ganancias o pidiendo ayuda desde algún país de reconocida pobreza. Este tipo de estafas aparecen también en anuncios de compra/venta o webs de contactos donde los ciberdelincuentes establecen una relación con la víctima hasta conseguir engañarle y pedirle una suma de dinero para poder continuar su idilio.

Ataques Dos y Ddos:

Los ataques de Denegación de Servicio cuyas siglas en ingles son “Dos” (Denial of Service) y la versión extendida denominada “Ddos” (Distribute Denial of Services) no son más que el bloqueo o indisponibilidad de una red o sistema ya sea agotando sus recursos o saturando la misma.

Defacement:

El Defacement es la traducción inglesa de la palabra “desfiguración”. Este consiste en la alteración visual de un sitio web.

2.2.2.2 Ciberdelincuencia social: Ciberbullying, Ciberstalking, cibergrooming.

Acorde a la clasificación de delitos de alta tecnología que se ha presentado, la mayor parte de ellos persiguen un fin lucrativo, es decir una remuneración económica a cambio de las acciones ilícitas que llevan a cabo. Sin embargo, la ciberdelincuencia social rompe este esquema debido a que el objeto de esta clase de delitos no son recursos monetarios. Ahora bien, ¿Por qué se han presentado como un tipo de delito de alta tecnología? ¿Qué objeto tienen esta clase de delitos? ¿Qué perfil presentan los sujetos activos que los cometen?

Mateos Pascual, I. (2013) define la ciberdelincuencia social como:

> Aquellos delitos informáticos cometidos contra los derechos o la integridad propia de una persona, individuo o sociedad tanto en su carácter público como privado y cuyo único objetivo es el de obtener un beneficio o satisfacer una motivación, personal por parte de los ciberdelincuentes a costa de sus víctimas.

A partir de esta definición podemos deducir que este tipo de delitos, tal y como su nombre lo indica, tienen un trasfondo social y que el perfil que reviste a los agentes activos que los cometen podría estar vinculado a trastornos sociópatas y conductas antisociales per se. La mayor parte de las representaciones de estas conductas suelen darse por medios electrónicos, por lo cual han sido colocados en esta categoría.

Tabla No. 16. Tipos de ciberdlincuencia social: Ciberacoso.

	Tipo	Descripción
Ciberacoso	Ciberbullying	Término utilizado para aludir a los casos de Ciberacoso en los que, sirviéndose de los mismos medios que el anterior, tanto víctima como agresor son menores de edad.
	Cyberstalking	Con origen en el término en inglés, stalking, en español acecho, se basa en las acciones desempeñadas por algunos individuos, generalmente con algún tipo de trastorno o motivación obsesiva, mediante el uso de las tecnologías de comunicación, para acechar o acosar a una persona, grupo de personas u organización.
	Cybergrooming	Conocido también simplemente como Grooming, o Child Grooming, la utilización de este término se emplea para referirse al tipo de técnicas empleadas en los casos de acoso sexual hacia un menor a través de Internet. El principal comportamiento de los individuos que lo practican se basa en el establecimiento de una relación y control emocional sobre un menor para, posteriormente, mantener una relación sexual de manera virtual.

Fuente: Elaboración propia, a partir de la información obtenida de Mateos Pascual, I. (2013). Ciberdelincuencia: desarrollo y persecución tecnológica.

La tabla No. 16 presenta los tipos de ciberacoso y la definición de los mismos. Como puede notarse, acorde los conceptos esbozados en la tabla, todos estos tipos tienen características comunes que nos permiten reconocerlos como tal.

El “Ciberbullying” son actos de amenazas, insultos, humillaciones realizadas por parte de un individuo (sujeto activo) en contra de una persona (personas físicas o jurídicas) que se hacen públicos por los medios electrónicos y cuyas implicaciones afectan de forma social y psicológica a sus víctimas.

El término “Cyberstalking” proviene de la palabra en ingles “stalking” la cual se traduce al español como “acecho”. En esencia se trata de sujetos que se dedican a espiar y perseguir la actividad en Internet de otros sujetos, con la finalidad de realizar de forma pública declaraciones al respecto.

En cuanto al tercer término denominado como “Cybergrooming” Mateos Pascual, I. (2013) asegura que:

> Los delincuentes suelen presentarse ante sus víctimas a través de servicios de chat, redes sociales o incluso sitios web de juegos online para niños, donde estos dejan sus datos de contacto para compartir experiencias con sus iguales, presentando falsas identidades que les permitan establecer un primer contacto y una relación de amistad.

2.2.2 TEORÍA DEL DELITO APLICADA A LA CIBERDELINCUENCIA ECONÓMICA Y CIBERDELINCUENCIA SOCIAL.

Para considerar la ciberdelincuencia económica y social como delitos, deben las mismas reunir los elementos que se requieren acorde a la teoría del delito. A partir de este requerimiento podemos señalar que la ciberdelincuencia económica y la ciberdelincuencia social:

- Suponen acciones o conductas determinadas, lo cual se traduce en el primer elemento que es la acción.
- Las conductas han sido descritas técnicamente señalando cada una de ellas y plasmándolas en una figura como tal, es decir, se ha identificado la acción en concreto (elemento objetivo) y la parte volitiva (o elemento subjetivo.

- Dichas conductas son contrarias a las normas establecidas y lesionan o ponen en peligro determinados bienes jurídicos protegidos, ya sean patrimoniales o sociales.

- En las mismas no deben concurrir causas de justificación acorde a nuestras leyes (estado de necesidad, ejercicio de un derecho, cumplimiento de la ley, etc.)

- Estas acciones pueden ser imputables a un determinado sujeto (acorde a la clasificación presentada, siempre que no concurran causas de inimputabilidad como la minoría de edad, enfermedades mentales, entre otras.

- Detectados los elementos de la antijuridicidad e imputabilidad podemos deducir que un determinado sujeto puede ser catalogado como responsable de las mismas, lo cual constituye el elemento de la culpabilidad.

- En consecuencia y por la reunión en estas determinadas conductas, de los elementos del delito (acción, antijuridicidad, tipicidad, imputabilidad, culpabilidad) la misma es pasible de la imposición de una sanción, es decir una pena, previamente establecida.

Como puede observarse la ciberdelincuencia económica y la ciberdelincuencia social reúnen perfectamente los elementos que compone a todo delito. Sin embargo, estas conductas no se han incorporado de forma clara en nuestra legislación, sino que por una mala adaptación analógica son muchas veces encasilladlos en el cuerpo de otros delitos. En aras de proteger nuestros marcos legales y velar por el respeto del principio de legalidad que recubre al derecho en todas sus ramificaciones, somos de opinión que estas conductas deberían ser incorporadas a la ley 53-07, sobre crímenes y delitos de alta tecnología.

La incorporación de estos tipos penales no podría hacerse de forma efectiva mediante un reglamento o disposiciones aisladas de órganos institucionales. En este sentido la responsabilidad propiamente dicha recae sobre los órganos

legislativos, quienes deben legislar y al igual que el caso de la ley anti Spam, establecer de forma sustantiva las conductas descritas. De igual forma la jurisprudencia y los órganos judiciales tienen una cuota importante de este proceso, debido a que es deber de los mismos sentar las bases jurisprudenciales de estos delitos especiales.

CONCLUSIÓN

El presente trabajo final fue concebido con el objeto de realizar un análisis comparativo de la de la ley 53-07, sobre crímenes y delitos de alta tecnología, respecto de la clasificación y categorización que esta prevé sobre los delitos que la misma regula. Este objeto surgió ante la no identificación de los criterios bajo los cuales se realizo la división y tipificación de los delitos que en la misma se encuentran.

Tras un exhaustivo estudio del tratamiento otorgado a los delitos de alta tecnología en el marco del derecho comparado se advirtió la existencia de conductas y técnicas que teniendo lugar en nuestra realidad diaria no figuran en ningún instrumento legislativo o doctrina nacional. La ausencia de tipificación de estas conductas en nuestras leyes permite que las mismas se desarrollen en el más amplio marco de impunidad, debido a que en respeto al principio de legalidad las mismas no pueden ser perseguidas. El reconocimiento de estas conductas se hizo a partir de planteamientos doctrinales e investigaciones previas en la materia, sin embargo, ante la ausencia de los criterios puntuales para la categorización de los delitos de alta tecnología la inclusión de los mismos en nuestras leyes depende básicamente de nuevas leyes.

Partiendo de esta problemática y con el empleo de los métodos adecuados en nuestra investigación pudieron identificarse criterios internacionales, que adaptados a nuestra realidad y cultura, permiten catalogar delitos de alta

tecnología que aun no están en nuestras leyes y agrupar de forma efectiva aquellos que si lo están.

La propuesta realizada en la tabla No. 13 del segundo capítulo, presenta de forma ordenada, una nueva clasificación de los delitos de alta tecnología. Este criterio gira en torno a la división realizada por Téllez Valdez pues parte de la premisa de que todo delito obedece a una de las dos naturalezas presentadas. El primer grupo reúne a aquellos delitos cuyo objeto es atentar contra sistemas informáticos. El segundo grupo en cambio va más allá, ya que estos delitos se auxilian de forma técnica de la tecnología para la comisión de ilícitos.

En la propuesta existen grupos que ya definidos en nuestra legislación, tal es el caso del grupo de los delitos contra sistemas informáticos, tanto los delitos contra sistemas informáticos como aquellos que se cometen contra sistemas electrónicos. Sin embargo, el caso de los delitos de alta tecnología con auxilio de de sistemas informáticos y/o electrónicos resulto ser más complejo, y en consecuencia fue necesario describir y analizar grupos como la ciberdelincuencia económica y la ciberdelincuencia social que no están previstos de esta forma en nuestra ley. Para ello se definió a nivel técnico estas categorías para luego de forma categórica aplicar a los mismos la teoría del delito. El resultado que este análisis arrojo fue satisfactorio, ya que las conductas propuestas contiene todos y cada uno de los elemento requeridos para que las mismas sean consideradas como delitos propiamente dichos. Las conclusiones obtenidas en este trabajo podrían servir para investigaciones futuras, debido a que la constate evolución de la tecnología influye de forma directamente proporcional en la aparición de nuevos

delitos informáticos. Asi mismo, a partir de los resultados de la presente investigación podría legislarse con relación a los nuevos tipos penales presentados y con ello cerrar el ciclo de los mismos.

BIBLIOGRAFÍA

- ACURIO DEL PINO, S. (2008). Delitos Informáticos: Generalidades. Consultado en fecha 17 del mes de septiembre del año 2014 en: http://uvirtual.ufg.edu.sv/uvirtual/vmateriales/images/stories/recursos_master/admonce/LCE/un01tm05/cyb_ecu_delitos_inform.pdf

- Alegsa, L. (27 de octubre de 2014). Alegsa. Obtenido de http://www.alegsa.com.ar/Dic/tecnologia.php

- BORGHELLO, C. F. (2001). Seguridad Informática, sus Implicancias e Implementación. Buenos Aires. Consultado el 29 de octubre del año 2014 en: http://www.segu-info.com.ar/tesis/

- Constitución Política de la República Dominicana, proclamada el 26 de Enero del año 2010. Publicada en la Gaceta Oficial No. 10561, del 26 de enero de 2010.

- Convenio sobre la Ciberdelincuencia del Consejo de Europa, del 23 de Noviembre del 2001. Consultado el 14 de septiembre del 2014 en: http://conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm

- Cotrina, R. (2009). Obtenido de http://webcache.googleusercontent.com/search?q=cache:VdSdTFBd3QoJ:es.slideshare.net/thefighter14/delitos-informticos-2021092+&cd=1&hl=es&ct=clnk&gl=do&client=firefox-a

- Diccionario de la lengua española (DRAE). Recuperado el 1hacker 0 de septiembre 2014, de: http://lema.rae.es/drae/?val=tecnologia+

- Escuela Nacional de la Judicatura. (2007). *Teoría del Delito*. Escuela de la Judicatura. Consultado el 15 de noviembre del año 2014 en: http://www.google.com.do/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB4QFjAA&url=http%3A%2F%2Fenj.org%2Fweb%2Fdocman%2Fdoc_download%2F62-teoria-del-delito.html&ei=t-NmVIy7CsmfNsOihJgD&usg=AFQjCNHILyHAA7OxXT4TK0vawvm7G1vX9A&sig2=TN-WVYw-D_E2gpLFKF9C8g

- Española, R. A. (27 de 10 de 2014). Real Academia de la Lengua Española. Obtenido de http://lema.rae.es/drae/?val=tecnologia
- Faz, j. (s.f.). Poder judicial del Estado de Baja California . Obtenido de http://www.poder-judicial-bc.gob.mx/admonjus/n29/AJ29_004.htm
- Gálvez, J. C. L., Maraboli, M. M., & Bonvin, P. V. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. Revista Chilena de Derecho y Tecnología, 3(1). Consultado el 20 de septiembre de 2014 en: http://rchdt.uchile.cl/index.php/RCHDT/article/viewArticle/32222.
- Gamba, J. (2010). Panorama del derecho informático en América Latina y el Caribe. Consultado el 20 de septiembre del 2014 en http://repositorio.cepal.org/handle/11362/3744
- Guevara Mendoza, A. V. (2012). Aproximación a la problemática de la delincuencia informática, punibilidad y ley aplicable. Consultado el 20 de septiembre de 2014 en: http://www.tesis.uchile.cl/handle/2250/112851
- Hall, A. (s.f.). Foro de Profesionals Latinoamericanos de Seguridad . Obtenido de http://www.forodeseguridad.com/artic/discipl/disc_4016.htm
- Hofmann, M. A. E. O. LA (IN) DEFINICIÓN DEL DERECHO. SUBDIRECCIÓN DE ANÁLISIS E INVESTIGACIÓN. Consultado en fecha 15 del mes de octubre del año 2014 en: http://www.tfjfa.gob.mx/investigaciones/pdf/REVISTAPRAXISNUMERO4.pdf#page=321
- Informático, D. (2009). Alegsa. Com. [En línea]. Consultado en fecha 27 del mes de octubre del año 2014 en: http://www.alegsa.com.ar/Dic/tecnologia.php
- Larios Escamilla, J. A., & Sánchez González, R. J. (2014). Ciberdelito. Consultado en fecha 27 del mes de octubre del año 2014 en: http://www.ptolomeo.unam.mx:8080/jspui/bitstream/132.248.52.100/4884/2/Tesis.pdf

- Ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, consultado en fecha 21 del mes de septiembre del 2014 en: http://www.presidencia.gob.do/noticias/nueva-ley-310-14-regula-envio-de-correos-electronicos-comerciales-no-deseados

- Ley No. 53-07, sobre Crímenes y Delitos de Alta Tecnología, del 23 del mes de abril del año 2007.

- Manjarrés, I & Jiménez, F. (2012). Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, 71-82.consultado el 17 de septiembre del 2014 en: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoa ericano/article/view/126

- Mateos Pascual, I. (2013). Ciberdelincuencia: desarrollo y persecución tecnológica. Consultado en fecha nueve del mes de noviembre del año 2014 en: http://oa.upm.es/22176/

- Ollé Sesé, M. (2014). REFLEXIONES SOBRE CIBERDELINCUENCIA Y REDES SOCIALES DIGITALES. Revista Estudios Jurídicos. Segunda Época. Consultado el 18 de septiembre del 2014 en: http://revistaselectronicas.ujaen.es/index.php/rej/article/viewFile/1310/1087

- Orti, C. B. (s.f.). Las tecnologias de la informacion y comunicacion (T.I.C.). Valencia. http://www.uv.es/~bellochc/pdf/pwtic1.pdf

- Página principal de la Organización para la Cooperación y el Desarrollo Económico OCDE. Consultada en fecha 15 del mes de octubre del año 2014 en: http://www.oecd.org/centrodemexico/laocde/

- Paulina, J. (2007). Delitos electrónicos, informáticos y de telecomunicaciones. Consultado el 13 de octubre del año 2014 en http://do.vlex.com/vid/delitos-informa-ticos-telecomunicaciones-450232310?utm_expid=6072114-15.wkYviiCHQw-2rOlOmla-dQ.0

- PORTILLO, L. A. J. M. UNIVERSIDAD RAFAEL LANDIVAR FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES. Consultado el 15 de noviembre del año 2014 en: http://scholar.google.es/scholar?q=DELITOS+CONTRA+EL+DERECHO+DE+AUTOR%2C+LA+PROPIEDAD+INDUSTRIAL%2C+Y+DELITOS+INFORM%C3%81TICOS+LEONEL+ARMANDO+JOSE+MENDIZABAL+PORTILLO&btnG=&hl=es&as_sdt=0%2C5

- Prieto, A., Lloris, A., & Torres, J. C. (1995). Introducción a la Informática.McGraw-Hill. Consultado el 15 de septiembre del año 2014 en: http://scholar.google.es/scholar?hl=es&q=informatica%3A+&btnG=&lr=

- Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, del 30 de enero del 2003. Consultado el 28 de octubre del 2014 en: http://www.plataformaong.org/conferencia/wp-content/uploads/2014/10/Protocolo_adicional_convencion_cibercrimen.pdf

- Quintero, R. D. S. DELITOS INFORMATICOS. Consultado el nueve de noviembre del año 2014 en: http://scholar.google.es/scholar?hl=es&q=DELITOS+INFORMATICOS+Ren%C3%A9+De+Sola+Quintero&btnG=&lr=

- Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense, (47), 209-234.

- Recovery labs. Delito informático. Consultado el 17 de septiembre del 2014 en: http://delitosinformaticos.info/faqs/sobre_peritaje_informatico.html.

- Romero Echevarría, L. M. (2005). Marco conceptual de los delitos informáticos. Consultado el 29 de octubre del año 2014 en http://cybertesis.unmsm.edu.pe/handle/cybertesis/2675

- Universidad de Castilla-La mancha . (27 de octubre de 2014). Obtenido de http://edii.uclm.es/~jmlova/Archivos/IIA/Archivos/IIA_Tecnologia.pdf

- VALDIVIA, I. G., & RUBÍ, A. (2011). *DELITOS INFORMÁTICOS-CASO DE ESTUDIO* (Doctoral dissertation).Consultado en el 15 de noviembre del año 2014 en: http://www.repositoriodigital.ipn.mx/handle/123456789/12653

ANEXOS

Escuela de Graduados

Anteproyecto de trabajo final para optar por el titulo de:

Maestría en Derecho Penal y Procesal Penal

"Criterios Generales del Derecho Comparado para catalogar los delitos de alta tecnología en la República Dominicana".

Sustentante:

Massiel Victoria Pichardo Bido

2008-1511

Asesora:

Varleny I. Díaz Payano, MA

Santo Domingo, D. N.
Septiembre, 2014

ÍNDICE

I. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN.

El diccionario de la Real Academia de la Lengua Española define la palabra tecnología como: “Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico”.

En los últimos años la tecnología ha experimentado un desarrollo vertiginoso. Cada día se descubren un sin número de posibilidades y aplicaciones científicas que van separando el ayer del mañana. Las ciencias en su conjunto más amplio, las artes y la humanidad se han visto permeadas por la alta tecnología o “*hig-tech*”, lo cual nos ha vuelto dependientes y hasta cierto punto vulnerables. En definitiva los avances tecnológicos han facilitado nuestras vidas en innumerables formas, sin embargo, como cualquier herramienta esta depende del uso que se le dé y más aún, del sujeto que la posea y su intención.

Desde hace más de una década hemos observado cómo la tecnología, una herramienta tan poderosa, ha servido de base para la comisión de una serie de delitos. En principio sirvió como canal; tal es el caso de las clonaciones de tarjetas de crédito por medios electrónicos; sin embargo hoy el canal se ha convertido en el delito mismo, por ejemplo en los casos de sabotaje donde se altera o maltrata un sistema electrónico.

En el caso particular de la República Dominicana, la antigua ley General de las Telecomunicaciones No.153-98 del 27 de mayo de 1998, estatuía la obligación de respetar la inviolabilidad de las telecomunicaciones y prohibía su uso cuando fuera contrario a las leyes y las buenas costumbres. Sin embargo dejaba un vacio sobre ciertos tipos penales, imposibilitando la persecución y sanción sobre los autores de los delitos no previstos en la ley. Esto motivo la creación de una norma más vanguardista y acorde a los nuevos tiempos, la ley No. 53-07, sobre Crímenes y delitos de alta

tecnología[1]. Esta ley establece a partir de su art. 4 una serie de definiciones, dentro de la cual encontramos:

> Delito de Alta Tecnología: Aquellas conductas atentatorias a los bienes jurídicos protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Se entenderán comprendidos dentro de esta definición los delitos electrónicos, informáticos, telemáticos, cibernéticos y de telecomunicaciones.

De igual forma, esta ley enuncia a partir de su segundo título el derecho penal sustantivo a aplicar, haciendo una primera división entre los crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información; una segunda división donde se prevén lo delitos de contenido; una tercera división sobre los delitos de propiedad intelectual y afines; un cuarto capítulo sobre los delitos contra las telecomunicaciones; y un quinto capítulo sobre los delitos contra la nación y actos de terrorismo.

Sin duda alguna la estructura de la ley y la división de delitos que realiza es interesante, pues en mucho de ellos define una forma genérica conductas especificas, tratando con ello de abarcar cualquier acción que pudiera encajar en la descripción de los tipos penales que ella misma describe. Pero es estática, pues no presenta los parámetros o criterios que en un futuro nos permitan con facilidad identificar cuando estamos en presencia de un delito de alta tecnología y cuando no lo estamos.

Sin embargo, esta situación nos genera algunas inquietudes y motiva el planteamiento de las siguientes interrogantes: ¿Cuáles parámetros se utilizan en el derecho comparado para identificar acciones como delitos de alta tecnología? ¿Bajo qué criterios opera la clasificación realizada sobre los delitos de alta tecnología en la ley 53-

[1] En lo adelante (LCDAT)

07? ¿Cuáles estándares internacionales podrían ser tomados en consideración para tipificar los delitos de alta tecnología en el marco de la ley 53-07?

De estas inquietudes se desprende la formulación del problema que motiva esta investigación: ¿Cuáles criterios, extraídos del derecho comparado, podrían utilizarse en el marco de la ley 53-07 para catalogar los delitos de alta tecnología?

II. OBJETIVOS DE LA INVESTIGACIÓN.

Objetivo General:

Analizar los criterios extraídos del derecho comparado que pueden utilizarse en el marco de la ley 53-07, sobre crímenes y delitos de alta tecnología, para catalogar los delitos de alta tecnología en la República Dominicana.

Objetivos Específicos:

a) Identificar los criterios para catalogar los delitos de alta tecnología en el ámbito del Derecho Comparado.

b) Establecer la regulación sobre delitos de alta tecnología que establece la ley No. 53-07 en la República Dominicana.

III. JUSTIFICACIÓN DE LA INVESTIGACIÓN.

- **Justificación práctica:**

La investigación propuesta acerca de los delitos de alta tecnología tiene su origen en una serie de casos que se han venido suscitando, en los cuales el medio común es la tecnología y el uso de la misma. Al revisar algunos de estos casos nos encontramos

con una serie de hechos cuyas características y elementos nos lanzan hacia un nuevo modo de operación delictivo, donde los elementos constitutivos de los delitos comunes han cambiado.

La sociedad dominicana se ha visto permeada por la tecnología y sus usos. Una sociedad moderna como la nuestra debe tener los mecanismos de protección bien definidos y prever el alcance y proyección de los mismos.

Con la determinación precisa de los parámetros existentes en el ámbito internacional, podemos formular los criterios necesarios para identificar cuando una acción o hecho podría constituir un delito de alta tecnología en la República Dominicana. Con esta inclusión podrá preverse los vacíos y ambigüedades existentes en nuestra legislación, permitiendo a las autoridades y al Estado dominicano trazar una mejor política criminal para el combate de los delitos de alta tecnología.

IV. MARCO DE REFERENCIA.

a. Marco teórico:

La delincuencia informática surge y se mantiene en una estrecha relación con los avances tecnológicos, principalmente por el desarrollo que en materia computacional a nivel mundial se produjo en la década de los sesenta, pudiendo indicarse que no es un fenómeno que se delimite claramente sino que seguirá en constante evolución, lamentablemente en forma más rápida que el desarrollo del derecho llamado a reprimirlo y sancionarlo, lo cual se traduce en una gran ventaja para el delincuente informático, siendo factores relevantes en la proliferación de los mismos, entre otros, la necesidad de tener conocimientos especiales en materia informática para entender estos ilícitos y poder enfrentarlos en forma, la insuficiencia de los sistemas de seguridad para impedir su ejecución, la carencia de leyes especiales que aborden globalmente esta delincuencia, que por sus especiales características requiere un

tratamiento diverso a los tipos comunes. Huerta Miranda, M. (citado por Guevara Mendoza, 2012, P. 3)

Al buscar un concepto de delitos informáticos, nos encontramos con el aportado por Téllez Valdés, J. (citado por Landa Duran, 2007) quien define los delitos informáticos como: “Conductas típicas, antijurídicas y culpables, en las cuales las computadoras pueden ser el instrumento o el fin”. (P. 233)

Una definición más restingida es la que plantea Nidia Callegari (citada por Landa Duran, 2007) quien define al delito informático como: “Aquel que se da con la ayuda de la informática o de técnicas anexas”. (P. 233)

Con el objeto de abarcar la diversidad de medios informaticos, Cassou Ruiz, J. (2009) expresa por delito informático, suele entenderse como: “Toda aquélla conducta ilícita susceptible de ser sancionada por el derecho penal, consistente en el uso indebido de cualquier medio informático”. (P. 217)

El bien jurídico protegido en esta clase de delitos es amplio y fundamental al momento de estudiarlos. Algunos autores como Campoli, G. (citado por Cassou Ruiz, J., 2009) señalan que:

> Los delitos informáticos son aquéllos 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 indebida de medios informáticos, agrega que delitos electrónicos o informáticos electrónicos, son una especie del género delitos informáticos, en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad de los equipos electrónicos y la intimidad de sus propietarios. (p. 217)

Por otro lado Ollé Sesé, M. (2014) aborda la problemática de los ciberdelitos basándose en las redes sociales, explicando que:

> Las redes sociales digitales ofrecen indudables ventajas y bondades para los usuarios de los mismos, como, por ejemplo, la obtención y compartición de información para la diversión o para el trabajo. Sin embargo, las peculiaridades propias de lo digital llevan en ocasiones a lamentables consecuencias, convirtiéndose en un instrumento para la comisión de diferentes delitos. (P. 2)

En la República Dominicana, la ley No. 53-07, sobre crimenes y delitos de alta tecnologia, define en su art. 4 el delito de alta tecnologia como: “Aquellas conductas atentatorias a los bienes jurídicos protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Se entenderán comprendidos dentro de esta definición los delitos electrónicos, informáticos, telemáticos, cibernéticos y de telecomunicaciones”.

Recovery Labs (2012), la primera empresa en España que ha conseguido la certificación de su Sistema de Gestión de Calidad ISO 9001:2008 para sus servicios de recuperación de datos, borrado seguro y peritaje informático, plantea tres caracteristicas principales de los delitos informaticos:

a) Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.
b) Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.
c) Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos.

(P. 77)

Según el abogado e investigador Téllez Valdés, J. (citado por Majares & Jimenez, 2012) los delitos informáticos presentan caracteristicas como:

a) Son conductas criminales de cuello blanco (*white collar crime*), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se haya trabajando.
c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
d) Provocan serias pérdidas económicas, ya que casi siempre producen “beneficios económicos” al hechor.

Las características propias de este tipo de delito los ubican en un plano preferencial en cuanto a la aparición y evolución de los mismos. La aparición y avance de los delitos de alta tecnología es directamente proporcional al desarrollo de la tecnología en si misma.

Baón Ramírez (Citado por Acurio del Pino S., 2008) define la criminalidad informática como:

> La realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevadas a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).

Gamba J. (2010) sostiene que:

> Bajo un punto de vista legal, este proceso de adaptación de la normativa general a casos particulares, no previstos, aumenta el riesgo de

> impunidad, porque algunos delitos informáticos pueden no tener los requisitos mínimos de parecidos hechos penales “clásicos” (el delito de hurto en muchas legislaciones necesita de la presencia de una “posesión física” por parte del sujeto que roba, cosa que no pasa si un estafador online simplemente usa los datos de otra persona sin que los mismos entren “físicamente” en su posesión).

La República Dominicana en su afán por la efectiva protección de los derechos constitucionales y libertades de sus ciudadanos, y en ausencia de criterios generales, continuamente se ve en la obligación de legislar a los fines de poder contrarrestar efectivamente los delitos de alta tecnología debido a su avance de los mismos; este es el caso de la reciente ley No. 310-14 que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014. Esta normativa dispone en su art. 1 lo siguiente:

> Esta ley tiene como objeto regular el envío de comunicaciones comerciales, publicitaria o promocionales no solicitadas, realizadas vía correos electrónicos, sin perjuicio de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor.

Esta ley nos presenta solo una de las nuevas conductas que están surgiendo y que indudablemente puede catalogarse como un delito de alta tecnología.

b. Marco conceptual:

Computadora. De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, computadora es:

> Cualquier dispositivo electrónico, independientemente de su forma, tamaño, capacidad, tecnología, capaz de procesar datos y/o señales, que

> realiza funciones lógicas, aritméticas y de memoria por medio de la manipulación de impulsos electrónicos, ópticos, magnéticos, electroquímicos o de cualquier otra índole, incluyendo todas las facilidades de entrada, salida, procesamiento, almacenaje, programas, comunicación o cualesquiera otras facilidades que estén conectadas, relacionadas o integradas a la misma.

Comunicaciones comerciales no solicitadas y/o Spam. Acorde a lo dispuesto en la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, Spam es: “Todo mensaje de datos enviado a un número indiscriminado de personas, sin su debida autorización, dirigido a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial industrial, artesanal o profesional”.

Delito de Alta Tecnología. De a cuerdo a la definición expresada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, delito de alta tecnología es : “Aquellas conductas atentatorias a los bienes jurídicos protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Se entenderán comprendidos dentro de esta definición los delitos electrónicos, informáticos, telemáticos, cibernéticos y de telecomunicaciones”.

Delito cibernético. Según la Organización de las Naciones Unidas (ONU) (citado por Gálvez, J. C. L., Maraboli, M. M., & Bonvin, P. V. (2014) define delito cibernético como: “todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos”

Hardware. Prieto, A., Lloris, A., & Torres, J. C. (1995) definen el hardware como: “la maquina en sí; es decir, el conjunto de circuitos electrónicos, cables, dispositivos electromecánicos y otros elementos físicos que forman los ordenadores”.

Internet. Según la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, el internet es: “un sistema de redes de computación ligadas entre sí por un protocolo común especial de comunicación de alcance mundial, que facilita servicios de comunicación de datos como contenido Web, registro remoto, transferencia de archivos, correo electrónico, grupos de noticias y comercio electrónico, entre otros”.

Informática. Prieto, A., Lloris, A., & Torres, J. C. (1995), definen la informática como: “El conjunto de conocimientos científicos y técnicas que hacen posibles el tratamiento automático de la información por medio de ordenadores”.

Red Informática. De a cuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, es informática es: “Interconexión entre dos o más sistemas informáticos o entre sistemas informáticos y terminales remotas, incluyendo la comunicación por microondas medios ópticos, electrónicos o cualquier otro medio de comunicación, que permite el intercambio de archivos, transacciones y datos, con el fin de atender las necesidades de información y procesamiento de datos de una comunidad, organización o un particular”.

Sistema de Información. Según la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, Sistema de información es: “Dispositivo o conjunto de dispositivos que utilizan las tecnologías de información y comunicación, así como cualquier sistema de alta tecnología, incluyendo, pero no limitado a los sistemas electrónicos, informáticos, de telecomunicaciones y telemáticos, que separada o conjuntamente sirvan para generar, enviar, recibir, archivar o procesar información, documentos digitales, mensajes de datos, entre otros”.

Sistema Electrónico. De a cuerdo a la definición expresada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, Sistema electrónico es: “Dispositivo o conjunto de dispositivos que utilizan los

electrones en diversos medios bajo la acción de campos eléctricos y magnéticos, como semiconductores o transistores".

Sistema Informático. La ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4 defines Sistema informático como: "Dispositivo o conjunto de dispositivos relacionados, conectados o no, que incluyen computadoras u otros componentes como mecanismos de entrada, salida, transferencia y almacenaje, además de circuitos de comunicación de datos y sistemas operativos, programas y datos, para el procesamiento y transmisión automatizada de datos".

Sistema de Telecomunicaciones. según a la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, sistema de telecomunicaciones es: "Conjunto de dispositivos relacionados, conectados o no, cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales, señales electromagnéticas, signos, escritos, imágenes fijas o en movimiento, video, voz, sonidos, datos o informaciones de cualquier naturaleza, por medio óptico, celular, radioeléctrico, electromagnético o cualquiera otra plataforma útil a tales fines. Este concepto incluye servicios de telefonía fija y móvil, servicios de valor agregado, televisión por cable, servicios espaciales, servicios satelitales y otros".

Software. Para Prieto, A., Lloris, A., & Torres, J. C. (1995) software es: "el conjunto de programas ejecutables por el ordenador"

Transferencia Electrónica de Fondos (T.E.F). La ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, explica que transferencia electrónica es: "toda transferencia de fondos iniciada a través de un dispositivo electrónico, informático o de otra naturaleza que ordena, instruye o autoriza a un depositario o institución financiera a transferir cierta suma a una cuenta determinada".

Usuario. De a cuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, usuario es: “Persona física o jurídica que adquiere de manera, legítima bienes o servicios de otra”.

V. ASPECTOS METODOLÓGICOS.

TIPOS DE INVESTIGACIÓN:

Investigación aplicada: El carácter práctico es un aspecto fundamental de esta investigación, debido a que su finalidad será la aplicación de los conocimientos adquiridos. Una vez identificados los criterios de categorización de los delitos de alta tecnología contaremos con los parámetros necesarios para establecer cuando una conducta nueva constituye un ilícito de esta especie.

Investigación documental: Al implementar este tipo de investigación se recopilará la documentación e información escrita existente sobre el tema de estudio, en este caso los delitos de alta tecnología, con la finalidad de analizar y sintetizar dicha información. Asimismo podrán valorarse las diferentes leyes, tratados y acuerdos, nacionales e internacionales, que recogen las disposiciones establecidas en este tipo de delitos, todo ello basado en los escritos existentes al respecto.

Investigación descriptiva: Este tipo de investigación permitirá reseñar los parámetros establecidos para identificar los delitos de alta tecnología. Asimismo veremos en detalle cuales son los componentes y las características esenciales de algunas conductas y acciones pasibles de ser catalogadas como ilícitos informáticos.

MÉTODOS DE INVESTIGACIÓN:

Método descriptivo: Mediante el empleo de este método realizaremos una exposición detallada de los delitos de alta tecnología y los criterios existentes para la identificación de estos en el derecho comparado.

Método deductivo: Al utilizar este método se podrán identificar y estudiar características comunes de los delitos de alta tecnología, encontradas en los acuerdos, tratados internacionales y la legislación extranjera, los cuales al ser considerados en su extensión general, nos ayudaran a entender los criterios de identificación de esta clase de delitos en otros países.

Método de análisis: Aplicando este método se estudiaran a profundidad las leyes, tratados y acuerdos internacionales recopilados a los fines de realizar una distinción y clasificación de los criterios previamente identificados para extraer los elementos necesarios que permitan comprender que constituye un delito de alta tecnología dentro del derecho comparado.

Método comparativo: Mediante el empleo de este método podremos contrastar los delitos de alta tecnología identificados en las diferentes legislaciones y con ellos extraer los parámetros utilizados en cada caso.

TÉCNICAS DE INVESTIGACIÓN:

La recopilación documental: Mediante el empleo de esta técnica podremos obtener datos e información sobre el tratamiento de los delitos de alta tecnología. Teniendo en cuenta la finalidad u objetivo de esta investigación se podrá compilar los pactos, tratados, convenios, legislación y cualquier otro documento de fuentes confiables, para comparar, analizar y sintetizar la misma.

Entrevista: Con preguntas abiertas a profesionales expertos en informática sobre el tratamiento que se le da a los delitos de alta tecnología.

VI. TABLA DE CONTENIDO PRELIMINAR.

VII. BIBLIOGRAFÍA PRELIMINAR.

ACURIO DEL PINO, S. (2008). Delitos Informáticos: Generalidades. Consultado en fecha 17 del mes de septiembre del año 2014 en: http://uvirtual.ufg.edu.sv/uvirtual/vmateriales/images/stories/recursos_master/admonce/LCE/un01tm05/cyb_ecu_delitos_inform.pdf

Constitución Política de la República Dominicana, proclamada el 26 de Enero del año 2010. Publicada en la Gaceta Oficial No. 10561, del 26 de enero de 2010.

Convenio sobre la Ciberdelincuencia del Consejo de Europa, del 23 de Noviembre del 2001. Consultado el 14 de septiembre del 2014 en: http://conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm

Diccionario de la lengua española (DRAE). Recuperado el 1hacker 0 de septiembre 2014, de: http://lema.rae.es/drae/?val=tecnologia+

Gálvez, J. C. L., Maraboli, M. M., & Bonvin, P. V. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. Revista Chilena de Derecho y Tecnología, 3(1). Consultado el 20 de septiembre de 2014 en: http://rchdt.uchile.cl/index.php/RCHDT/article/viewArticle/32222.

Gamba, J. (2010). Panorama del derecho informático en América Latina y el Caribe. Consultado el 20 de septiembre del 2014 en http://repositorio.cepal.org/handle/11362/3744

Guevara Mendoza, A. V. (2012). Aproximación a la problemática de la delincuencia informática, punibilidad y ley aplicable. Consultado el 20 de septiembre de 2014 en: http://www.tesis.uchile.cl/handle/2250/112851

Ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, consultado en fecha 21 del mes de septiembre del 2014 en: http://www.presidencia.gob.do/noticias/nueva-ley-310-14-regula-envio-de-correos-electronicos-comerciales-no-deseados

Ley No. 53-07, sobre Crímenes y Delitos de Alta Tecnología, del 23 del mes de abril del año 2007.

Manjarrés, I & Jiménez, F. (2012). Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, 71-82.consultado el 17 de septiembre del 2014 en: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/view/126

Ollé Sesé, M. (2014). REFLEXIONES SOBRE CIBERDELINCUENCIA Y REDES SOCIALES DIGITALES. Revista Estudios Jurídicos. Segunda Época. Consultado el 18 de septiembre del 2014 en: http://revistaselectronicas.ujaen.es/index.php/rej/article/viewFile/1310/1087

Prieto, A., Lloris, A., & Torres, J. C. (1995). Introducción a la Informática.McGraw-Hill. Consultado el 15 de septiembre del año 2014 en: http://scholar.google.es/scholar?hl=es&q=informatica%3A+&btnG=&lr=

Recovery labs. Delito informático. Consultado el 17 de septiembre del 2014 en: http://delitosinformaticos.info/faqs/sobre_peritaje_informatico.html.

GLOSARIO

Acceso Ilícito: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, acceso ilícito es: El hecho de ingresar o la intención de ingresar sin autorización, o a través del acceso de un tercero, a un sistema de información, permaneciendo o no en él.

Afectar: De conformidad con la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, afectar es: Alterar, provocar anomalías en cualquiera de las operaciones a realizar por un programa, software, sistema, red de trabajo, o a la computadora misma, impidiendo su uso normal por parte del usuario.

Campo del asunto: Acorde a la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, campo del asunto es: El área que contiene una breve descripción del contenido del mensaje.

Clonación: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, clonación es: Duplicación o reproducción exacta de una serie electrónica, un número o sistema de identificación de un dispositivo o un medio de acceso a un servicio.

Código de Acceso: La ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4 define código de acceso como: Información o contraseña que autentica a un usuario autorizado en un sistema de información, que le permite el acceso privado y protegido a dicho sistema.

Código de Identificación: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, código de identificación es: Información, clave o mecanismo similar, que identifica a un usuario autorizado en un sistema de información.

Código Malicioso: conforme a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, código malicioso es: Todo programa, documento, mensaje, instrucciones y/o secuencia de cualquiera de éstos, en un lenguaje de programación cualquiera, que es activado induciendo al usuario quien ejecuta el programa de forma involuntaria y que es susceptible de causar algún tipo de perjuicio por medio de las instrucciones con las que fue programado, sin el permiso ni el conocimiento del usuario.

Computadora: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, computadora es: Cualquier dispositivo electrónico, independientemente de su forma, tamaño, capacidad, tecnología, capaz de procesar datos y/o señales, que realiza funciones lógicas, aritméticas y de memoria por medio de la manipulación de impulsos electrónicos, ópticos, magnéticos, electroquímicos o de cualquier otra índole, incluyendo todas las facilidades de entrada, salida, procesamiento, almacenaje, programas, comunicación o cualesquiera otras facilidades que estén conectadas, relacionadas o integradas a la misma.

Comunicaciones comerciales no solicitadas y/o Spam. Acorde a lo dispuesto en la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, Spam es: “Todo mensaje de datos enviado a un número indiscriminado de personas, sin su debida autorización, dirigido a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial industrial, artesanal o profesional”.

Consentimiento del interesado. Según lo dispuesto en la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, consentimiento del interesado es: Toda manifestación de voluntad, libre, inequívoca, espcdlica e informada, mediante la que el interesado consienta el envío de comunicaciones comerciales.

Criptografía: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, criptografía es: Rama de las matemáticas aplicadas y la ciencia informática que se ocupa de la transformación de documentos digitales o mensajes de datos, desde su presentación original a una representación ininteligible e indescifrable que protege su confidencialidad y evita la recuperación de la información, documento o mensaje original, por parte de personas no autorizadas.

Datos: La ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, define datos como: Es toda información que se transmite, guarda, graba, procesa, copia o almacena en un sistema de información de cualquiera naturaleza o en cualquiera de sus componentes, como son aquellos cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales electromagnéticas, signos, señales, escritos, imágenes fijas o en movimiento, video, voz, sonidos, datos por medio óptico, celular, radioeléctrico, sistemas electromagnéticos o cualquier otro medio útil a tales fines.

Datos relativos a los usuarios: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, los datos relativos a los usuarios son: Se entenderá toda información en forma de datos informáticos o de cualquiera otra forma, que posea un proveedor de servicios y que esté relacionada con los usuarios a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:

a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio;

b) La identidad, la dirección postal o geográfica y el número de teléfono del usuario, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;

c) Cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

Delito de alta tecnología: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, delito de alta tecnología son: Aquellas conductas atentatorias a los bienes jurídicos protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Se entenderán comprendidos dentro de esta definición los delitos electrónicos, informáticos, telemáticos, cibernéticos y de telecomunicaciones.

Delito cibernético. Según la Organización de las Naciones Unidas (ONU) (citado por Gálvez, J. C. L., Maraboli, M. M., & Bonvin, P. V. (2014) define delito cibernético como: “todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos”

Destinatario: Según lo dispuesto en la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, el destinatario es: La persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a titulo de intermediario con respecto a ese mensaje. A los fines de la presente ley, si un desti natario tiene una

o más direcciones electrónicas adicionales a la dirección a la cual le fue enviado el mensaje, el destinatario deberá ser tratado como un destinatario distinto a cada una de sus direcciones.

Desvío de facilidades contratadas: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, el desvío de facilidades contratadas es: Se produce cuando se contratan facilidades de transmisión de tráfico de gran capacidad para uso privado y posteriormente, se les emplea con fines comerciales sin la autorización de la prestadora de servicios.

Desvío de Servicios: según la definición referida por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, el desvío de servicios: Se produce cada vez que se conectan irregularmente las facilidades internacionales a la red pública conmutada para terminar tráfico.

Dispositivo: De acuerdo a la definición contenida en por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, un dispositivo es: Objeto, artículo, pieza, código, utilizado para cometer delitos de alta tecnología.

Dispositivo de acceso: De acuerdo a la definición dispuesta por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, un dispositivo de acceso: Es toda tarjeta, placa, código, número, u otros medios o formas de acceso, a un sistema o parte de éste, que puedan ser usados independientemente o en conjunto con otros dispositivos, para lograr acceso a un sistema de información o a cualquiera de sus componentes.

Documento digital: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, documento digital: Es la información codificada en forma digital sobre un soporte

lógico o físico, en el cual se usen métodos electrónicos, fotolitográficos, ópticos o similares, que se constituyen en representación de actos, hechos o datos.

Hardware. Prieto, A., Lloris, A., & Torres, J. C. (1995) definen el hardware como: "la maquina en sí; es decir, el conjunto de circuitos electrónicos, cables, dispositivos electromecánicos y otros elementos físicos que forman los ordenadores".

Informática. Prieto, A., Lloris, A., & Torres, J. C. (1995), definen la informática como: "El conjunto de conocimientos científicos y técnicas que hacen posibles el tratamiento automático de la información por medio de ordenadores".

Información de cabecera: Según la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, la informacion de cabecera es: La fuente. destino y ruta de la información adjunta en un mensaje de datos, incluyendo el nombre de dominio de origen y la dirección electrónica de origen y toda otra información que aparezca en la linea identificadora, que permita de manera fehaciente el origen real y el camino seguido por el correspondiente mensaje de datos.

Iniciador: De acuerdo a lo dispuesto en la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, el iniciador es: Toda persona que, al tenor de un mensaje de datos, haya actuado por su cuenta o en cuyo nombre se haya actuado, para enviar o generar dicho mensaje antes de ser archivado, si este es el caso, pero que no lo haya hecho a título de intermediario con respecto a ese mensaje.

Interceptación: De acuerdo a la definición que aparece en la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, la interceptación es: Apoderar, utilizar, afectar, detener, desviar, editar o mutilar, de cualquier forma un dato o una transmisión de datos perteneciente a otra

persona física o moral, por su propia cuenta o por encargo de otro, para utilizar de algún modo o para conocer su contenido, a través de un sistema de información o de cualquiera de sus componentes.

Intermediario. Según la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, el intermediaio es: Toda persona que, en relación con un determinado mensaje de datos actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él.

Internet: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, internet: Es un sistema de redes de computación ligadas entre sí por un protocolo común especial de comunicación de alcance mundial, que facilita servicios de comunicación de datos como contenido Web, registro remoto, transferencia de archivos, correo electrónico, grupos de noticias y comercio electrónico, entre otros.

Mensajes de datos. Según la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, un mensaje de datos es: La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), el correo electrónico, el telegrama, el télex, el telefax, el Servicio de Mensajes Cortos (SMS) o el Servicio de Mensajes Multimedia (MMS).

Pornografía infantil: Según la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, la pornografía infantil es: Toda representación, por cualquier medio, de niños, niñas y adolescentes, dedicados a actividades sexuales explícitas, reales o simuladas o toda representación de las partes genitales de niños, niñas y adolescentes con fines primordialmente sexuales. Se considera niño o niña, a toda persona desde su

nacimiento hasta los doce años, inclusive, y adolescente, a toda persona desde los trece años hasta alcanzar la mayoría de edad.

Proveedores de servicios. Según la ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (spam), de fecha 08 del mes de agosto del año 2014, proveedor de servicios es: Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de enviar datos informáticos a través de un sistema informático. Se entenderá también como proveedor de servicios cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.

Red informática: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, red informática es: Interconexión entre dos o más sistemas informáticos o entre sistemas informáticos y terminales remotas, incluyendo la comunicación por microondas medios ópticos, electrónicos o cualquier otro medio de comunicación, que permite el intercambio de archivos, transacciones y datos, con el fin de atender las necesidades de información y procesamiento de datos de una comunidad, organización o un particular.

Salario mínimo: La ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, establece que: Para los fines de la presente ley, se entenderá como el salario mínimo nacional más bajo percibido por los trabajadores del sector privado no sectorizado de empresas industriales, comerciales y de servicios, fijado por el Comité Nacional de Salarios de la Secretaría de Estado de Trabajo de la República Dominicana.

Señal de disparo: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, señal de disparo es: Señal generada a una plataforma la cual devuelve el tono de

marcar, ya sea proveniente de un sistema de información o a través de un operador.

Sin autorización: La ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4**,** define el termino “sin autorización” como: Sin facultad o autoridad legal, estatutaria, reglamentaria o de cualquier otra índole para poseer, usar o hacer algo, sin tener poder legítimo. Esto incluye la falta o carencia total de autorización, expresa o tácita, y la transgresión del límite de la autorización que se posee.

Sistema de información: De acuerdo a la definición otorgada por la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, sistema informático es: Dispositivo o conjunto de dispositivos que utilizan las tecnologías de información y comunicación, así como cualquier sistema de alta tecnología, incluyendo, pero no limitado a los sistemas electrónicos, informáticos, de telecomunicaciones y telemáticos, que separada o conjuntamente sirvan para generar, enviar, recibir, archivar o procesar información, documentos digitales, mensajes de datos, entre otros.

Sistema electrónico: Según la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, sistema electrónico es: Dispositivo o conjunto de dispositivos que utilizan los electrones en diversos medios bajo la acción de campos eléctricos y magnéticos, como semiconductores o transistores.

Sistema informático: Según la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, sistema informático es: Dispositivo o conjunto de dispositivos relacionados, conectados o no, que incluyen computadoras u otros componentes como mecanismos de entrada, salida, transferencia y almacenaje, además de circuitos de comunicación de datos y

sistemas operativos, programas y datos, para el procesamiento y transmisión automatizada de datos.

Sistema de telecomunicaciones: En el contexto de la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, sistema de telecomunicaciones es: Conjunto de dispositivos relacionados, conectados o no, cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales, señales electromagnéticas, signos, escritos, imágenes fijas o en movimiento, video, voz, sonidos, datos o informaciones de cualquier naturaleza, por medio óptico, celular, radioeléctrico, electromagnético o cualquiera otra plataforma útil a tales fines. Este concepto incluye servicios de telefonía fija y móvil, servicios de valor agregado, televisión por cable, servicios espaciales, servicios satelitales y otros.

Sistema telemático: Según la ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, sistema telemático es: Sistema que combina los sistemas de telecomunicaciones e informáticos como método para transmitir la información.

Spam: De acuerdo a la definición otorgada por la ley No. 310-14, que regula el envio de correos electrónicos comerciales no solicitados (spam), del 8 de agosto del año 2014, en su art. 2, numeral 2, spam es: Comunicaciones comerciales no solicitadas y/o Spam es todo mensaje de datos enviado a un número indiscriminado de personas, sin su debida autorización, dirigido a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial industrial, artesanal o profesional.

Software. Para Prieto, A., Lloris, A., & Torres, J. C. (1995) software es: “el conjunto de programas ejecutables por el ordenador”

Sujeto Activo: La ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, define sujeto activo como: Aquel que intencionalmente viole o intente violar, por acción, omisión o por mandato, cualquiera de las actuaciones descritas en la presente ley. A los fines de la presente ley se reputa como sujeto activo a los cómplices, los cuales serán pasibles de ser condenados a la misma pena que el actor principal de los hechos.

Sujeto Pasivo: La ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, define sujeto pasivo como: todo aquel que se sienta afectado o amenazado en cualquiera de sus derechos por la violación de las disposiciones de la presente ley.

Transferencia Electrónica de Fondos (T.E.F): La ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, define T.E.F. como: Es toda transferencia de fondos iniciada a través de un dispositivo electrónico, informático o de otra naturaleza que ordena, instruye o autoriza a un depositario o institución financiera a transferir cierta suma a una cuenta determinada.

Usuario: La ley 53-07, sobre crímenes y delitos de alta tecnología, del 23 de abril del año 2007, en su artículo 4, conceptualiza el término usuario como: Persona física o jurídica que adquiere de manera, legítima bienes o servicios de otra.

Entrevista:

Esta entrevista es estructurada, y cuenta con una serie de preguntas abiertas cuyo objeto es recoger la mayor cantidad de información posible sobre el tema en cuestión y la apreciación de los entrevistados al respecto. La información obtenida en esta entrevista sera de uso académico exclusivamente.

Nombre: _____

Empresa o Institución: _____

Cargo: _____

1. ¿Qué considera usted como alta tecnología?

2. ¿Qué diferencia existe entre los siguientes términos: Delito informático, delito de alta tecnología y delito cibernético?

3. ¿Cómo podría definir delitos de alta tecnología?

4. ¿Cuáles conductas denominadas como delitos de alta tecnología conoce?

5. ¿Conoce usted la ley 53-07 sobre crimenes y delitos de alta tecnologia? En caso de conocerla ¿Cuál es su opinión sobre ella?

6. ¿Cuáles delitos de alta tecnología se presentan en el desarrollo de su trabajo?

7. ¿Cuáles conductas, según su criterio, podrían constituir delitos de esta especie?

Gracias por su atención.