HURTO POR MEDIOS INFORMÁTICOS ¿UN DELITO INFORMÁTICO?

MAJER ABUSHIHAB

2016

TABLA DE CONTENIDO

INTRODUCCIÓN.....	5
CAPÍTULO I. APROXIMACIÓN A LOS DELITOS INFORMÁTICOS	12
1. <i>Postura que adopta el concepto de Cibercrimen.....</i>	<i>13</i>
1.1. <i>Fundamentos de la postura</i>	<i>14</i>
1.1.1. <i>El cibercrimen es un concepto más adecuado para definir las conductas cometidas mediante “internet”</i>	<i>14</i>
1.1.2. <i>El concepto de cibercrimen abarca mayor cantidad de conductas</i>	<i>15</i>
1.1.3. <i>El concepto de cibercrimen es un concepto complementario</i>	<i>17</i>
1.2. <i>Críticas a la postura</i>	<i>18</i>
1.2.1. <i>El concepto de cibercrimen no aglomera delitos que atenten contra un mismo bien jurídico, lo que imposibilita un estudio sistemático.....</i>	<i>18</i>
1.2.2. <i>El concepto de cibercrimen es excesivamente amplio.....</i>	<i>19</i>
1.2.3. <i>El cibercrimen es un delito común cometido a través de medios cibernéticos</i>	<i>20</i>
2. <i>Postura que adopta el concepto de delito informático en sentido amplio.....</i>	<i>20</i>
2.1. <i>Fundamento de la adopción de la acepción delito informático en sentido amplio</i>	<i>22</i>
2.2. <i>Criticas al concepto de delito informático en sentido amplio</i>	<i>23</i>
2.2.1. <i>Excesiva vaguedad y amplitud del concepto.....</i>	<i>23</i>
2.2.2. <i>Imposibilidad de aproximación dogmática idéntica</i>	<i>24</i>
2.2.3. <i>Falta de fundamento para el estudio conjunto de delitos informáticos como concepto extensivo.....</i>	<i>24</i>
3. <i>Toma de postura: adopción del concepto de delito informático en sentido limitado</i>	<i>25</i>
<i>Fundamentos de la adopción del concepto de delito informático en sentido limitado....</i>	<i>26</i>
3.1. <i>El objeto de protección es la “informática”. Esa es la razón para denominarlos delitos “informáticos”</i>	<i>26</i>
3.2. <i>El delito informático en sentido limitado se encuentra compuesto por un conjunto de delitos que afectan un mismo bien jurídico</i>	<i>27</i>
3.3. <i>Posibilidad de estudio contiguo de los delitos informáticos entendidos en sentido restringido</i>	<i>27</i>
3.4. <i>Bien jurídico autónomo.....</i>	<i>28</i>
4. <i>Principales atentados en contra de sistemas informáticos, telemáticos y de la información allí contenida.....</i>	<i>29</i>
4.1. <i>“Hacking” o acceso no consentido a sistemas informáticos.....</i>	<i>29</i>

4.2.	<i>Sabotaje informático</i>	33
5.	<i>Aspectos criminológicos del delito informático</i>	37
5.1.	<i>La aparición de nuevos riesgos como fundamento de la punición del delito informático</i>	38
5.2.	<i>Los riesgos generados con la aparición de las redes informáticas y telemáticas. Manifestaciones concretas de la aparición del delito informático</i>	40
5.2.1.	<i>El acceso abusivo a bases de datos y sistemas informáticos</i>	41
5.2.2.	<i>La interceptación de telecomunicaciones a través del ciberespacio</i>	43
5.2.3.	<i>La reproducción y transmisión de contenido ilícito mediante sistemas informáticos y telemáticos</i>	43
5.3.	<i>Principales causas en las que radica la peligrosidad de los riesgos generados por el surgimiento de los sistemas informáticos y telemáticos</i>	45
5.3.1.	<i>Anonimidad en la comisión del delito</i>	46
5.3.2.	<i>Facilidad de encubrir los hechos y borrar las pruebas</i>	48
5.2.	<i>Perfil criminológico del delincuente informático</i>	49
5.3.	<i>Perfil criminológico de la víctima informática</i>	53
5.4.	<i>Algunas cifras relativas a los delitos informáticos</i>	55
6.	<i>¿Es necesaria la existencia de delitos típicamente informáticos?</i>	56
6.1.	<i>Justificación de la existencia de los delitos típicamente informáticos. Necesaria referencia a la creación de un nuevo bien jurídico</i>	58
6.1.1.	<i>Postura que niega la existencia de un nuevo bien jurídico</i>	59
6.1.2.	<i>Postura que afirma la existencia de un nuevo bien jurídico</i>	61
6.1.3.	<i>Toma de postura</i>	63
6.1.3.1.	<i>Dependencia de la organización social en los sistemas y redes informáticos</i> 64	
6.1.3.2.	<i>La Insuficiencia de las figuras delictivas clásicas para la protección de las bases de datos</i>	66
6.1.3.3.	<i>Protección temprana de otros bienes jurídicos</i>	68
6.2.	<i>Si existe un nuevo bien jurídico, entonces, ¿cuál es?, y ¿en qué consiste ese bien jurídico?</i> 69	
CAPÍTULO II. EL DELITO INFORMÁTICO EN OTROS ORDENAMIENTOS JURÍDICOS		73
1.	<i>CONVENIO DE BUDAPEST SOBRE CIBERCRIMINALIDAD</i>	73
1.1.	<i>Acceso ilícito</i>	74
1.2.	<i>Interceptación ilícita</i>	75
1.3.	<i>Ataques a la integridad de los datos</i>	76
1.4.	<i>Ataques a la integridad del sistema</i>	77
1.5.	<i>Conclusión parcial</i>	78
2.	<i>ESPAÑA</i>	79
2.1.	<i>El descubrimiento de secreto recogido en archivo o registro. Artículo 197 apartado 2 Código Penal español</i>	80

2.2.	Acceso a datos y sistemas informáticos. Artículo 197bis del Código Penal español	83
2.3.	Sabotaje Informático. Artículo 264 Código Penal español.....	86
2.4.	Interrupción de funcionamiento de sistema informático. Artículo 264 bis del Código Penal español.	89
3.	ITALIA	90
3.1.	Daño a informaciones, datos y sistemas informáticos ajenos. Artículo 635-bis Código Penal italiano.	90
3.2.	Daños a sistemas informáticos o telemáticos. Art. 635-quater. Código Penal italiano.	91
3.3.	Daños a datos y a sistemas informáticos públicos o de utilidad pública. Arts. 635-ter y 635-quinques del Código Penal italiano.	93
4.	CHILE	94
4.1.	Daño o inutilización en contra de un sistema de tratamiento de datos	95
4.2.	Acceso a sistema de tratamiento de datos (sistema informático) con fines de espionaje	97
4.3.	Daño en contra de los datos contenidos en el sistema	98
4.4.	Revelación de los datos contenidos en un sistema de información	99
	CAPITULO III. HURTO POR MEDIOS INFORMÁTICOS.	101
1.	Perspectiva general del hurto por medios informáticos.....	102
2.	El bien jurídico protegido por el hurto por medios informáticos	104
2.1.	Primera postura. El bien jurídico protegido es el de la información y los datos	105
2.1.1.	Ubicación del tipo penal de hurto por medios informáticos	105
2.2.	Segunda postura. El bien jurídico protegido es el patrimonio económico	109
2.2.1.	Remisión en la conducta	109
2.2.2.	Remisión en la sanción.....	110
2.3.	Posturas mixtas.....	112
3.	Análisis dogmático del tipo penal de hurto por medios informáticos	115
3.1.	Elementos Objetivos	115
3.1.1.	Sujetos activo y pasivo	116
3.1.2.	Conducta	117
3.1.3.	Medios determinados	118
3.1.4.	Objeto material sobre el que recae la acción.....	122
3.2.	Elementos subjetivos del tipo penal.....	124
3.3.	Conclusiones parciales	124
3.3.1.	El hurto por medios informáticos es un delito subordinado.....	125
3.3.2.	El hurto por medios informáticos es un tipo penal de medios determinados	126
3.3.3.	El hurto por medios informáticos no es un delito informático	126

4.	<i>Problemas derivados de la tipificación autónoma del hurto por medios informáticos. Proposición de solución a esos problemas</i>	<i>127</i>
4.1.	<i>Concurso aparente de tipos penales con la circunstancia de calificación del hurto. Art. 240, numeral 4 del Código Penal colombiano.</i>	<i>128</i>
4.2.	<i>Ubicación deficiente del tipo penal de hurto por medios informáticos</i>	<i>130</i>
4.3.	<i>Diferenciación en la competencia de tipos penales idénticos.....</i>	<i>132</i>
4.4.	<i>Incoherencia y falta absoluta de razones de política criminal</i>	<i>134</i>
CAPÍTULO IV: PROPUESTA PARA SUPERAR ESTAS FALENCIAS		136
CONCLUSIONES		139
BIBLIOGRAFÍA		144

INTRODUCCIÓN

El riesgo en las sociedades modernas y aún en la historia misma de la humanidad, ha justificado el accionar del derecho penal en una función preventiva del crimen, que busca no solo sancionar o castigar el delito, sino con una anticipación de las barreras punitivas del Estado (ex ante), para procurar su prevención, como lo explica Paladines, (2012): “el riesgo desmantela la función del derecho penal, obligándolo a reprimir el futuro” (p. 17), esto supone que las categorías del delito se direccionen hacia la criminalización de meras expectativas y se antepongan a las actuaciones concretas o a la materialidad de conductas que lesionan efectivamente bienes jurídicos.

No obstante lo anterior, la sociedad del riesgo lleva consigo la necesidad de aceptar actividades que se enmarcan dentro del concepto de riesgo permitido, en tanto que las mismas se adecuen a los parámetros socialmente aceptados y al respeto de los derechos ajenos. Las Tecnologías de la Información, entendidas como “los procesos de producción de contenidos: prensa escrita, prensa electrónica, producción multivisual, datos y textos”

(Rodríguez, 2004, p. 12), y por otro lado las Tecnologías de las Comunicaciones definidas como aquellas “que permiten la utilización de las plataformas de espectro radioeléctrico, redes y aplicaciones, tales como posiciones orbitales, bandas y frecuencias; redes físicas, satelitales e híbridas; telefonía fija e inalámbrica y Protocolo IP” (Rodríguez, 2004, p. 12) , en pleno siglo XXI, adquieren una relevancia inusitada que se materializa en el propio desarrollo de las sociedades, y cuyo avance lleva a situaciones que años atrás eran impensables para el hombre, implicando necesariamente "... la aceptación de un riesgo implícito e inevitable" (Álvarez, 2003, p. 112).

Desde el punto de vista social, la tecnología es una herramienta que suple necesidades y propende por la realización del ser humano y de lo que hoy en día concebimos como mundo globalizado, que por demás incide en las políticas criminales de los Estados pues "Dado el carácter transnacional de este tipo de delincuencia, muchas veces la decisión de penalizar determinadas conductas no depende de la determinación autónoma de cada país" (Prías, 2006, p. 13).

Bajo el mismo tópico es importante referir que la delincuencia como fenómeno social y dentro de ella el delincuente como actor directo de dicho fenómeno, acuden a mecanismos sofisticados cuya base y desarrollo se derivan justamente de los avances tecnológicos lo que requiere una reacción del aparato represor del Estado ya que “cada vez es más habitual encontrar en la página de sucesos algún ilícito, por lo general de dimensiones grandilocuentes, en el que esté presente, de alguna forma, el uso abusivo de las altas tecnologías de la información” (Balmaceda, 2009, p.46).

De esta forma entonces, la tecnología como mecanismo de desarrollo, se torna de manera paralela en un instrumento que diluye el actuar del delincuente y facilita la realización de conductas delictivas pues la identificación del sujeto activo se dificulta y por ende acudir a dichos mecanismos resulta más atractivo y de mayor rentabilidad, sin dejar de lado en igual medida, la importancia de la persecución penal como quiera que la organización social esta cimentada en un esquema informático como lo afirma Rueda (2009):

Nuestra organización social (la administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte, las empresas, los particulares, etc.) ha pasado a depender de forma extraordinaria de unos sistemas y redes informáticos, por lo que de los riesgos que se derivan de su vulnerabilidad ha surgido, consecuentemente, un interés en la seguridad de la utilización de las TIC... (p. 183).

Teniendo en cuenta que la tecnología y la informática avanzan conjuntamente en magnitudes insospechadas y a velocidades incalculables, el derecho y con él la regulación en el entorno colombiano, deben acompasarse y adecuarse a las necesidades y retos que imponen tales desarrollos, pues "Las primeras manifestaciones de legislación en materia de sistemas e informática cuentan ya con al menos dos décadas de desarrollo" (Prias, 2006, p. 10). Es así, como los Estados y dentro de ellos Colombia (a partir del año 2009), han incorporado al ordenamiento jurídico-penal, una serie de conductas que han

pretendido hacer frente a los llamados delitos “informáticos”, presentando ya un problema en punto del objeto de protección –bien jurídico tutelado-, pues por ejemplo para el caso colombiano, el bien jurídico ha sido denominado “protección de la información y de los datos”, concepto que si bien es adecuado, no es del todo acertado y menos consecuente con algunas de las conductas delictivas allí desarrolladas, como por ejemplo el ilícito de hurto por medios informáticos, el cual será abordado y analizado con suficiencia en el presente trabajo.

La determinación clara de los bienes jurídicos protegidos para el esquema de la teoría del delito, y especialmente para la verificación de su real afectación o puesta efectiva en peligro (antijuridicidad material), es un punto de especial relevancia en la construcción de la teoría que debe gobernar esta nueva e inexplorada vertiente del derecho penal; desde antaño se advertía la dificultad del establecimiento y delimitación del bien jurídico:

La primera dificultad, es la de establecer el objeto jurídico a tutelar, pues como se deduce de esto, mediante la utilización delictiva de los diversos servomecanismos o aparatos cibernéticos, son muchos los tipos que se pueden estructurar y muy diversos los bienes e intereses jurídicos que se pueden menoscabar. (Solano, 1997, p. 281)

Situación que inclusive al día de hoy no es pacífica como lo afirman Rey & Nuñez (2011): "Es claro que para la doctrina ha sido de suma dificultad definir unánimemente el delito informático y precisar el bien jurídico protegido" (p. 626), lo que hace necesario que se

continúe aportando al desarrollo en este sentido.

De esta forma entonces, la tecnología y dentro de ella la informática son conceptos afines con los problemas actuales del derecho penal y especialmente con toda la moderna teoría del derecho penal económico, pues aunque los medios informáticos pueden, y de hecho son utilizados para la comisión de una amplia gama de delitos, la mayoría de los casos, y dentro de ellos la delincuencia organizada y sofisticada, persigue un interés de contenido económico y una facilidad tecnológica que pueda ser utilizada como puente para alcanzar ese objetivo.

Por otro lado, no puede despreciarse la relevancia que ha adquirido la información (bases de datos y confidencialidad de ellos) como fuente de negocio y como mecanismo de comisión de delitos, situación que toca temas de responsabilidad empresarial, máxime con los avances en materia de protección de la información en campos inclusive extrapenales.

Además de lo anterior, surgen igualmente interrogantes acerca del potencial delictivo de generaciones modernas que nacen rodeadas de medios tecnológicos e informáticos “Muy a menudo se trata de intrusiones realizadas por parte de jóvenes *hacker* con el fin de averiguar el nivel de seguridad de los sistemas informáticos o para demostrar sus habilidades para infringir las medidas de seguridad que los protegen” (Salvadori, 2013, p. 6), lo que permite efectuar un estudio criminológico sobre factores propios del entorno social aterrizados sobre quienes pueden constituir posibles sujetos activos de este tipo de delitos, y cuya facilidad de acceso se evidencia con los avances sociales y por supuesto tecnológicos.

De otra parte, la creación de un mundo paralelo denominado *ciberespacio* es una realidad, que pese a ser un escenario incorporeal tiene una connotación real y verificable con importantes implicaciones en preciados bienes de la comunidad:

Según funcionarios estadounidenses, después del 11 de septiembre el próximo campo de batalla será el ciberespacio. Es otro tipo de guerra distinta a la convencional donde los sistemas informáticos, lejos del cumplimiento de fines exclusivamente filantrópicos, son, antes que cualquier cosa, instrumentos y al mismo tiempo un espacio de confrontaciones igualmente aterradoras. (Guerrero, 2004, p. 21)

Así las cosas, la problemática de la delincuencia informática, presenta grandes desafíos a la comunidad jurídica especializada. No obstante ello, sería además de infructuoso, imposible abordar todas y cada una de esas problemáticas, por lo que nos centraremos en algunas de ellas las cuales hacen específica relación con el título, pero además presentan un escenario de discusión actual y relevante para la realidad colombiana en la materia, aspecto que como se verá ya incluso ha sido planteado ante los altos tribunales, sin que lo allí expuesto sea suficiente para el aporte a la problemática.

El presente trabajo busca entonces fijar la discusión actual en materia de ciberdelitos y delitos informáticos, aspecto de trascendental importancia para identificar el estado actual de la cuestión, para con posterioridad definir el bien jurídico que consideramos debe ser objeto de protección, pero especialmente, presentando una propuesta que

permita acoger el concepto más adecuado a la problemática de la realidad colombiana, y concretamente los ilícitos con que el derecho penal colombiano pretende proteger el bien jurídico tutelado.

Una vez sentado este asunto, entraremos a la discusión directa del delito de hurto por medios informáticos, para analizarlo, determinar sus elementos y establecer cuál es su real objeto de protección, así como la ubicación que debe presentarse de conformidad con la estructura jurídica colombiana.

En otras palabras, la hipótesis de investigación que se pretende resolver en este texto va encaminada a determinar cuál es la naturaleza del hurto por medios informáticos, qué bien jurídico protege, y cuáles son los problemas pragmáticos que se han generado a raíz de su tipificación autónoma, ello dentro del marco de contextualización de la problemática de la criminalidad informática. Todo ello para concluir que su tipificación autónoma genera serios inconvenientes desde un punto de vista práctico, que llevan a rescatar la necesidad de creación de una causal de calificación que cobije tales hipótesis.

Ahora bien, con el fin de desatar integralmente el problema de investigación se hará uso del método analítico deductivo, descomponiendo los elementos criminológicos y dogmáticos del fenómeno en cuestión. Así, una vez determinados y explicados tales elementos, se concluirá que el hurto por medios informáticos no encaja dentro de los mismos, lo que hace necesaria la adopción de la solución que se esgrimirá al final del presente trabajo de grado.

CAPÍTULO I. APROXIMACIÓN A LOS DELITOS INFORMÁTICOS

Previo al análisis de la conducta de hurto por medios informáticos, y concretamente del estudio de la tipificación y las consideraciones al respecto, es necesario analizar de manera breve pero completa, el contexto y aproximación a los delitos informáticos.

De esta forma, es necesario precisar en primer lugar las diferencias conceptuales respecto de los conceptos de delito informático y cibercrimen. En la doctrina moderna se discute acerca de cuál de estos dos conceptos resulta más apropiado de cara a la explicación de la comisión de delitos relacionados con las tecnologías de la información y la comunicación (TIC), especialmente, cuando estos son cometidos en contra de sistemas informáticos o en contra de la información allí contenida.

Asimismo, y sin que se desborde el objeto de esta investigación, especial mención merecen los principales atentados en contra de los sistemas informáticos, telemáticos y de la información allí contenida, los cuales se abordan de manera general, para identificar allí, el objeto central de este trabajo, pero especialmente, para empezar bajo un concepto negativo, a identificar, que conductas no constituyen atentados informáticos.

De otro lado, el análisis criminológico de los delitos informáticos, adquiere especial relevancia, pues nos permite entender la problemática, desde la fenomenología de sus causas. Es así como la identificación de los riesgos, de las características de victimarios y víctimas, así como las bondades para el delincuente y dificultades en su persecución, nos facilitan la aproximación a la problemática que plantea este trabajo, sin dejar de lado la

referencia a las cifras que nos muestran con criterios estadísticos, la realidad y estado de la criminalidad en Colombia.

Finalmente, y como un preámbulo a la discusión, la identificación del bien jurídico, la delimitación de su objeto de protección, y la diferenciación de las conductas que en esencia pertenecen a él, establecen con precisión el contexto previo necesario para abordar la discusión que permitirá dar respuesta a la pregunta planteada.

1. Postura que adopta el concepto de Cibercrimen

En los años recientes, gran parte de la Doctrina ha adoptado el concepto de cibercrimen para referirse a la totalidad de conductas punibles que involucren, tanto en sus medios de comisión, como en sus resultados, la utilización de redes informáticas o telemáticasⁱ. Entonces, a modo de ejemplo, para los partidarios de esta postura será igualmente un cibercrimen el hurto de los dineros depositados en una entidad financiera, que se comete mediante el acceso a los sistemas informáticos bancarios, como aquellos atentados en contra de una página web perteneciente a una entidad estatal, o inclusive los delitos de pornografía infantil que se cometan mediante internet. Es decir, siempre que haya un elemento “cibernético”ⁱⁱ en la comisión de un delito, se estará hablando de un cibercrimen.

Lo importante entonces, para este concepto, no es el bien jurídico objeto de protección, sino única y específicamente, que el ilícito se realice mediante un elemento cibernético, lo que supone entonces, que cualquier conducta punible que sea susceptible de ser cometida por tal medio, estará llamada a ser considerada como un cibercrimen.

1.1. Fundamentos de la postura

Los ***fundamentos*** de quienes adoptan este conceptoⁱⁱⁱ pueden resumirse de esta forma:

1.1.1. El cibercrimen es un concepto más adecuado para definir las conductas cometidas mediante “internet”

Una primera justificación sobre la pertinencia del concepto de cibercrimen, consiste en que es más exacto de cara a la explicación de los delitos cometidos “a través” de internet o redes telemáticas semejantes. ¿Por qué? Porque con el surgimiento del internet se creó a su vez el ciberespacio. Y el concepto más adecuado terminológicamente para referirse a los delitos cometidos “en” o “a través” del ciberespacio es el de cibercrimen. Más no el de delito informático.

En otras palabras, el advenimiento del internet, y de las redes telemáticas en general, ha impuesto la necesidad de repensar el concepto de delito informático, pues parece referirse más a la “información” que al concepto nuevo que pretenden explicar: “el ciberespacio”. Así, como señala Romeo Casabona (2006), los partidarios de esta postura sostienen que las redes telemáticas –especialmente el internet- dan lugar a una variada e impensable gama de riesgos. De ahí que, el concepto clásico de delito informático se quede corto, lo que ha llevado a la gran mayoría de la doctrina foránea especializada a adoptar el término cibercrimen.

Lo anterior, debido a que, al fin y al cabo, si bien Internet, la Red más popular y a través de la cual se realizarán prácticamente todas estas infracciones, es en sí misma un medio informático y, por tanto, todos los ciberdelitos podrían entrar dentro de la categoría de los

delitos informáticos; con la utilización del término cibercriminalidad se pone de manifiesto que sus implicaciones de riesgo van más allá de la utilización de tecnologías informáticas y se relacionan mucho más con el hecho de que estos comportamientos están unidos en la actualidad a redes telemáticas, con los particulares problemas político-criminales que ello plantea (Miró, 2012)

Es entonces esa vinculación entre las nuevas formas de criminalidad y las redes telemáticas (internet, ciberespacio, etc) lo que fundamenta la adopción de este nuevo concepto.

1.1.2. El concepto de cibercrimen abarca mayor cantidad de conductas

Un segundo argumento que permite a este sector de la doctrina, liderado por el tratadista español Fernando Miró, afirmar la preferencia por el concepto de cibercrimen sobre el de delito informático, radica en que dentro del concepto de cibercrimen se puede abarcar una mayor cantidad de delitos que comparten un elemento en común: su comisión a través de redes telemáticas, es decir “a través del ciberespacio”. Esclarecedor resulta el siguiente ejemplo: “Así, el acoso sexual por Internet, el acoso a menores realizado en la Red o por medio de los *smartphones*, y la instigación al delito terrorista en el entorno virtual entre otros, parecen encajar mucho más con la idea de «lo cibernético» que con la de «lo informático»” (Miró, 2012, p. 39).

En esta misma línea argumentativa, Romeo Casabona (2006) señala:

Los perfiles de los delitos informáticos han de ser sometidos a las peculiaridades jurídicas que pueden ofrecer nuevos recursos técnicos o de uso más extendido,

como ha sucedido con las comunicaciones telemáticas abiertas, en particular con Internet. Como se indicó más arriba, estos medios permiten una ilimitada posibilidad de transferencia, flujo y comunicación de la información, así como el ofrecimiento de servicios de cualquier tipo, desde cualquier origen geográfico y hacia cualquier destino, prácticamente con una absoluta libertad de acceso y de puesta en circulación de cualquier información, así como de tratarla y manipularla.

De esta constelación de presupuestos fácticos surge la necesidad de distinguir una ulterior generación de delincuencia vinculada con las TIC y llevan a plantearse si expresiones nuevas o cuyo uso se está extendiendo podrían aglutinar todos los diversos aspectos que presenta la criminalidad vinculada con la combinación de los sistemas informáticos y telemáticos actuales. A este planteamiento responde, por ejemplo, la adopción y preferencia por el término «cibercrimen» (o «ciberdelito»), el cual se ha incorporado incluso a la legislación internacional. (p. 9)

Otro importante argumento se advierte, en punto de la preferencia de esta forma denominativa cuando se señala que:

Desde una perspectiva criminológica, nos interesa el cibercrimen como una categoría amplia (amplia porque abarca los atentados a través de redes telemáticas) en aras a la prevención del mismo, de modo que limitarnos a las conductas que están presentes en el Código Penal actual, resultaría contradictorio con estos objetivos. (Miró, 2012, p. 39). Paréntesis fuera de texto original.

1.1.3. El concepto de cibercrimen es un concepto complementario

Este argumento puede explicarse de la siguiente forma. En principio podría señalarse que los delitos informáticos son los delitos cometidos a través de los sistemas informáticos. Decimos en principio porque consideramos que esa es una concepción errada de los delitos informáticos^{iv}. Ahora bien, la informática es definida por la Real Academia de la Lengua española como “El conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático y racional de la información por medio de computadoras” (RAE, 2012). Resulta evidente que, en la definición de “informática” no se percata la presencia de ningún elemento relacionado con el internet ni con el ciberespacio. Sino simplemente con el tratamiento automatizado de la información.

Entonces, ¿qué incluye el concepto de cibercrimen que no abarca el de delitos informáticos? La comisión de delitos a través de redes telemáticas. Pues, al ser definida la telemática como la “aplicación de las técnicas de la telecomunicación y de la informática a la **transmisión a larga distancia de información computarizada**” (RAE, 2012) es claro que es un concepto que va más allá de la informática. Debido a que, consiste en **la transmisión** de esos datos automatizados, es decir, de los datos informáticos. En otros términos, la informática aglutina datos, los trata y almacena; mientras que la telemática se refiere a la transmisión de los mismos, en ambos casos mediante el uso de computadoras.

Esto les permite a los partidarios del concepto de cibercrimen señalar que, sólo acogiendo la acepción de cibercrimen puede abarcarse a los delitos cometidos a través de internet. Pues si se habla simplemente de delitos informáticos, se dejarían por fuera las conductas punibles cometidas en el ciberespacio (transmisión a larga distancia de información

computarizada). En cambio, al hablar de cibercrimen, se incluyen la comisión a través de redes telemáticas. Lo que convierte al cibercrimen en un concepto más amplio, que absorbe inclusive, al de delito informático.

1.2. Críticas a la postura

Al concepto de cibercrimen se le endilgan, fundamentalmente, tres críticas, a saber:

1.2.1. El concepto de cibercrimen no aglomera delitos que atenten contra un mismo bien jurídico, lo que imposibilita un estudio sistemático

La primera crítica consiste en que los delitos aglomerados dentro del concepto de cibercrimen no atentan en contra de un mismo bien jurídico, sino que por el contrario, se trata de toda una serie de conductas punibles que afectan bienes jurídicos diversos. Así, el hurto cometido por medios telemáticos, afecta el patrimonio económico; la distribución “online” de pornografía infantil^v, afecta la libertad, integridad y formación sexuales^{vi}; por su parte, la violación a través de internet de los derechos morales de autor, afecta los derechos de autor; y así podríamos seguir haciendo referencia a todos los delitos que tienen la potencialidad de ser cometidos a través de redes informáticas o telemáticas, y nos percataríamos de que siempre afectan bienes jurídicos completamente diferentes.

Ahora bien, la consecuencia de que no se aglomere en el concepto objeto de crítica un grupo de delitos que afecten un mismo bien jurídico, no es otra diferente a que se imposibilita el llevar a cabo un estudio sistemático y conjunto de los mismos. Dado que, cada tipo penal tiene características absolutamente particulares y necesariamente independientes. Lo único que compartirían los cibercrimenes es un elemento cibernético,

pero esto no es suficiente para afirmar que se puede llevar a cabo un estudio dogmático conjunto. Así lo resalta Romeo Casabona (2006), quien señala:

Desde un punto de vista técnico-jurídico tampoco parece, sin embargo, que el término cibercrimen pueda llegar a satisfacer plenamente una función dogmática de integración de estos delitos de nueva generación, sin perjuicio de que desde planteamientos criminológicos pueda ser adecuado para cumplir una función descriptiva o de identificación de un fenómeno criminal singular y el espacio — virtual— en el que se manifiesta, pues presenta unos perfiles diferentes respecto a lo que se venía entendiendo por delito o delitos informáticos y, desde luego, respecto a cualesquiera otros delitos. (p. 9)

1.2.2. El concepto de cibercrimen es excesivamente amplio

Una segunda crítica evidente, pero no por ello menos importante, que puede predicarse del concepto en mención, es que es absolutamente amplio y difuso. Puesto que abarca cualquier delito que pueda llegar a tener alguna relación, mediata o inmediata, con sistemas telemáticos. Esto quiere decir que, lo que para los partidarios de la postura es un punto a favor, para sus contradictores es una falencia insalvable. Esa excesiva amplitud del concepto genera que sus componentes, es decir, los delitos cometidos en el ciberespacio, no guarden ninguna armonía entre sí. Y por lo tanto, su agrupación no tenga ningún sentido.

1.2.3. El cibercrimen es un delito común cometido a través de medios cibernéticos

Desde nuestro punto de vista, consideramos que existe una crítica más que puede elevarse frente al concepto de cibercrimen. Así que, a modo de anticipo –pues la explicación cabal la daremos más adelante–, resulta necesario señalar que el cibercrimen no es más que un delito común (hurto, pornografía infantil, injuria, etc) cometido a través de un nuevo medio: el ciberespacio. Por lo que su agrupación sería exorbitantemente arbitraria. Sucedería lo mismo si deciden agruparse, por ejemplo, todos los delitos cometidos a través de automóviles, bajo la rúbrica de “delitos automovilísticos”.

2. Postura que adopta el concepto de delito informático en sentido amplio

La doctrina dominante aun acoge el concepto de delito informático. Sin embargo, desde ya, debemos distinguir el concepto limitado, y el concepto extensivo de delito informático.

Quienes adoptan el concepto de delito informático en **sentido extensivo**^{vii}, agrupan en una misma categoría, tanto las conductas delictivas clásicas cometidas a través de medios informáticos (por ejemplo hurto o daño en bien ajeno), como las cometidas en contra de los sistemas informáticos y de la información que esos sistemas contienen^{viii}. Para ellos, los tipos penales considerados como delitos informáticos no necesariamente revisten una naturaleza similar, ni tienen idénticos problemas dogmáticos, así como tampoco protegen bienes jurídicos en común. Simplemente, se trata de conductas punibles que tienen un elemento en común: su vinculación, así sea meramente remota, con un sistema informático^{ix}.

En este sentido, *Miró* (2012) afirma:

La categoría de los delitos informáticos, o quizá mejor, de la criminalidad o delincuencia informática, no definía un bien jurídico protegido común a todos ellos, sino más bien un ámbito de riesgo, el que derivaba de la expansión social de la tecnología informática, común a muchos bienes jurídicos cuya tutela completa por parte del legislador parecía requerir una modificación de los tipos penales existentes para su adaptación a las nuevas realidades informáticas o la creación de tipos distintos que respondiesen a las nuevas necesidades de protección. (p.35)

El concepto de delito informático, es desarrollado por Romeo Casabona (2006), de la siguiente forma:

—Aquéllas (conductas) que atentan de forma grave a determinados bienes de titularidad individual —de personas físicas, pero también de personas jurídicas—, que presentan una configuración específica y exclusiva de la actividad informática y telemática y han sido sometidos a una 'tipología' técnico-criminológica: acceso, alteración, ocultación o destrucción no autorizados o no consentidos de los datos almacenados en un sistema informático; reproducción completa o parcial de datos contenidos en un sistema informático, así como la distribución o comercialización de los mismos. Asimismo, solían incluirse otras conductas, como la sustracción del 'tiempo' o utilización ilegítima de equipos, sistemas, y redes informáticos o telemáticos, etc. (p. 5)

Una definición, similar, pero mucho más genérica, es la proporcionada por Bramont-Arias (s.f.), quien señala:

De manera general, se puede definir el delito informático como aquél en el que, para su comisión, se emplea un sistema automático de procesamiento de datos o de transmisión de datos.

2.1. Fundamento de la adopción de la acepción delito informático en sentido amplio

El principal *fundamento* de la adopción del concepto de delito informático en sentido amplio o extensivo, consiste en que en él se cobijan todas aquellas conductas delictivas que tienen un elemento en común: el uso de sistemas informáticos, sin importar cuál es el bien jurídico que resulte efectivamente lesionado^x. Así, podría afirmarse que al adoptar el concepto de delito informático, “...el patrimonio y el orden económico, bienes personalísimos como la intimidad o la libertad sexual, y otros bienes supraindividuales o difusos, se consideraban protegidos por «los delitos informáticos»” (Miró, 2012, p. 35).

No obstante las bondades que parece presentar el concepto de delito informático, entendido en forma extensiva, debido a que abarca múltiples bienes jurídicos, las *críticas* por sus diversas falencias vienen siendo las mismas que se pueden elevar respecto del concepto de cibercrimen. Motivo por el cual, estudiaremos esas críticas de forma brevísima.

2.2. Criticas al concepto de delito informático en sentido amplio

2.2.1. Excesiva vaguedad y amplitud del concepto

En primer lugar, la acepción de delito informático en sentido amplio es criticada por su *excesiva vaguedad y amplitud*. Lo que parecía ser una de sus bondades, terminó siendo, a la luz de la doctrina especializada, una de sus mayores falencias, puesto que, este concepto de delito informático es tan excesivamente amplio que el mismo no puede circunscribirse a un bien jurídico determinado, ni tampoco a una conducta punible específica. Y por ende, su alcance de protección tampoco va a poder ser delimitado de forma clara y efectiva^{xi}. Así lo pone de presente *Mata Y Martin* (2001) cuando afirma:

En ocasiones la referencia a los hechos delictivos relacionados con la informática se realiza mediante la expresión o denominación de «delito informático», expresión que posee cierto atractivo por su simplicidad y por responder a la terminología anglosajona *computer crime*. En realidad se trata de un concepto ambiguo que no se corresponde en sentido estricto con ninguna categoría jurídico-penal, con un exclusivo hecho punible de los previstos en el Código penal.

La polimórfica realidad de la criminalidad informática, se refleja y manifiesta en los intentos de definición o conceptualización de la misma, así como en las clasificaciones de los hechos a las que da lugar el estudio de este fenómeno. Así la aproximación a un concepto genérico, omnicomprensivo del hecho informático penalmente relevante da lugar necesariamente a definiciones muy amplias. (p. 21)

2.2.2. Imposibilidad de aproximación dogmática idéntica

De otro lado, el concepto en mención es sumamente criticado, debido a que resulta un despropósito que los tipos penales que conforman los delitos informáticos en sentido extenso, no tengan una aproximación dogmática idéntica, debido a que se trata de una simple agrupación de delitos con características medianamente similares. En este orden de ideas, el estudio dogmático de los tipos en mención, será idéntico al de los delitos tradicionales. Razón suficiente para afirmar que su agrupación en el concepto “delitos informáticos” deviene altamente inútil. En otras palabras:

La categoría de los delitos informáticos, como constructo doctrinal que se usó por la doctrina penal alemana y española durante los años setenta, ochenta, noventa y al principio de este nuevo siglo, y que sigue usándose por parte de la doctrina, no se concibió por quienes lo utilizaban en el sentido de grupo autónomo de infracciones penales con caracteres sistemáticos, o de contenido material de protección, homogéneos que exigirían una metodología distinta al resto de grupos o de una valoración político-criminal común, al tutelar intereses sociales de idéntica naturaleza. (Miró, 2012, p. 34).

2.2.3. Falta de fundamento para el estudio conjunto de delitos informáticos como concepto extensivo

En el mismo sentido de la crítica anterior, también se ha señalado por la doctrina que, la simple constatación empírica de que ciertos delitos se hayan cometido en relación con sistemas informáticos, no es motivo fundado para que esos tipos penales sean agrupados

como un fenómeno criminal independiente^{xii}. Frente al particular, Romeo Casabona (2006) afirma:

A la vista de las anteriores observaciones es cuestionable que, en sentido estricto, sea aceptable la denominación, en ocasiones generalizada, de «delito informático». La simple comprobación empírica de que estos nuevos 'delitos' (o hechos merecedores de una estudiada respuesta político-criminal) pueden ser cometidos en conexión con las TIC no es un argumento o razón suficiente para tratar, por lo menos en singular, de ellos como un fenómeno criminal autónomo («delito informático»). (p. 6)

A modo de conclusión, debe decirse que para los detractores del concepto amplio de delito informático “el desafortunado término "delito informático" es, a *nuestro entender*, ambicioso y artificial: ambicioso, porque es difícil delimitar con exactitud los contornos de lo "informático" frente al delito; y artificial, porque en estricto rigor jurídico el denominado *delito informático* no existe” (Balmaceda, 2009, p. 81).

3. Toma de postura: adopción del concepto de delito informático en sentido limitado

Teniendo en cuenta que, ninguno de los dos conceptos estudiados con antelación – cibercrimen y delito informático en sentido amplio- se encuentra exentos de críticas **absolutamente fundadas**, nos vemos en la necesidad de ir en contravía de la doctrina mayoritaria y acoger el concepto de delito informático en un sentido limitado.

Entonces, ***sólo es delito informático el ataque en contra de un sistema informático o telemático, o en contra de la información allí contenida***^{xiii}. Desde nuestro personal punto

de vista, el concepto de delito informático sólo abarca aquellos atentados cometidos, a través de redes informáticas o telemáticas, **en contra de los datos o de los sistemas informáticos**^{xiv}. Así pues, contrario a lo que pregonan una parte representativa de la doctrina, consideramos que no basta con que se utilice como medio un sistema informático o una red telemática en la comisión del delito, para que a dicha conducta se le pueda denominar delito informático. Se requiere pues la presencia de una de dos circunstancias. Por un lado, que haya un atentado en contra de la información o los datos contenidos en el sistema informático o telemático, o por otro lado, que se ataque directamente un sistema informático o telemático^{xv}.

Así las cosas, aquellos ataques contra el patrimonio económico en los que se utilicen medios informáticos, no encuadran dentro de nuestra concepción de delito informático^{xvi}. Tampoco serán delitos informáticos las injurias que se cometan a través de redes sociales. Ni mucho menos será delito informático el lavado de activos que se cometa mediante una tienda virtual. Pues, simplemente, se tratan estos actos de delitos comunes, cometidos a través de un medio novedoso: el sistema informático. Entonces, la concepción de delito informático que adoptamos, es una concepción limitada^{xvii}.

Fundamentos de la adopción del concepto de delito informático en sentido limitado

3.1. El objeto de protección es la “informática”. Esa es la razón para denominarlos delitos “informáticos”

Exclusivamente la adopción de un concepto limitado de delito informático como el propuesto con antelación, va a corresponder totalmente con el término “informática”.

Debido a que, si entendemos la informática como “el tratamiento automático y racional de la información (y los datos) por medio de computadoras” (RAE, 2012) resulta incontrovertible que el objeto de protección de los delitos informáticos son los sistemas de tratamiento automatizado de datos y los datos que allí se manipulan. De lo contrario, sería como afirmar que los delitos patrimoniales no protegen el patrimonio económico.

3.2. El delito informático en sentido limitado se encuentra compuesto por un conjunto de delitos que afectan un mismo bien jurídico

Si acogemos el concepto restringido de delitos informáticos, los delitos que se van a agrupar sí protegerían un mismo bien jurídico: la confidencialidad, integridad y disponibilidad de los sistemas informáticos y de los datos allí contenidos. Razón por la cual, este concepto sería inmune a la crítica ya estudiada elevada ante el concepto de cibercrimen, y frente al de delito informático en sentido amplio.

3.3. Posibilidad de estudio contiguo de los delitos informáticos entendidos en sentido restringido

Debido a que revisten características similares y afectan un mismo bien jurídico, los delitos informáticos entendidos en un sentido restringido, sí pueden ser estudiados desde la dogmática jurídico penal de forma conjunta. Motivo por el cual, su agrupación, a diferencia de lo que sucede con los cibercrimenes y los delitos informáticos entendidos en sentido amplio, no deviene inútil en lo absoluto.

3.4. Bien jurídico autónomo

Quizás el fundamento más importante, y de mayor relieve para efectos de este trabajo, es justamente el que señala que el reconocimiento del concepto de delito informático en sentido restringido es justamente el principal argumento para establecer un bien jurídico autónomo, que justifique un esfuerzo de protección penal, y que dé alcance al objeto a tutelar, cual es la protección de la confidencialidad, integridad y disponibilidad de los sistemas de información y los datos, es decir, siendo absolutamente coherentes, si admitimos la existencia de un bien jurídico objeto de protección, será un evidente contra sentido sostener el grado difuso, que por ejemplo abarca la cibercriminalidad.

Ya se ha dicho que la cibercriminalidad no hace referencia a un bien jurídico autónomo, sino a conductas desplegadas mediante medios informáticos o telemáticos, con independencia del bien jurídico que protegen. Pues bien, la limitación del concepto de delito informático debe circunscribirse a lo que el bien jurídico entraña en sí mismo.

Son estas las razones que fundamentan nuestra postura, y de antemano señalamos que a lo largo del presente texto, siempre que se utilice el término delito informático, el mismo corresponderá a su concepción en sentido restringido o limitado. Es decir, ***al ataque en contra de un sistema informático o telemático, así como el ataque en contra de la información allí contenida.***

4. Principales atentados en contra de sistemas informáticos, telemáticos y de la información allí contenida

Más allá de que algunas de las conductas que describiremos en los próximos párrafos ya hayan sido configuradas como delictivas en la legislación colombiana y otras no, a continuación explicaremos brevemente a modo de contexto, en qué consisten dichas conductas, y por qué pueden considerarse como atentatorias en contra de los sistemas informáticos y telemáticos, así como de la información contenida en esos sistemas.

Sin embargo, debido a que las diferentes modalidades de delitos informáticos avanzan conforme avanzan las TIC, sería un imposible el tratar de abordar todas las formas que existen para atacar los sistemas informáticos y telemáticos. Adicionalmente, un estudio de dicha naturaleza excedería el objeto del presente trabajo. Por tal razón, nos limitaremos a estudiar los dos principales atentados típicamente informáticos: el “hacking” o acceso no consentido a sistemas informáticos y el sabotaje informático.

4.1. “Hacking” o acceso no consentido a sistemas informáticos

El atentado más común en contra de los sistemas informáticos es el conocido “hacking”, o acceso no autorizado a sistemas informáticos. Conducta cometida por los denominados “hackers”, que consiste en la intromisión no consentida a un sistema informático violando los sistemas de seguridad existentes, sin que concurra en el autor ninguna intención adicional. Esto quiere decir que no se busca provocar un daño en el sistema informático, sino que simplemente se desea acceder a él^{xviii}.

Diferentes definiciones sobre este atentado informático pueden encontrarse en la doctrina foránea. A continuación, traemos a colación las definiciones de los más renombrados académicos alrededor del globo. Fernando Miró (Miró, 2012) define esta conducta de la siguiente forma:

(...)podríamos describir el hacking como cualquier conducta por la cual un sujeto accede a un sistema o equipo informático sin autorización del titular del mismo, de una forma tal que tiene capacidad potencial de utilizarlo o de acceder a cualquier tipo de información que esté en el sistema. (p.53)

Para los argentinos Gustavo Eduardo Aboso y Maria Florencia Zapata (Aboso, 2006) este atentado cibernético:

(....) consiste en el acceso no autorizado a un sistema de datos a través de un proceso de datos a distancia, cometido sin intención fraudulenta ni de sabotaje o espionaje. Esta conducta, denominada "Computerhacking", significa ingresar en el sistema informático de otro, sin el propósito de manipularlo, sabotearlo o espiarlo, sino de "pasear" o interiorizarse sobre las medidas técnicas de seguridad del sistema. Queda claro que esta acción se presenta, en muchos casos, como la puerta de ingreso para la comisión de otro tipo de delitos más graves. (p.50)

En Chile, Rodolfo Herrera Bravo y Alejandra Núñez Romero (Herrera y Nuñez, 1999) han señalado lo siguiente:

Es un delito informático que consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con

el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor.

En este delito es imprescindible que su motivación no sea el causar daño a través de otros ilícitos, como el sabotaje o el espionaje informático, o la piratería, las cuales son obras de los crackers más que de los hackers. Más bien persigue satisfacciones personales, basados (SIC) en la burla de los sistemas de seguridad dispuestos, es decir, en logros exitosos frente a los retos intelectuales que se autoimpone.

Se trata de un delito de resultado que se consuma al momento de ser descifrados los códigos de acceso secretos, y no dependiendo del conocimiento o ignorancia que pueda tener el sujeto pasivo sobre este hecho.

De todas las citas expuestas en antelación, puede inferirse que son dos los elementos distintivos del "hacking". Por un lado, el acceso ilegítimo a un sistema informático. Y por otro, la ausencia de un ánimo destructor o dañino en el "hacker". Es decir que, quien accede al sistema informático no desea obtener un beneficio económico, ni tampoco desea generar algún daño con su conducta. Sólo desea acceder al sistema. Nada más.

No obstante que, frente a la definición y aspectos esenciales del "hacking" no se presenta mayor discusión en la doctrina, frente a su punibilidad no sucede lo mismo. ¿Por qué?

Porque una parte de la doctrina considera que al no existir un ánimo destructivo en el “hacker” no existe fundamento para su represión desde el Derecho Penal^{xix}.

Tal y como lo habíamos señalado en el capítulo anterior, Morón Lerma (2002) ha sido enfática en señalar que el “hacking” no es una conducta que deba ser sancionada desde el punto de vista jurídico penal. Sino que, por el contrario, sólo adquiere relevancia penal, y por ende debe ser castigado como delito, cuando quien realiza la conducta busca un fin ilícito alternativo^{xx}. Como la obtención de un provecho económico, por ejemplo. Es decir, cuando dejar de ser “hacking”. Pues recordemos que, cuando concurre una finalidad destructiva en el acceso al sistema informático, ya no se habla de “hacking” sino de “cracking”^{xxi}.

En contra de esta postura, y afirmando la completa tipicidad del “hacking”, Herrera y Nuñez (1999) señalan:

Rechazamos las opiniones que surgen a favor de la atipicidad del hacking directo y que recurren al argumento de la no intencionalidad de causar daños al sistema en que se ingresa, ya que no es posible que un hacker desconozca que su conducta no le está permitida por el sujeto pasivo debido a la forma irregular en que ingresa. Además, los gastos en que incurren las empresas para adoptar mecanismos de seguridad de sus sistemas son cuantiosos, por lo que un hacker que intencionadamente rompe tales medidas, aunque sea como un simple juego, obligará a invertir en ello nuevamente. Y lo más importante, la intimidad se ve violada de un modo manifiesto al acceder sin derecho a los programas ajenos, sin que sea necesario para ello otra acción que el ingreso, así como en la violación de

correspondencia basta abrir la carta para cometer el delito, sin necesidad de que su contenido sea leído, alterado, destruido o difundido, por ejemplo. Claro que la penalidad del hacking directo debe ser baja en relación a los otros delitos informáticos. (p. 242)

Pues bien, la solución adoptada en Colombia mediante la ley 1276 de 2009, evidentemente se inscribió en esta última postura. Pues el acceso abusivo a sistema informático se castiga sin requerir para la tipicidad de la conducta un elemento subjetivo especial del tipo penal que requiera una finalidad concreta en el acceso. Así, el artículo 269A del Código Penal Colombiano, tipifica:

Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de (...).

Así las cosas, tenemos entonces decantada la discusión en punto del acceso a un sistema informático o telemático, y su tratamiento en la doctrina foránea, y la legislación interna.

4.2. Sabotaje informático

A diferencia del “hacking”, el sabotaje informático si lleva ligada una intención destructora. Consiste, en términos generales, en la propagación de virus^{xxii}, programas maliciosos o cualquier maniobra dañina^{xxiii}, en contra de sistemas informáticos ajenos con el fin de destruir archivos, de interceptar datos industriales o corporativos, o cualquier otra intención destructora^{xxiv}. Sin embargo, la utilización de virus no es el único medio

para la comisión del sabotaje informático, pues por ejemplo, un empleado de una entidad financiera podría utilizar el propio programa del banco para modificar, sustraer o destruir la información contenida en el sistema informático. Lo que sin duda constituiría un sabotaje^{xxv}.

Miro (2012) ha señalado acerca del sabotaje informático que: “Uno de los principales riesgos que, para particulares y, muy especialmente, para empresas, conlleva el acceso al ciberespacio por medio de sistemas informáticos, es el de sufrir lo que se ha venido denominando «sabotaje informático», incluyendo a su vez en él tanto los comportamientos, ya conocidos y asumidos como comunes en el entorno virtual, consistentes en el envío a través de redes telemáticas de virus informáticos que aprovechan la inmensidad de la Red para multiplicarse y acceder a miles de terminales, como cualesquiera otras formas de destrucción de archivos o datos de terminales concretos y determinados, con fines industriales o de daño individual” (p. 57).

Para Herrera y Nuñez (1999) el sabotaje informático puede definirse de la siguiente forma: “Definiremos al sabotaje informático como la acción típica, antijurídica y dolosa destinada a destruir o inutilizar el soporte lógico de un sistema computacional mediante el empleo natural de las tecnologías de la información” (p. 229).

En similar sentido Aboso (2006) cuando afirma:

El sabotaje informático (“Computersabotage”) se ha transformado en una de las actividades ilícitas más extendidas en el marco de la delincuencia informática. Esta modalidad consiste en dañar el funcionamiento del sistema informático, ya sea en

sus elementos físicos (hardware) o en la información intangible contenida en sus programas. Para ello acude al recurso del llamado "programa gusano" o "virus informático", que afecta el uso correcto del sistema o lo ralentiza. El principal peligro que se presenta con el uso de virus informáticos es la enorme capacidad de daño que tiene su uso en las redes telemáticas actuales.

La dependencia de la "comunidad informática" de los sistemas de telecomunicaciones y telemáticos demuestra, una vez más, que el sabotaje informático aparece como una actividad ilícita que debe ser tenida especialmente en cuenta. La pérdida de información almacenada y la afectación de los procesos de comunicación de datos constituyen el talón de Aquiles de nuestra moderna sociedad.

A modo de conclusión, constituye sabotaje informático cualquier conducta tendiente a destruir, sustraer o modificar información contenida en un sistema informático, así como aquellas tendiente a inutilizar, obstruir o entorpecer el funcionamiento de un sistema informático o telemático^{xxvi}. Es decir, los ataques, por un lado, en contra de los sistemas informáticos y telemáticos, y por otro lado, los ataques a la información contenida en dichos sistemas^{xxvii}.

Contrario a lo que sucede con el acceso abusivo a sistema informático, el sabotaje informático no fue objeto de tipificación expresa en el Código Penal colombiano mediante la reforma introducida por la ley 1276 de 2009. Sin embargo, sí existen cuatro conductas que podrían cobijar lo que la doctrina foránea conoce como sabotaje informático.

En primer lugar, la conducta típica contenida en el artículo 269B del Código Penal de Colombia, denominada “obstaculización ilegítima de sistema informático o red de telecomunicación” la cual castiga a “el que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena (...)”.

La segunda conducta punible que, en nuestra legislación, abarcaría el sabotaje informático, es la contenida en el artículo 269C, denominada “interceptación de datos informáticos”. Conducta que comete “el que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte (...)”.

Asimismo, se encuentra la conducta tipificada en el artículo 269D: “daño informático”. Esta conducta la comete “el que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos”.

Por último, se encuentra el “uso de software malicioso”, conducta tipificada en el artículo 269E. Este tipo penal castiga a quien “sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos”.

Se trata pues, de varios tipos penales que, en su sumatoria, abarcan la gran mayoría de conductas de sabotaje informático. Desde aquellas maniobras delictivas destinadas a

atacar los sistemas informáticos y telemáticos, hasta las actividades punibles que tienen como objetivo atacar la información contenida en esos sistemas.

Lo esbozado en los párrafos anteriores constituye un panorama en extremo breve de los atentados que pueden resultar vulneratorios de la confidencialidad, integridad y disponibilidad de los sistemas informáticos y telemáticos, así como de la información en ellos contenida. Ahora bien, antes de culminar con el presente capítulo, es necesario recordar, una vez más, que el “hacking” y las diferentes formas de sabotaje informático, son los verdaderos delitos informáticos.

Pues, como expondremos en la segunda parte de este trabajo, y como ya señalamos en el primer capítulo, el hurto informático y la transferencia no consentida de activos son delitos que no afectan el bien jurídico de la confidencialidad, integridad y disponibilidad de los sistemas informáticos y telemáticos, así como de la información en ellos contenida, sino que por el contrario, son delitos cometidos “por medios informáticos” que afectan el patrimonio económico. Y, por ende, su caracterización como delitos informáticos, resulta incorrecta. En otras palabras: no son más que delitos comunes cometidos a través de medios novedosos.

5. Aspectos criminológicos del delito informático

5.1. La aparición de nuevos riesgos como fundamento de la punición del delito informático

Siempre que el ingenio humano produce alguna nueva herramienta de utilidad para la sociedad, se produce un correlativo aumento de la incertidumbre por los riesgos que puedan generarse, así como una sensación generalizada de inseguridad. Tal fue el caso del surgimiento de las imprentas, el nacimiento de los automóviles, la creación de la aeronáutica y en general de todo aquello que genera innovación. Así lo ilustra *Mata Y Martin* (2003) cuando señala:

Hoy nos puede sorprender, pero podemos ver algunos ejemplos de estos sobresaltos a los que se ha visto sometida la sociedad. Con la aparición de la imprenta se produjo un inmenso beneficio para la difusión de la cultura pero al tiempo un cierto temor. Mientras se trataba exclusivamente de manuscritos, por su menor difusión, el problema era menor, aunque también existen precedentes de prohibiciones especialmente en algunos períodos del derecho romano (...) Otro ámbito en el que se generan temores y precauciones será el de los Automóviles. Con estos nuevos medios de transporte la sensación de inseguridad se reproduce. Así el Código Penal español de 1928 establece como agravante genérica aplicable, en principio, a cualquier delito) la realización del hecho punible o la huida mediante un vehículo a motor, lo que delata la preocupación del legislador por este nuevo medio técnico a disposición de los criminales. (p. 937)

Entonces, resulta innegable que la aparición de redes telemáticas como el internet ha revolucionado el mundo como se lo conocía. Las comunicaciones a través de internet han reemplazado los métodos clásicos de correo y mensajería; las transacciones comerciales “on line”, tanto con entidades financieras, como entre consumidores, han tomado el lugar de las antiguas transacciones realizadas en forma personal; las interacciones mediante redes sociales, han reemplazado, en gran medida, aquellas que se realizaban en forma presencial; las consultas académicas en plataformas virtuales, han desplazado las visitas a las bibliotecas; el almacenamiento digital de archivos ha sustituido a las enormes e inacabables bodegas en las que se resguardaban los documentos físicos de las empresas; las clases virtuales, han entrado a ocupar junto con las clases presenciales, un lugar que antes sólo era dominado por estas últimas. Estos son tan sólo algunos de los miles de ejemplos que podríamos traer a colación, acerca de los aportes que los sistemas informáticos y telemáticos le han hecho al mundo contemporáneo^{xxviii}.

Pues bien, así como es cierto que con el nacimiento de los sistemas informáticos y telemáticos surgieron innumerables herramientas de inocultable importancia, también es cierto que a raíz de su surgimiento, se incrementaron muchos riesgos ya existentes, al tiempo que se crearon otros que no existían. Y, precisamente, es la creación de nuevos riesgos, y el aumento de los riesgos ya existentes, el fundamento mismo de la punición independiente de aquellos delitos cometidos en contra de los sistemas informáticos y de la información contenida en esos sistemas^{xxix}.

Esta problemática ha sido descrita por Fernández (2007), en los siguientes términos:

El incesante desarrollo y expansión de Internet como vía de comunicación y transmisión masiva de datos le ha otorgado en los últimos años una extraordinaria trascendencia social, adquiriendo con ello un rol esencial para el desarrollo de todo tipo de actividades de carácter lúdico, cultural, financiero o comercial. Sin embargo, dicha expansión también ha determinado la inevitable entrada de un porcentaje de actividades nocivas para los ciudadanos, algunas de las cuales producen la lesión de bienes jurídicos relevantes.

Además, pese a que la mayoría de las conductas desarrolladas a través de internet no sean en esencia algo nuevo, la extraordinaria peculiaridad del medio dota a las mismas de una especial estructura que obliga a actualizar los tipos delictivos, los cuales -como apuntamos- han sido configurados sobre la base de una dinámica delictiva basada en relaciones más o menos directas e interpersonales. (p. 13)

5.2. Los riesgos generados con la aparición de las redes informáticas y telemáticas.

Manifestaciones concretas de la aparición del delito informático.

Como ya se mencionó, la aparición de los sistemas informáticos y telemáticos, ha estado acompañada del surgimiento de nuevos riesgos, los cuales, de forma correlativa, han conllevado a la aparición de los delitos informáticos^{xxx}. No obstante, debido a que la cantidad de riesgos generados haría que enlistarlos a todos sea un trabajo interminable –y en parte, altamente inútil-, en los párrafos siguientes señalaremos sólo las manifestaciones concretas más relevantes en las que esos riesgos podrían materializarse.

Pues bien, en contra de los sistemas informáticos y de la información allí contenida se pueden cometer una gran cantidad de conductas lesivas, sin embargo, para efectos del análisis criminológico que se realiza en este capítulo, basta con exponer de forma detallada las tres manifestaciones más relevantes de la aparición de esos riesgos.

5.2.1. El acceso abusivo a bases de datos y sistemas informáticos

En primer lugar, piénsese en el más evidente y renombrado de esos fenómenos: los accesos no consentidos a bases de datos o sistemas informáticos ajenos. Fenómeno conocido como “hacking”. Las actuaciones de los “hackers” son la más notoria manifestación de los riesgos surgidos a raíz de la aparición de la informática, y pueden tener como finalidad la producción de uno de dos tipos de acciones: las acciones destructivas o las acciones neutras, también conocidas como “intromisión blanca”.

Las acciones destructivas son conocidas con el anglicismo “cracking”^{xxxi} que bien podría traducir “rompimiento” o “destrucción”. Como su nombre lo indica, son acciones destinadas al cataclismo de las bases de datos o de los sistemas informáticos. Un ejemplo claro, sería el caso de un programador activista que decide irrumpir a las páginas web del gobierno con el fin de dejarlas inoperantes, sin más finalidad que la de interrumpir el normal funcionamiento de la página web estatal.

Por su parte, las acciones de “intromisión blanca” no buscan nada diferente al acceso a la información contenida en la base de datos. Serán acciones neutras siempre y cuando no se busque un propósito diferente al acceso a la información. Pues, si además de buscar por ejemplo, el acceso a la información, el “hacker” también desea utilizar esa

información para acceder a un sistema financiero (como sería el caso de las claves de acceso a sucursales virtuales de entidad financiera) su acción ya no sería de “intromisión blanca”, sino que encuadraría en el fenómeno denominado como el “cracking”.

Las bases de datos computarizadas, son hoy en día un activo de especial importancia, y muy apetecido por los sectores más destacados de la economía. Es así como por ejemplo las entidades financieras, las compañías que ofrecen productos y servicios, tienen como uno de sus activos más importantes la relación de datos sistematizados de sus usuarios. Tanto así que, se destinan importantes recursos económicos y humanos para mantener organizadas y actualizadas esas bases de datos.

Adicionalmente, la tecnología y especialmente las redes, han entrado a reemplazar actividades cotidianas, y mecanismos tradicionales de comunicación y almacenamiento de información; facilitando a la humanidad su tráfico y distribución, pero generando paralelamente un alto riesgo de concentración en espacios virtuales, que luce atractivo por lo que representa para delincuentes o expertos informáticos que deseen lucrarse con ello.

Así las cosas, desde las perspectivas criminológica y sociológica, el riesgo que presenta la organización de datos, y lo apetecido de su acceso, es lo que justifica y hace necesario instaurar una barrera de contención que permita su protección desde la esfera penal.

5.2.2. La interceptación de telecomunicaciones^{xxxii} a través del ciberespacio

La segunda manifestación puntual de los riesgos generados con la creación de los sistemas informáticos y telemáticos, es la posibilidad de interceptar comunicaciones de cualquier naturaleza. Como por ejemplo:

(...) las comunicaciones de carácter personal o de otra naturaleza (financiera, comercial, etc.), como pueden ser los mensajes de correo electrónico, conversaciones orales o escritas a tiempo real (teléfonos por cable, celulares o móviles, foros restringidos, *chat*), remisión o intercambio de documentos, etc.
(Romeo Casabona, 2006, p. 2)

Frente al particular, basta con resaltar que cualquier comunicación llevada a cabo mediante internet –la red telemática por excelencia-, es susceptible de ser interceptada por un tercero con inmedible facilidad. Incluso, resulta más sencillo y asequible (tanto en términos tecnológicos como económicos) la interceptación de comunicaciones realizadas a través de sistemas informáticos, que las comunicaciones telefónicas mismas^{xxxiii}. Pues, para el acceso a estas últimas, se requieren plataformas especializadas que suelen ser mucho más costosas que las requeridas para “hackear” un “chat” o un correo electrónico.

5.2.3. La reproducción y transmisión de contenido ilícito mediante sistemas informáticos y telemáticos

La propagación de la pornografía infantil a través de sistemas informáticos y telemáticos es la muestra perfecta de los nuevos riesgos generados con la aparición de la informática. Si bien es cierto, se trata de un fenómeno que de antaño ha producido preocupación al

Derecho Penal, también es cierto que la prevención y el control de ese problema nunca se había dificultado tanto, como se empezó a dificultar –casi imposibilitar- cuando surgieron las tecnologías de la información y la telecomunicación. Ubeda (2007) ha resumido este problema así:

Internet supone una vía privilegiada para la difusión de la pornografía infantil. Además, está provocando que los centros de producción de pornografía infantil se vayan desplazando hacia lugares donde expresamente no aparecen tipificadas estas conductas o donde se protege únicamente a personas de edad muy inferior a los 18 años. La falta de uniformidad legal, y de colaboración internacional, determina una especial dificultad en la persecución de aquellos que producen este material, y, por ello, convierten en ilusoria la defensa adecuada de los menores que son objeto de estas prácticas. La actuación de los Tribunales en nuestro entorno se limita, con contadas excepciones, a las conductas de difusión de material ya elaborado o de tenencia de pornografía (p. 1).

Este es un claro ejemplo de los riesgos que, pese a no haber sido *creados* con la aparición de los sistemas informáticos y redes telemáticas^{xxxiv}, sí se ha visto *incrementado* en enormes proporciones con el surgimiento de estas redes. Pues, fue con la informática que los delincuentes dedicados a la pornografía infantil encontraron el medio perfecto para la comisión impune –la mayoría de las veces- de sus conductas delictivas^{xxxv}. En apoyo a este argumento debe señalarse que:

Pese a la dificultad del cómputo, se estima que ya en el año 2005 existían más de cuatro millones de sitios en Internet con material de sexo con menores, los cuales

recibirían más de dos mil millones de visitas anuales. Este tipo de materiales están alojados principalmente en servidores de países de la antigua Unión Soviética y en algunos de América Latina, donde la legislación es mucho más permisiva, lo que plantea relevantes dificultades a las autoridades judiciales y policiales españolas en virtud de la vigencia de una serie de principios como el de territorialidad. Se estima que nuestro país alberga el 1% del total de sitios que contienen material de sexo con niños. Desde el punto de vista del consumo de estos materiales y también en base (SIC) al estudio de investigación que ANESVAD realizó durante el año 2002, España sería el segundo país del mundo (y el primero de Europa) que más pornografía infantil consume. (Fernández, 2007, p. 54)

5.3. Principales causas en las que radica la peligrosidad de los riesgos generados por el surgimiento de los sistemas informáticos y telemáticos

Habiendo señalado de forma somera y por demás genérica, cuales son los principales y más comentados riesgos generados con la aparición de la informática y la telemática, resulta forzoso determinar por qué esos riesgos son tan difíciles de controlar^{xxxvi}. Por la doctrina se han esbozado dos rasgos generales que generan la vocación incontrolable de los delitos informáticos: por un lado, la potencial anonimidad con la que se comete el delito, y por otro, la facilidad de encubrir los hechos y de borrar las pruebas incriminatorias. Circunstancias ambas que conducen a predicar la enorme dificultad de prevenir, investigar y sancionar los delitos informáticos.

5.3.1. Anonimidad en la comisión del delito

La primera circunstancia que hace que los riesgos creados por la informática sean especialmente peligrosos, es la *anonimidad* con la que se cometen los delitos informáticos. Anonimidad no en sentido estricto, sino en el sentido de que para establecer la identidad del delincuente informático debe pasarse por una multiplicidad de procedimientos engorrosos y en ocasiones cuantiosos, a tal punto que la vocación de prosperidad de esos procedimientos puede llegar a ser nula. Entonces, "... (el) problema lo constituye la de la individualización de la responsabilidad criminal en el ámbito de los hechos punibles cometidos en Internet. No resultará fácil la determinación de la responsabilidad de los plurales sujetos que aparecen en el contexto general de la red". Paréntesis fuera del texto original (Mata Y Martin, 2003, p. 938).

Piénsese que, tan sólo para verificar desde qué dirección IP se cometió un delito se requiere de un procedimiento tecnológico que no puede ser realizado por cualquier investigador. Pero esto no es todo, pues una vez se logre identificar la dirección IP, aún falta por recorrer la mitad del camino. En Colombia, por ejemplo, sería necesario solicitar una búsqueda selectiva en base de datos, con el fin de que las entidades prestadoras del servicio de internet proporcionen toda la información relacionada con esa dirección IP.

Pero aquí no se acaba el procedimiento, pues todavía subsiste el problema de individualizar a la persona que cometió el delito informático. Pues, por ejemplo, si un computador es usualmente utilizado por cinco personas integrantes de una familia, debe determinarse quién de esos individuos fue el que cometió la conducta punible. Y, además

de determinarse, debe probarse más allá de toda duda razonable esa responsabilidad penal individual.

En fin, este ejemplo se esboza sólo para mostrar lo difícil que puede llegar a ser la identificación e individualización de un delincuente informático^{xxxvii}. Si es difícil en el ejemplo básico que se ha planteado, necesario resulta concluir que será mucho más complejo –casi imposible– llevar a cabo dicha individualización en supuestos en los que el delito se comete por decenas de personas, utilizando decenas de computadores diferentes, ubicados en decenas de países diferentes, todo de forma simultánea.^{xxxviii}

Frente a este tópico, Mata y Martin (2001) señala:

Como se ha dicho estos procedimientos representan particulares dificultades en el descubrimiento de los hechos y su persecución. En el ámbito de la delincuencia informática se presentan sin duda importantes complicaciones para el descubrimiento y la investigación de los hechos en y mediante el ordenador, de forma que puede en ocasiones no ser raro que muchos de los casos no lleguen nunca a detectarse. Según datos del FBI sólo se llegan a descubrir un 1% de los casos, de estos únicamente el 14 se ponen en conocimiento de las autoridades y, finalmente, tan sólo un 3% de estos últimos acaba en una sentencia condenatoria, con lo que se evidencian los graves problemas que —desde muchas ópticas— se ciernen sobre la lucha contra este tipo de hechos. Las alteraciones de datos y programas y los accesos a sistemas informáticos no dejan huellas semejantes a la de la delincuencia tradicional, de forma que las «huellas electrónicas» introducen una gran novedad y complejidad. Existe la posibilidad de identificar quienes de

manera ilícita introducen y procesan datos mediante *loggins* y otros registros. (p. 27).

5.3.2. Facilidad de encubrir los hechos y borrar las pruebas

Al problema de la potencial anonimidad al momento de cometer el delito informático, se suma la facilidad que existe de *encubrir los hechos y borrar las pruebas* de la comisión del mismo^{xxxix}. En palabras de Davara (2005):

Esas mismas facilidades enunciadas en el apartado anterior, y su utilización en la comisión del delito, ofrecen unas condiciones óptimas para encubrir el hecho. Es posible modificar, por ejemplo, un programa, para que realice una actividad ilícita en beneficio del autor y establecer una rutina software que vuelva a modificar el programa, en forma automática, una vez realizado el hecho dejándole tal y como se encontraba al principio.

De esta forma, ni visualmente, ni con el análisis del programa, ni con el estudio del proceso, sería posible detectar lo que ha ocurrido y cómo se ha cometido el hecho. Solamente podríamos acudir al resultado para comprobar que la acción ha sido cometida. Pero como el resultado será la producción de un beneficio para su autor y un perjuicio para otro, es posible que no se pueda nunca comprobar que el hecho producido ha sido uno de los ilícitos que hemos considerado como delito informático (p. 368).

Facilidad también predicable de la erradicación de las pruebas de la conducta punible^{xl}.

Pues:

Existe una gran facilidad para borrar todas las pruebas que hace prácticamente imposible detectar la acción cometida. Esta facilidad proviene, a veces, de la pertenencia del delincuente a la plantilla profesional de la empresa en la que se encuentra el ordenador con el que se ha cometido el delito y ello facilita la actuación, con carácter incluso «profesional», en el borrado de las pruebas. (Davara, 2005, p. 369)

5.2. Perfil criminológico del delincuente informático^{xli}

Continuando con el análisis criminológico de la criminalidad informática, es necesario llevar a cabo un perfilamiento criminológico del sujeto activo que incurre en el delito informático. Esto es, el denominado delincuente informático. Antes de iniciar con el análisis propuesto, es importante aclarar que lo pretendido por este apartado consiste en esbozar los rasgos comunes que **suelen** compartir aquellos que se dedican a conductas punibles relacionadas con las TIC. Esto quiere decir que, bajo ninguna circunstancia el estudio que se realizará en los párrafos siguientes pretende abarcar la totalidad de características que posee un delincuente informático, pues un propósito de tal naturaleza resultaría ser un imposible, pero además desbordaría el objeto de este trabajo.

Bien, aclarado lo anterior, deseamos iniciar señalando que la definición que reina en el criterio doctrinal especializado^{xlii}, con algo más o algo menos, es aquella que señala al delincuente informático como un “joven intelectualmente superdotado y con unos problemas de adaptación social tales que le llevan a volcar todo su interés en el denominado universo cibernético, olvidándose casi por completo de lo que acontece en el mundo real” (Galán, 2006, p. 19).

Se trata pues, de una persona con un nivel cognoscitivo e intelectual tan elevado^{xliii}, que le permite descifrar códigos, contraseñas, medidas y esquemas de protección y, en general, todas aquellas barreras que le plantean los sistemas informáticos que desea acceder. Ese nivel cognoscitivo ha sido más fácilmente adquirido debido a su edad. Por ser el cibercriminal una persona joven, ha tenido acceso y contacto permanente a las tecnologías de la información y la comunicación, y ese acceso ininterrumpido le ha permitido permearse del conocimiento necesario para un cabal manejo de los sistemas informáticos y telemáticos^{xliv}.

Ahora bien, con el excesivo despliegue global que han tenido los sistemas informáticos, resulta evidente que ya no es necesario para ser un delincuente informático (hacker, cracker, etc) tener elevadísimos conocimientos de informática. Basta con que la persona cuente con mínimos conocimientos que le permitan acceder a manuales, guías o tutoriales de “hacking”. ¿Manuales de “hacking”? Sí. Inclusive, existen millares de páginas web dedicadas a explicar cómo acceder de forma abusiva a correos electrónicos, conversaciones de “whatsapp” ajenas, o a cualquier tipo de sistema informático.

Para constatar esta afirmación, es suficiente con digitar en un motor de búsqueda las palabras “cómo acceder a un correo electrónico ajeno”, “cómo “hackear” una página web” o “cómo acceder a un Facebook ajeno”^{xlv}, y en cuestión de milisegundos, se tendrá la información detallada, clara y completa, acerca de cómo llevar a cabo un atentado en contra de un sistema informático ajeno.

En este sentido, Palazzi (2000) ha señalado que:

Para algunos autores, el sujeto activo de estos delitos se encuentra conformado por un grupo de personas con una inteligencia y educación que superan el común, con vastos conocimientos informáticos (...) Pero es un mito que el delincuente informático deba forzosamente poseer conocimientos profundos en la materia. A nuestro juicio la computación se halla tan extendida hoy día, que cualquier persona que posea conocimientos mínimos de informática y tenga acceso a un ordenador, incluso desde su casa, puede realizar un delito informático. (p. 67)

Siguiendo la misma línea argumentativa, Miró (2012) aclara que gran parte de los “hackers” actuales no tienen conocimientos especializados en informática, sino que se aprovechan de aplicaciones y programas sencillos que hacen gran parte del trabajo criminal. Lo afirmado por el autor es lo siguiente:

En la actualidad, gran parte de los hackers-crackers ya no son expertos informáticos sino que también comienzan a realizar tales actividades, generalmente jóvenes, con conocimientos básicos de informática que aprovechan programas y aplicaciones sencillas para realizar sus incursiones. (p.236).

Ilustrativa para esta discusión resulta la siguiente tabla elaborada por Palazzi (2000), acerca de las características y posiciones que suele ocupar el delincuente informático según el delito que cometa:

Clase de delito	Sujetos
Delitos patrimoniales contra bancos y	Empleados, en especial cajeros o personal

entidades financieras.	del área de sistemas, ex empleados, terceros en connivencia ^{xlvi} .
Delitos de acceso ilegítimo o delito de daños menores.	Hackers, usuarios descontentos.
Daño o sabotaje informático.	Empleados de la empresa (<i>insiders</i>) ^{xlvi} , o espías profesionales o industriales ^{xlvi} .
Violaciones a la privacidad, tratamiento ilícito de datos personales.	Investigadores privados, Empresas de marketing. Agencias de informes crediticios y de solvencia patrimonial.
Violaciones a la propiedad intelectual del software y bancos de datos, con informes o compilaciones de datos.	Piratas informáticos, o también usuarios ("la copia amigable"), empresas que realizan competencia "parasitaria".

A modo de conclusión, puede afirmarse que en la actualidad los conocimientos profundos en informática no son una característica imprescindible en el delincuente informático^{xl}, puesto que, dicho nivel cognoscitivo ha sido paulatinamente desplazado por el uso de programas informáticos que hacen gran parte del "hacking"^l. No obstante lo anterior, frente a sistemas informáticos que cuentan con elaboradísimas barreras de seguridad, como los de las instituciones financieras a modo de ejemplo, resulta evidente que para

lograr superar dichas estructuras, se requieren conocimientos profundos que difícilmente pueden ser reemplazados por un sistema automatizado de datos dedicado al “hacking”^{li}.

5.3. Perfil criminológico de la víctima informática

La compilación de las características de la víctima informática en un solo perfil criminológico resulta ser una tarea casi imposible de llevar a cabo, y altamente inútil frente a los resultados que puede generar. La razón de esta contundente afirmación es simple: cualquier persona que tenga aunque sea un mínimo acceso a un sistema informático o telemático, tiene la potencialidad de ser víctima de un delito informático. Cualquier persona que tenga un correo electrónico, puede ser víctima de un acceso no consentido en ese correo electrónico. Cualquier persona que tenga un “Smartphone” puede ser víctima de una interceptación mediante maniobras de “hacking”. En definitiva, cualquier persona que tenga acceso, aunque sea temporal, a un procesador de datos (computador, Smartphone, tableta, etc) puede ser objeto de ataques provenientes de los delincuentes informáticos.

En este mismo sentido, Miró (2012) señala:

Cualquier usuario de Internet, cualquier persona que tenga un sistema informático conectado a una red o que a través de los sistemas existentes en colegios, bibliotecas, universidades, instituciones públicas, ciber-cafés, hoteles y demás, puede ser víctima de cibercrímenes de muy distinto tipo, dependiendo de la motivación del sujeto que realiza el ataque pero, también, del tipo de actividad que el propio usuario realice. De nuevo, por tanto, escapa a lo posible la

configuración de un perfil único de víctima potencial del cibercrimen, puesto que por lo menos habrá tantos perfiles como ámbitos de oportunidad criminal en el ciberespacio, pero entendiendo el ámbito de oportunidad como también definido por el actuar de la víctima. Esto significa, como ya se vio, que no es únicamente la motivación criminal la que define el ámbito de oportunidad criminal en el ciberespacio, sino que la propia víctima con su conducta también construye los ámbitos de riesgo.

Mención especial al respecto, merecen las personas jurídicas, pues para un sector de la Doctrina, en la gran mayoría de los casos, son ellas las víctimas de los delitos informáticos. Así lo afirma Alastuey (1994):

Como puede deducirse de las páginas anteriores y como demuestra la experiencia extranjera y los pocos casos que se han dado a conocer en España, las víctimas del ilícito informático son, casi sin excepción, personas jurídicas. Parece ser que, por regla general, se trata de bancos o compañías de seguros o empresas del sector pero, como advierte ROMEO, también las empresas públicas son víctimas de estos ilícitos y pone como ejemplo de estos últimos casos las diversas actividades de los servicios postales o de la Seguridad Social.

En definitiva, cualquier persona natural o jurídica puede ser una víctima informática, siempre y cuando tenga acceso, cuando menos temporal, a un sistema informático o telemático^{lii}.

5.4. Algunas cifras relativas a los delitos informáticos

Hay un aspecto relativo al análisis criminológico de los delitos informáticos que no puede dejarse de lado, cual es justamente el relativo a las cifras, tanto de delitos informáticos propiamente dichos, como de delitos comunes cometidos a través de medios informáticos. Frente al particular, es pertinente resaltar dos cifras específicas que permiten dimensionar la importancia y trascendencia de este tipo de criminalidad en el mundo moderno: i) por un lado, la cifra relativa a la cantidad de delitos informáticos y de delitos comunes cometidos a través de medios informáticos; y ii) el costo, en términos puramente económicos, que estos delitos han generado a sus víctimas.

Quizás el análisis más juicioso y detallado que se ha realizado sobre las “cifras” de la criminalidad informática, fue el realizado por la compañía Symantec, propietaria del antivirus Norton. En este informe, conocido también como el “Reporte Norton” (en adelante Norton, 2013) se muestra que, para el año en mención, se cometieron aproximadamente 378 millones de atentados informáticos –o económicos a través de medios informáticos- a nivel mundial. Lo que significa, en términos aproximados, que cada día hay más de un millón de víctimas informáticas a lo largo y ancho del globo.

Pero esto no es todo, pues en el mismo reporte Norton (2013), se muestra cómo en Colombia, el 64% de los habitantes han sido víctimas de cualquier forma de criminalidad relacionada directa o indirectamente con la informática. Es decir que, casi dos terceras partes de la población nacional, se han visto afectadas por este tipo de conductas delictivas. Lo que demuestra la importancia de enfrentar esta forma de criminalidad, y

adicionalmente, lleva a concluir de forma anticipada que es absolutamente imperiosa la necesidad de intervención penal efectiva en estos ámbitos.

El costo económico que le han representado este tipo de actuaciones punibles a las víctimas, según el reporte en comento, asciende a ciento trece (\$113) millones de dólares anuales a nivel mundial. Específicamente en Colombia, ese perjuicio asciende a aproximadamente cuatrocientos mil dólares (\$400.000). Ahora bien, es necesario aclarar que, esa cifra en la realidad, muy seguramente es sustancialmente mayor, pues, la señalada en el reporte Norton (2013) hace referencia únicamente a los casos que fueron objeto de estadística. Pero lo cierto es que la “cifra negra” de la criminalidad informática, puede ser cientos de veces mayor.

6. ¿Es necesaria la existencia de delitos típicamente informáticos?

Este aparte busca dar respuesta a un interrogante que ha puesto en pugna a los más representativos sectores de la Doctrina dedicada al tema de la delincuencia informática. La esencia de la discusión consiste en determinar si ¿bastan los delitos clásicos para dar respuesta a las nuevas formas de criminalidad? O ¿si es necesaria la implementación de nuevos tipos penales (delitos informáticos) para hacer frente a la criminalidad informática?

En otros términos:

En este momento de aplicación de las normas ya existentes a los nuevos sucesos surgen problemas al tratarse de una legislación que pese a las muchas reformas fundamentalmente está situada en el contexto histórico y tecnológico del siglo XIX.

Es decir, durante el primer periodo de aparición de estos hechos, se plantea el problema de si los nuevos hechos pueden castigarse con los viejos delitos. (Mata Y Martin, 2003, p. 939)

Entonces, es absolutamente necesario determinar, desde ya, si resulta pertinente la adopción de delitos típicamente informáticos, o si para la protección de esos mismos bienes jurídicos basta con los “viejos delitos”.

Sin embargo, aquí subyace un problema: si la discusión es abordada de forma general, esto es, frente a todos los fenómenos delictivos que lleven consigo un elemento informático (estafa y estafa informática, hurto y hurto por medios informáticos, distribución de pornografía infantil y distribución por medios cibernéticos, etc) las conclusiones a las que se arriben serán igualmente generales, abstractas y de utilidad mayormente teórica.

Asimismo, si se estudiara la necesidad de tipificación autónoma de cada tipo penal como informático, la conclusión a la que se arribaría podría ser diferente para cada tipo penal. Por ejemplo, la conclusión frente a si es necesario o no un tipo de estafa informática, podría no ser la misma a la que se adopte al interrogarse sobre si resulta conveniente un tipo independiente de hurto informático, así como la conclusión podría ser diferente si lo que se estudia es la necesidad de un tipo autónomo de distribución de pornografía infantil por medios informáticos.

Pues bien, previendo este tipo de impases, el presente capítulo abordará brevemente la discusión en términos generales, por lo que el desarrollo específico será abordado en la

segunda parte de este proyecto^{liii}, donde se evaluará exclusivamente la necesidad o ausencia de ella, respecto de la existencia el tipo penal de hurto por medios informáticos. En otras palabras, en este apartado se determinará si es necesaria la existencia de delitos autónomos (típicamente informáticos), cuyo objeto de protección jurídica sean los sistemas informáticos y la información allí contenida. A modo de anticipo, ha de señalarse que dicha necesidad es innegable.

6.1. Justificación de la existencia de los delitos típicamente informáticos. Necesaria referencia a la creación de un nuevo bien jurídico.

La necesidad de la existencia de los delitos informáticos está inescindiblemente ligada a la existencia de un bien jurídico nuevo que demanda protección por parte del Derecho Penal. Es decir que, si concluimos que existe un nuevo bien jurídico merecedor de tutela penal, automáticamente debemos concluir que sí es necesaria la existencia de delitos informáticos (entendidos en sentido limitado o restringido). Por el contrario, si la conclusión a la que arribamos nos señala que los bienes jurídicos que se encuentran en riesgo con el nacimiento de las redes informáticas y telemáticas son los clásicos, que ya se encuentran tutelados por el Derecho Represor (patrimonio, indemnidad sexual, etc.), entonces sería acertado pensar que no es pertinente la existencia de delitos típicamente informáticos, sino que basta con los “viejos delitos” para proteger esos intereses (hurto, estafa, etc.).

Así las cosas, a continuación se estudiarán los argumentos de aquellos que niegan la necesidad de tipificación autónoma de los delitos informáticos.

6.1.1. Postura que niega la existencia de un nuevo bien jurídico

Un sector, minoritario valga decir, de la doctrina^{liv} afirma que no existe un nuevo bien jurídico objeto de protección penal, sino que por el contrario, lo que debe protegerse son los bienes jurídicos tradicionales de las nuevas formas de comisión delictiva mediante sistemas informáticos y telemáticos. Así, para los suscriptores de esta postura las conductas de accesos abusivos a sistemas informáticos sólo deberían ser conductas punibles en los eventos en que, además del mero acceso al sistema informático o a la información allí contenida, se busque perjudicar otro bien jurídico, como el patrimonio por ejemplo.

Ilustradoras de la posición de quienes niegan la existencia de un nuevo bien jurídico, y la correlativa falta de sanción autónoma, resultan las palabras de Rueda Martin (2009) cuando señala que algunos autores “sí exigen la necesidad de añadir un fin ilícito a estas conductas de hacking para que intervenga el Derecho penal, de modo que estas conductas de simple acceso no deberían encontrar una respuesta jurídica en el ámbito del Derecho penal sino en el ámbito del Derecho administrativo sancionador, como, por ejemplo, en la Ley Orgánica 15/1999^{lv}, de Protección de Datos Personales”^{lvi} (p. 174).

Los argumentos en los que descansa esta postura, pueden resumirse de la siguiente forma:

i) Afirma Moron Lerma (2002) que:

(...)el debate en torno a la conveniencia político-criminal de la represión autónoma de estos comportamientos no puede desvincularse del estudio de los principios

informadores en los que descansa el sistema penal. En este punto, resultan especialmente afectados el principio de intervención mínima y el de «ultima ratio». Las garantías inherentes a un Derecho Penal mínimo deslegitiman la huida a éste, sin el recurso previo a otros instrumentos jurídicos no penales. (p. 76)

Así, la institución de un nuevo bien jurídico de esta naturaleza, constituiría, bajo la óptica de la autora citada, un adelantamiento injustificado de las barreras punitivas, que conllevaría a una violación de los principios de intervención mínima y última ratio.

ii) Asimismo, la autora en cita, afirma que:

(...) si uno de los motivos para tipificar las conductas de mero intrusismo reside en su configuración como conductas antesala de otros ilícitos más graves, una adecuada respuesta penal a esos otros ilícitos de mayor gravedad conduce a que estas formas más peligrosas, en que pueden derivar las conductas de hacking, hallen un reproche jurídico-penal menos conflictivo. Así, el acceso no consentido a un sistema informático, verificado con ánimo de vulnerar la privacidad ajena obtiene sanción penal en sede de atentados contra la intimidad informática o «habeas data». (p. 76)

En otras palabras, lo afirmado por Morón Lerma consiste en que, si un acceso a un sistema informático puede conllevar a una vulneración de otro bien jurídico, lo que se debe proteger es ese bien jurídico violentado. Más no, el mero acceso no autorizado al sistema informático. Es decir que, esas conductas deben encontrar respuesta en las instituciones clásicas del derecho penal.

Aunque estos argumentos serán debatidos en el apartado de “toma de postura”, vale la pena anticipar que los consideramos erróneos, puesto que, los sistemas informáticos, y la información allí contenida, “mueven” a la sociedad actual. Es decir, que se han convertido en valores esenciales. Y como valores indispensables de la organización social contemporánea, deben ser objeto de tutela penal, sin que pueda llegar a entenderse que su protección constituye una violación a los principios de intervención mínima y “ultima ratio”.

6.1.2. Postura que afirma la existencia de un nuevo bien jurídico

Pues bien, la gran mayoría de la doctrina^{lvii} es enfática al reconocer el surgimiento de un nuevo bien jurídico ligado al nacimiento de los sistemas informáticos y telemáticos^{lviii}. ¿La razón? Con el nacimiento de los sistemas automatizados de datos e información se creó un nuevo interés susceptible de tutela penal autónoma. Frente al particular, Aboso (2006) afirma:

De esta manera, existen dos senderos posibles para recorrer: el primero está constituido por la indagación sobre la existencia o no de un nuevo interés social que demanda una urgente protección jurídica, particularmente la ofrecida por el derecho penal; el segundo, diametralmente opuesto al primero, correr el velo de esta supuesta necesidad normativa de regular el uso abusivo de los elementos y datos informáticos y revelar, así, que lo que subyace, es en el fondo, una nueva forma de arista carente de tutela jurídica de bienes jurídicos ya conocidos por todos.

Como se desarrollará en el presente trabajo, consideramos que la primera opción es la correcta; es decir, el avance tecnológico que representa Internet y los problemas presentados por el uso generalizado de los sistemas informáticos disparan necesidades propias para el derecho penal, que ahora tiene ante sí un nuevo interés social digno de protección: la información y su transmisión a través de los sistemas telemáticos (p. 16).

En Chile, Herrera y Nuñez (1999), han afirmado con vehemencia que es necesaria la existencia de un nuevo bien jurídico, y han relatado cómo, en su país, dicha necesidad ya se materializó con la creación de nuevos intereses susceptibles de tutela penal mediante la ley 19.923^{lix}:

Cuando la ley recoge la necesidad social de proteger un bien determinado, éste pasa a denominarse bien jurídico, y recibe de parte del Derecho la atención requerida para ser salvaguardado y conservado íntegramente. La protección que el legislador le otorga la realiza a través de la prohibición de ciertas conductas que atentan contra el bien jurídico y la adecuación, encausamiento y regulación de otras, tendientes a conservarlo y fortalecerlo.

En relación a los delitos informáticos, en un principio se intentó adecuar tales conductas ilícitas a los tipos penales clásicos existentes en las distintas legislaciones. Sin embargo, esta experiencia demostró que no es posible hacerlo en la mayoría de los casos, si se pretende la completa asimilación a las figuras tradicionales, causando la atipicidad del delito informático. Esto motivó la creación

de figuras delictivas clásicas "informatizadas", y en ciertos casos en la creación de delitos nuevos, generando una diversidad de bienes jurídicos protegidos (p. 219).

En similar sentido, Sieber (2009) señala:

La ciberdelincuencia no sólo acarrea nuevas amenazas. Tal como se mostró antes, también conduce a nuevos escenarios para los delitos y nuevos problemas en las áreas del Derecho y la persecución penal. Estos problemas no sólo se causan por las dificultades prácticas para tratar los delitos informáticos. Más importante es el hecho de que las características especiales de los delitos informáticos están en completa oposición con las características fundamentales del Derecho tradicional (p. 166).

Resulta evidente que, si las características esenciales del delito informático están en evidente oposición a las del Derecho tradicional, solo mediante la constitución de un nuevo bien jurídico susceptible de protección penal, dichas oposiciones podrán ser solventadas. Adicionalmente, no existen tipos penales, ni tampoco bienes jurídicos, que hagan frente a la delincuencia típicamente informática, pues el sofisma de distracción, es utilizar el concepto de cibercrimen o delito informático en sentido amplio, para bajo ese velo, incluir, sin éxito ni fundamento, a los delitos típicamente informáticos.

6.1.3. Toma de postura

Consideramos entonces, que constituye un verdadero yerro afirmar que con el surgimiento de los sistemas informáticos y telemáticos no nació un nuevo interés susceptible de tutela penal. A continuación, expondremos las tres razones que nos

permiten afirmar que sí debe dársele una protección autónoma a los sistemas informáticos y telemáticos, y a la información en ellos contenida, mediante la intervención del aparato represor, es decir la tutela penal.

6.1.3.1. Dependencia de la organización social en los sistemas y redes informáticos

La sociedad como la conocemos, no puede concebirse sin la existencia de los sistemas informáticos. Como hemos referido con antelación, la gran mayoría de las actividades que antes eran desplegadas por el hombre en forma presencial, ahora se llevan a cabo a través de las redes informáticas y telemáticas. Así, muchos de los sectores de la economía serían actualmente inviables sin la existencia de los sistemas de almacenamiento y transmisión de datos.

Piénsese en cuán grande sería el debacle de las instituciones financieras si no pudieran utilizar las redes informáticas y telemáticas (internet) para la realización de sus operaciones bancarias. Lo mismo sucede con el sector bursátil. Sería, simple y llanamente, el final de la economía como la conocemos. Incluso, la misma afirmación podría predicarse del sistema de salud: ¿Qué pasaría si una institución prestadora del servicio de salud no pudiera verificar, mediante las bases de datos correspondientes, a qué entidad promotora de salud se encuentra afiliado el paciente?^{lx}o ¿Qué sucedería si se modifica la información de la historia clínica de un paciente que se encuentra contenida en un fichero informático?^{lxi}

Todo lo anterior para significar que, las redes telemáticas e informáticas van más allá de ser un mero medio de entretenimiento. Van más allá de ser el principal método de comunicación interpersonal, para constituir por el contrario una herramienta indispensable para el funcionamiento adecuado de la sociedad actual. En otros términos:

(...)nuestra organización social (la Administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte, las empresas, los particulares, etc.) ha pasado a depender de forma extraordinaria de la utilización de unos sistemas y redes informáticos, como medio de crecimiento económico y desarrollo social. (Rueda Martin, 2009, p. 190)

En ese orden de ideas, si los sistemas informáticos y telemáticos, así como la información allí contenida, son elementos esenciales para la sociedad contemporánea, mal haríamos en no proteger mediante el derecho represor esos elementos indispensables –sistemas informáticos-, dándoles el carácter de bienes jurídico-penalmente relevantes. Ya que, de no brindárseles dicho *status*, se dejaría tambaleante a todos aquellos sectores que necesitan de las redes telemáticas e informáticas para su correcto funcionamiento. Los cuales, en la actualidad, valga decir, son casi todos los sectores^{lxii}.

A similar conclusión arriba Rueda Martin (2009) cuando señala que “cabe destacar la importancia de proteger penalmente y no sólo administrativamente la función social que desempeña el bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos” (p.190).

Así las cosas, un valor como la información, es de especial importancia para la sociedad, lo que exige su elevación a rango de bien jurídico digno de tutelar, más aún cuando es la información un baluartepreciado de la sociedad, en las condiciones y concepciones contemporáneas actuales.

6.1.3.2. La Insuficiencia de las figuras delictivas clásicas para la protección de las bases de datos

La segunda razón que nos permite afirmar la existencia de un bien jurídico independiente objeto de tutela penal, consiste en la necesidad de proteger jurídico-penalmente la información contenida en las bases de datos^{lxiii}. Es conocido por todos que, una consecuencia práctica del surgimiento de los sistemas informáticos, fue la creación de las bases de datos, entendidas como aquellas herramientas que permiten llevar a cabo el tratamiento de datos personales^{lxiv}.

Así las cosas, resulta claro que de la creación de las bases de datos, surge un problema para el Derecho Penal: ¿cómo proteger la información contenida en ellas? Si tomamos como ejemplo la legislación Colombiana, hasta antes de la aprobación de la ley 1276 de 2009^{lxv}, la solución se torna en extremo complicada^{lxvi}.

No podríamos proteger la información contenida en las bases de datos, por ejemplo, mediante *el tipo penal de hurto*, por cuanto no podría hablarse de “apoderamiento” si el bien mueble continua en poder de su titular, cuál sería el caso de las bases de datos, ya que lo que obtiene quien accede a la información allí contenida, podría ser una copia de la

información. Entonces, no se estaría privando al titular de la información de la posibilidad de utilizar y acceder a ella.

A esto podemos sumar dos problemas para la configuración del hurto. Por un lado, la dificultad de encuadrar a la información como un “bien mueble”, teniendo en cuenta que conforme a la legislación colombiana, se trata de un bien intangible^{lxvii}. Y si es intangible ¿cómo puede ser objeto de un apoderamiento? Por otro lado, existe el problema de la vulneración al bien jurídico. Si la información y los datos contenidos en la base de datos no son susceptibles de valoración económica, no podría darse una vulneración al bien jurídico. Por lo que la configuración del tipo penal sería inviable^{lxviii}.

Tampoco podría darse la protección de la información contenida en la base de datos mediante los delitos que protegen los derechos de autor, puesto que para la configuración de dichos tipos penales se requiere un elemento “inventivo” en el objeto de protección^{lxix}. Y si bien es cierto, las bases de datos como tal, requieren de un proceso de “creación”, también es cierto que dicho elemento no puede predicarse de la información allí contenida, y es precisamente la información contenida en las bases de datos lo que se pretende proteger^{lxx}. Así que, testarudo resulta concluir que se puede proteger esa información mediante los tipos penales que protegen los derechos de autor.

Entonces, como la protección de la información contenida en las bases de datos no se puede dar mediante ninguna otra figura delictiva, ni mediante el derecho administrativo existente, resulta incontestable que dicha salvaguardia se debe dar mediante el delito informático. Y el delito informático, como figura autónoma, sólo puede existir si concurre a su vez un bien jurídico objeto de tutela. En este caso: la confidencialidad, integridad y

disponibilidad de los sistemas informáticos y telemáticos, así como la información allí contenida.

6.1.3.3. Protección temprana de otros bienes jurídicos

Por último, consideramos relevante la protección autónoma desde el campo penal de los sistemas informáticos y telemáticos, y de la información allí contenida, pues el amparo de este bien jurídico, significaría a su vez la salvaguardia temprana y anticipada de otros bienes jurídicos, tales como la intimidad, la integridad sexual, el patrimonio económico, entre otros. Con el fin de brindar claridad frente a este argumento, piénsese en el siguiente ejemplo.

Si un grupo de “crackers” desea obtener información almacenada en una base de datos de una entidad financiera, para después apropiarse de los recursos allí contenidos, la penalización del acceso a la base de datos, constituiría una protección temprana del patrimonio económico de los titulares de los dineros depositados en la entidad financiera, frente al ataque que llevarían a cabo los delincuentes después de haber logrado acceder a la información.

Dicha protección temprana o anticipada ha sido denominada por la doctrina especializada como “barreras de contención”^{lxxi}. Contención, porque evitan que el riesgo se propague a bienes jurídicos distintos. En este sentido, se ha señalado por parte de la doctrina más autorizada que “el bien jurídico aludido y que se refiere a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos constituye una barrera de contención de riesgos para otros bienes jurídicos que se puedan encontrar involucrados en la función

social que desempeñen tales sistemas y redes informáticos: la intimidad personal y familiar, el patrimonio, etc.” (Rueda Martin, 2009, p. 182).

Las razones expuestas con antelación, son las que nos llevan a afirmar con vehemencia que los sistemas informáticos y telemáticos, así como la información y los datos allí contenidos, deben ser objeto de tutela penal autónoma sin importar que no se llegue a violentar algún otro bien jurídico. Toda vez que, estos sistemas han cobrado tanta importancia para la sociedad en las últimas décadas, que su desprotección desde el punto de vista penal, sería un completo despropósito. Deseo dejar en el aire una reflexión: si el Derecho Penal no está para proteger aquellos bienes indispensables para el funcionamiento de la sociedad ¿entonces para qué está?

6.2. Si existe un nuevo bien jurídico, entonces, ¿cuál es?, y ¿en qué consiste ese bien jurídico?

Cuestión de gran importancia resulta la determinación de cuál es^{lxxii} y en qué consiste el bien jurídico protegido por los delitos informáticos^{lxxiii}. Si bien es cierto que, en Colombia mediante la ley 1273 de 2009, se nominó como bien jurídico protegido “de la protección de la información y los datos”, esa nominación resulta inexacta y no permite entender de forma cabal qué es lo que se pretende proteger^{lxxiv}.

En cambio, consideramos que una acepción más acertada del interés jurídico susceptible de tutela penal, es la confidencialidad, integridad, y disponibilidad de los sistemas informáticos y los datos^{lxxv}. Ese, desde nuestro punto de vista, debe ser el bien jurídico protegido^{lxxvi} mediante la tipificación de los delitos informáticos^{lxxvii}. Pero de nada valdría

realizar esa nominación, sin explicar en qué consiste el bien jurídico, por lo que procedemos a hacerlo, de conformidad con la posición esbozada por la profesora María Ángeles Rueda Martín (2009).

Por *integridad* de la información y los datos, debe entenderse la posibilidad que debe tener el titular del sistema informático o telemático, de utilizar la información allí contenida sin que la misma sufra ninguna modificación por parte de un tercero no autorizado. Esta faceta del bien jurídico se vería vulnerada en los eventos en que el “hacker” ingresa al sistema informático y borra, modifica, traslada o esconde la información allí contenida. Inclusive, se atentaría en contra de la integridad de la información y los datos, con la simple intrusión al sistema informático, pues el mero acceso deja rastros de “información” que no estaban antes^{lxxviii}. Lo que quiere decir que, estrictamente hablando, la información contenida después del acceso no autorizado, no va a coincidir con la existente antes del mismo.

Por su parte, *la confidencialidad* hace referencia a la potestad que tiene el titular del sistema informático, de decidir quiénes van a tener acceso al mismo, y a la información allí contenida. Es decir, esa libertad de elección sobre el acceso al sistema informático o telemático. En ese orden de ideas, la confidencialidad de la información y los datos se vería violentada, simple y llanamente, cuando una persona que no está autorizada para acceder al sistema, lo hace.

En cambio, frente la *disponibilidad* de la información y los datos, se protege el control que tiene la persona frente al sistema informático o telemático. Es esa capacidad de acabar,

vender, permutar, y en definitiva decidir cómo usar el sistema y la información allí contenida, lo que en últimas protege la disponibilidad.

En palabras de la doctrina^{lxxix}, esta triple dimensión del bien jurídico puede resumirse en los siguientes términos:

Esta seguridad en la utilización de los sistemas informáticos de forma más o menos generalizada se manifiesta en la confidencialidad, integridad y la disponibilidad de los sistemas de comunicación e información, y que constituye propiamente el bien jurídico a proteger en la tipificación de conductas de acceso ilícito a sistemas informáticos. La integridad de un sistema informático alude a su utilización con las pertinentes modificaciones del contenido de la información almacenada en el sistema por parte de la/s persona/s autorizada/s. La confidencialidad de dicho sistema se basa en que su utilización corresponde exclusivamente a la/s persona/s autorizada/s. La disponibilidad hace referencia al control sobre la utilización de un determinado sistema por parte de la/s persona/s autorizada/s. De esta manera cuando un hacker penetra ilícitamente en un sistema informático ajeno, tanto si se han infringido medidas de carácter técnico como si no ha sido así, se encuentra en un espacio, el propio sistema, en el que su integridad se ha visto afectada porque la sola entrada y el consiguiente uso del sistema da lugar a modificaciones en los datos del mismo, junto con las alteraciones de tales datos para intentar borrar los rastros que pudieran identificarles. Asimismo la confidencialidad del sistema se ve afectada si se utiliza por parte de una persona que no está autorizada. Finalmente la disponibilidad del sistema se afecta cuando penetra una persona no autorizada.

Se puede constatar que en estos supuestos de accesos ilícitos a un sistema informático se vulnera el bien jurídico expuesto con independencia de las ulteriores finalidades que haya perseguido el hacker con tales entradas (Rueda Martin, 2009, p. 187).

En el mismo sentido, en Colombia se ha señalado^{lxxx}, respecto de la protección del bien jurídico afectado por el delito de acceso abusivo a sistema informático –es decir, el delito informático por excelencia-, lo siguiente:

Este tipo penal pluriofensivo exige, en primer lugar, la afectación o vulneración del bien jurídico intermedio, público u autónomo de la seguridad de la información y los datos informáticos, con lo cual se sanciona la lesión de la confiabilidad, integridad y la libre disponibilidad directa de los sistemas informáticos y el peligro indirecto de los datos y la información almacenada en ellos (Posada, 2013, p. 109).

Así las cosas, una vez sentados conceptualmente los criterios dogmáticos y criminológicos en punto de la aproximación a los delitos informáticos, desde una perspectiva de contextualización y categorización, resulta de especial importancia, efectuar una referencia al tratamiento de esta modalidad delictiva en otros ordenamientos jurídicos, con el propósito de enriquecer el planteamiento central del presente trabajo, y de dotarlo, de un marco de referencia que nos permita nutrir con criterios de derecho comparado, las conclusiones y propuesta que al final habrá de presentarse.

CAPÍTULO II. EL DELITO INFORMÁTICO EN OTROS ORDENAMIENTOS JURÍDICOS

La punición del delito informático se ha tornado en un fenómeno global, a partir del cual, la mayoría de las legislaciones del mundo han optado por darle respuesta a las conductas atentatorias de los sistemas informáticos y de la información allí contenida. A continuación, estudiaremos aquellas legislaciones en las que se ha tipificado el delito informático de forma exhaustiva y autónoma. Como es apenas lógico, el estudio de todas las legislaciones en las que se haya consagrado, de una u otra forma el delito informático, sería una tarea que excedería los objetivos del presente texto. Razón por la cual, nos limitaremos a las legislaciones más relevantes y que mayores aportes le han hecho al tema que aquí se aborda, estas son: las legislaciones española, italiana, chilena y por supuesto, se hará referencia exhaustiva al importantísimo Convenio de Budapest sobre la Ciberdelincuencia.

1. CONVENIO DE BUDAPEST SOBRE CIBERCRIMINALIDAD^{lxxxii}

En el marco del Consejo de Europa, en el 2001 se gestó el Convenio de Budapest. Tratado que constituía el más importante esfuerzo internacional para combatir la criminalidad informática (denominada en forma genérica en el tratado como “cibercriminalidad”)^{lxxxii}. El Convenio de Budapest es el principal instrumento internacional referido a la comisión de delitos a través, y en contra de sistemas informáticos y telemáticos. En él, y en su protocolo adicional, se establecen múltiples obligaciones para los estados firmantes, como por ejemplo, la obligación de prevenir la propaganda racista a través de internet. Sin embargo, muchas de esas previsiones y obligaciones consagradas en el Convenio escapan

al objeto del presente texto, por lo que sólo se hará referencia a aquellas preceptivas que imponen la obligación a los Estados firmantes de tipificar los delitos informáticos.

Antes de entrar a estudiar el tratado, y corriendo el riesgo de tornarnos repetitivos, el cual aceptamos gustosos si en cambio somos claros, debemos señalar que sólo nos referiremos a las previsiones del tratado sobre delitos informáticos **entendidos en sentido restringido o limitado**. Es decir, aquellos atentados en contra de los sistemas informáticos y de la información que esos sistemas contienen. De esa forma, se dejarán de lado todas aquellas obligaciones para los Estados firmantes consagradas en el tratado que implican la tipificación de otro tipo de conductas punibles cometidas **a través** de medios informáticos (más no en contra de sistemas informáticos y la información allí contenida).

Aclarado lo anterior, debe mencionarse que en el capítulo II del convenio, relativo a las “medidas que deberán adoptarse a nivel nacional”, fue consagrado el título 1, llamado “Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos”. Allí se contempla la obligación para los Estados firmantes de tipificar como conductas delictivas las siguientes: i) el acceso ilícito; ii) la interceptación ilícita; iii) los ataques a la integridad de los datos; y iv) ataques a la integridad de los sistemas.

1.1. Acceso ilícito

La primera obligación impuesta a los Estados firmantes consiste en castigar el acceso deliberado e ilegítimo a un sistema informático. En todo o en parte. Y vulnerando las medidas de seguridad existentes o no. Es decir, se establece la obligación de volver el “hacking” un delito. A lo anterior debe añadirse que, según la previsión contenida en el

Convenio, la conducta ha de tipificarse sin importar cuál sea la finalidad que busque el delincuente. Por esta razón, se utiliza la fórmula “con la intención de obtener datos u otra intención delictiva”.

Lo señalado de forma expresa en el Convenio de Budapest es lo siguiente:

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que está conectado a otro sistema informático.

Valga recordar, de cara a la posible adhesión de Colombia al Convenio, que esta conducta fue tipificada en el artículo 269A de nuestro Código Penal colombiano. Significa esto que, por lo menos frente a esta primera obligación de tipificar el acceso ilícito, Colombia ya la cumple.

1.2. Interceptación ilícita

La segunda obligación que se deriva para los Estados parte del Convenio de Budapest, en lo referente a delitos informáticos, consiste en sancionar la interceptación de datos o informaciones que se transfieren mediante sistemas informáticos. Asimismo, el Convenio deja al arbitrio de las partes, la posibilidad de exigir o no una intención delictiva adicional para la tipificación del delito. Es decir, un elemento subjetivo especial del tipo penal.

Como podría ser, el revelar o acceder a información “secreta”, o también la búsqueda de un provecho económico injustificado.

Así, (...)cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Disposición que en nuestro concepto cumple con estos requisitos, es la tipificada en la legislación colombiana mediante el artículo 269C del Código Penal, denominada “interceptación de datos informáticos”. Conducta que comete “el que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte (...)”.

1.3. Ataques a la integridad de los datos

La integridad de los datos no fue tema olvidado en la Convención de Budapest del 2001 sobre la Cibercriminalidad. Así, en el artículo 4 del capítulo sobre delitos informáticos se señaló que era obligación de los Estados parte tipificar las conductas tendientes a dañar, borrar, deteriorar, alterar o suprimir datos informáticos. Por supuesto, cuando se hace

referencia a “datos informáticos” se está hablando acerca de aquellos datos e informaciones contenidas en un sistema informático. El artículo 4 señala:

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves.

Podría afirmarse que Colombia, aun cuando todavía no se encuentra obligada por no haberse adherido al tratado, ya cumple con esta obligación. Debido a que el artículo 269D del Código Penal sanciona el “daño informático”. Este delito lo comete “el que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos”.

1.4. Ataques a la integridad del sistema

La última conducta que deben sancionar los Estados que hagan parte del Convenio de Budapest es aquella que atenta contra la integridad, ya no de la información, sino de los sistemas en los que esa información es contenida. Además de la protección de la integridad de los sistemas informáticos, también se ordena en el artículo 5 del Convenio que se sancione la obstaculización al normal funcionamiento de los sistemas. Es decir que, deben tipificarse tanto el “daño” en contra de los sistemas como la “obstaculización” al normal funcionamiento.

El Convenio señala que:

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

De igual manera, así como en Colombia se cumple con las previsiones del Convenio estudiadas en los apartados anteriores, también se cumple con la obligación en comento. Es así como el artículo 269B contempla como conducta delictiva la “obstaculización ilegítima de sistema informático o red de telecomunicación” la cual castiga a “el que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena (...)”.

1.5. Conclusión parcial

A modo de conclusión, podemos afirmar sin lugar a equívocos que, en lo relativo estrictamente a delitos informáticos, Colombia cumple con todas las previsiones del Convenio de Budapest sobre la Cibercriminalidad. Y, en ese orden de ideas, nada obsta para que nuestro país se adhiera a ese tratado. Permitiéndonos, de esa forma, acceder a todos los mecanismos y herramientas con las que allí se cuenta en materia de lucha contra la delincuencia informática. Así, sin duda alguna, la adhesión al Convenio de Budapest significaría un enorme paso para el desarrollo de la materia en nuestro país.

2. ESPAÑA

Lo primero que debe señalarse acerca de la legislación española es que, a diferencia de otras legislaciones, no contempla un capítulo de delitos en contra de la información y los datos, o en contra de sistemas informáticos. Es decir, no existe un capítulo de delitos informáticos. Sin embargo, consiente de la necesidad de proteger los datos, la información y los sistemas en los que esos datos se albergan, el Rey de España dictó la ley orgánica 5 de 2010, por la cual se introducen modificaciones al Código Penal. En el numeral X del preámbulo de dicha ley se estableció que:

En el marco de los denominados delitos informáticos, para cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos. El primero, relativo a los daños, donde quedarían incluidas las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno. El segundo apartado se refiere al descubrimiento y revelación de secretos, donde estaría comprendido el acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o en parte del mismo.

Así las cosas, es necesario estudiar tangencialmente las cuatro conductas introducidas mediante la señalada ley. Estas son: i) el descubrimiento y revelación de secretos; ii) el

acceso a datos y sistemas informáticos; iii) el daño de sistema informático; y iv) la obstaculización al acceso de un sistema informático.

2.1. El descubrimiento de secreto recogido en archivo o registro. Artículo 197 apartado 2 Código Penal español

La primera de ellas, es la denominada como descubrimiento de secreto. Figura típica que sanciona “al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar o de otro, **que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos**, o en cualquier otro tipo de archivo o registro público o privado. Igualess penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero”.

Se trata pues de un delito típicamente informático. Dado que, lo que pretende proteger es la información contenida en soportes informáticos, electrónicos o telemáticos. Sin embargo, como anticipábamos, en España no se ha contemplado la existencia de un bien jurídico autónomo compuesto por los sistemas informáticos, telemáticos y la información allí contenida. Es por esta razón que, el bien jurídico que se encuentra protegido por el delito bajo estudio, es el de la intimidad, a diferencia de lo que ocurre, por ejemplo, en la legislación colombiana.

Frente al tema, Muñoz Conde (2013) señala:

La regulación penal de esta materia se inserta en un contexto más amplio en el que no sólo se brinda protección a los hechos que se consideran secretos, sino, de un

modo más general, al derecho a la intimidad, que se configura así, además de como un derecho constitucional (art. 18,1 CE), como un bien jurídico merecedor y necesitado de protección penal (p. 255).

Al referirse a la estructura típica del delito de descubrimiento de secreto recogido en archivo o registro, el autor en cita ha señalado que:

La característica principal de este precepto es que el objeto sobre el que recaen las distintas acciones en él tipificadas, «datos reservados de carácter personal o familiar de otro», se encuentran «registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado». La particularidad que el mismo encierra es que los datos referidos a la intimidad estén registrados de forma ordenada, normalmente a través de un mecanismo informático. De ahí que las conductas tipificadas no sólo se limiten a las consistentes en apoderamiento, utilización o modificación de los datos, sino que incluyen también el acceso a los mismos, como, por ejemplo, abriendo el ordenador o el móvil. (p. 261).

Recalcando la importancia del objeto de protección de este tipo penal, a tal punto que lo equipara a un derecho fundamental, Alvarez (1996) afirma:

El derecho a la privacidad (privacy) de los datos personales se ha convertido en un derecho fundamental de la persona, cuya defensa y protección frente a los poderes públicos se encomiendan a instituciones especializadas. Hoy en día, un sector importante de nuestra doctrina -véanse al respecto los trabajos del Profesor

PÉREZ LUÑO-, habla, a mi juicio con acierto, **del «habeas data» o derecho fundamental a la privacidad y a libertad en el conocimiento de nuestros datos personales por los poderes públicos** (p. 201).

De lo anterior se puede inferir con claridad que, en España, ni los sistemas informáticos ni la información que estos tienen, son propiamente un bien jurídico susceptible de protección penal. Por ejemplo, con el delito en comento, lo que se protege es el “Habeas Data”.

Sin embargo, hay quienes como Anarte, E, (2001), que consideran que más allá de la denominación que se le da al bien jurídico, lo cierto es que el objeto de protección del tipo penal no es, en términos exactos, la intimidad. Así lo señala el referido autor:

Partiendo de las rúbricas parece claro que el bien jurídico protegido en el artículo 197, número 2, sería la intimidad. Se trata, no obstante, de un concepto de extraordinaria amplitud y ambigüedad.

De todos modos la doctrina penal suele estar de acuerdo en que el derecho a la intimidad, entendido como garantía de un ámbito reservado, frente a injerencias de terceros, si bien ilustra mínimamente sobre el contenido tradicional, es, por lo menos, insuficiente para definir el bien jurídico protegido del número 2 del artículo 197. **Así resultaría claramente de los objetos sobre los que recaen las acciones típicas, que en principio constituyen la clave aglutinadora de los elementos en él aludidos: datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de fichero o registro público o privado** (p. 227).

No obstante la posición que tiene Anarte, E (2001), resulta claro que la legislación española no ha consagrado expresamente, como si lo hicieron por ejemplo la colombiana o la chilena, a los sistemas informáticos o la información allí contenida como un bien jurídico independiente objeto de protección penal. Por lo que los tipos penales que ataquen estos elementos se verán recogidos dentro de los capítulos relativos a otros bienes jurídicos, como la intimidad o el patrimonio económico.

2.2. Acceso a datos y sistemas informáticos. Artículo 197bis del Código Penal español

La conducta típica se encuentra descrita de la siguiente forma:

El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Se trata de la clásica conducta de “hacking”. Esto es, acceder de forma abusiva y no consentida a un sistema informático o telemático ajeno. Vale la pena aclarar que, en similar forma a lo que sucede en Colombia, esta conducta se tipifica con el mero acceso abusivo al sistema informático. Es decir que, no se requiere que se produzca un ulterior daño.

No obstante lo anterior, la redacción española difiere levemente de la colombiana, en cuanto que la legislación colombiana contempla como conducta delictiva el acceder a un sistema informático de forma no consentida, aun cuando el sistema no presente ninguna

medida de seguridad. Recordemos que la fórmula típica utilizada en Colombia consiste en “acceder en todo o en parte a un sistema informático protegido o no con una medida de seguridad”.

Caso contrario a la figura tipificada en España, pues no se ha vislumbrado la posibilidad de comisión del “hacking” sobre aquellos sistemas informáticos que no tienen ninguna barrera de seguridad.

Un ejemplo de “hacking” podría ser la conducta que se lleva a cabo mediante el llamado “caballo de troya”. Al respecto, Camacho (1987) expone:

Su nombre proviene de la hazaña narrada por Homero en *La Ilíada*, en la cual, durante el asedio a la ciudad de Troya, Ulises hizo construir un gran caballo de madera con el vientre hueco, ocultando allí un gran número de soldados, para a continuación regalárselo a los troyanos y simular el abandono del sitio de la ciudad. (...).

Después de esta digresión mitológica cuya única finalidad era explicar el porqué de este nombre, podemos precisar que este método consiste en introducir dentro de un programa de uso habitual una rutina o conjunto de instrucciones, por supuesto no autorizadas, para que dicho programa actúe en ciertos casos de una forma distinta a como estaba previsto.

Puede tratarse de que en determinadas circunstancias ejecute un cálculo de forma errónea, por ejemplo aumentando el importe de la nómina de un empleado, desviando partidas hacia cuentas ficticias, etc. (p. 38).

Ahora bien, es importante mencionar que con la reforma al Código Penal español realizada mediante ley orgánica 1/2015 del 30 de marzo de dicho año, se introdujo el numeral 2 al artículo 197bis objeto de estudio. Dicho numeral castiga a quien “mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos”.

Tipificación con la que se busca castigar aquellas interceptaciones que no atacan “comunicaciones” en términos estrictos, puesto que no se llevan a cabo entre personas. Con este nuevo artículo se busca castigar entonces aquellas interceptaciones a transmisiones realizadas automáticamente entre sistemas informáticos. Repetimos, incluso si en dichas transmisiones no interactúan seres humanos.

Para mayor claridad, veamos lo señalado en el numeral XIII de la reforma al Código Penal respecto del punto en cuestión:

Con el mismo planteamiento, y de acuerdo con las exigencias de la Directiva, se incluye la tipificación de la interceptación de transmisiones entre sistemas, cuando no se trata de transmisiones personales: la interceptación de comunicaciones personales ya estaba tipificada en el Código Penal; ahora se trata de tipificar las transmisiones automáticas –no personales– entre equipos.

Antes de continuar, se hace necesario recordar, una vez más, que, en España el bien jurídico protegido por los dos delitos mencionados con antelación, es el de la intimidad.

Por lo que resulta dable inferir que no se ha “creado” un nuevo bien jurídico susceptible de protección penal relativo exclusivamente a la informática.

2.3. Sabotaje Informático. Artículo 264 Código Penal español.

La Ley Orgánica 5 de 2010, tipificó el delito de daño en sistema informático, conducta a la cual nos hemos referido en párrafos pasados como sabotaje informático. La redacción legal del tipo penal es la siguiente:

El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave.

Se trata de una figurada cualificada del clásico delito de daño, o, conforme a la legislación colombiana, daño en bien ajeno. Conducta cuyo bien jurídico objeto de protección es el patrimonio económico. Así, “este delito comprende una serie de conductas que tienen en común que a través de diversos procedimientos impiden la posibilidad de uso de los datos, programas informáticos o documentos electrónicos. En este caso en el concepto de daño sí se incluye la afectación de la posibilidad de uso del objeto material sobre el que recae la acción, ya que aquí, a diferencia de lo que sucede con otros objetos materiales, el imposibilitar el uso del objeto material equivale al daño del mismo” (Muñoz Conde, 2013, p. 448).

Frente a este tipo penal subyace un problema consistente en que, el delito de daño en sistema informático, se encuentra ubicado dentro de los delitos en contra del patrimonio

económico. Esto quiere decir que para su consumación, la figura típica requiere que se dé una afectación al patrimonio económico del titular del sistema informático o telemático. ¿Por qué resulta problemática la ubicación dada al tipo penal? Porque pueden llegar a existir sistemas informáticos o documentos digitales que no sean susceptibles de valoración económica. Piénsese, a modo de ejemplo trivial, en aquellos sistemas que están tan mal diseñados, que nunca nadie pagaría un centavo por ellos. O en un documento digital cuya información sea completamente irrelevante y avalorada.

No obstante el inexistente valor económico de los sistemas o documentos, lo cierto es que la información allí contenida puede representar una importancia innegable para su titular. Pero, conforme a la legislación española, el daño sobre dichos sistemas o documentos carentes de valoración económica, sería impune; pues, el bien jurídico protegido por el delito es el patrimonio económico. Y si no hay afectación al patrimonio económico, no podrá afirmarse una antijuridicidad material en la conducta.

Situación diametralmente distinta es la acaecida en Colombia. Ya que, nuestra legislación contempla como bien jurídico protegido por el delito de “sabotaje informático” la información y los datos. Más no el patrimonio económico. Por lo que no adolecemos del problema que se presenta en la legislación española.

Ahora bien, con la reforma realizada al Código Penal español mediante la ley orgánica 1 del 30 de marzo de 2015, se introdujeron varias circunstancias de agravación punitiva para el tipo penal objeto de estudio. La primera de ellas, cuando el delito se cometa en el marco de una organización criminal. La segunda, cuando los daños hayan sido de especial gravedad o cuando se hayan afectado varios sistemas informáticos. Adicionalmente, es

una circunstancia de agravación el haber perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad. Por último, se agrava la pena cuando los hechos hayan afectado gravemente el sistema informático de una infraestructura crítica, es decir, cuando se afecte un sistema o parte del mismo que sea esencial para el mantenimiento de las funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico.

Antes de pasar a estudiar el siguiente tipo penal, hay que señalar que, el delito de sabotaje informático podría enmarcarse dentro de aquellas conductas delictivas que producen un perjuicio económico indirecto, pues la destrucción o alteración de un sistema informático podría acarrear un posterior perjuicio patrimonial. Camacho (1987) desarrolla con suficiencia este concepto:

1. *Perjuicio económico directo*. Es probablemente el caso más fácilmente identificable y uno de los pocos que pueden ser perseguidos y castigados de acuerdo con la legislación tradicional, ya que existe una apropiación de bienes, sea en la forma de dinero, mercancías, servicios o cualquier otro tipo de activo. El problema en este caso no es tanto descubrir el delito como poder probarlo.
2. *Perjuicio económico indirecto*. **Este es el caso en que no se produce una apropiación de bienes o servicios tangibles y valorables.** Ejemplo típico es la sustracción de información confidencial de carácter económico, comercial, etc., que daña los intereses de la organización, a veces a medio o largo plazo, y de una forma difícilmente cuantificable. ¿Cómo valorar una paulatina pérdida de cuota de

mercado porque nuestros competidores se adelantan a nuestras estrategias comerciales por conocerlas con anticipación? (p. 29)

2.4. Interrupción de funcionamiento de sistema informático. Artículo 264 bis del Código Penal español.

El Artículo 264, apartado 2 del Código Penal español señala: “el que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo o transmitiendo datos; o dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave”.

Este delito castiga a aquellos “hackers” o “crackers” que obstaculizan el normal funcionamiento de un sistema informático. Un ejemplo claro es el de aquellos activistas políticos que deciden “bloquear” el funcionamiento de las páginas web gubernamentales. Sin embargo, para la estructuración del delito se requiere que se dé alguna modificación en los datos contenidos en el sistema informático objeto de obstaculización.

El problema con este tipo penal es el mismo que se presenta con el de daño en sistema informático: el bien jurídico protegido es el patrimonio económico. Y por lo tanto, para la punición de la conducta se requiere que se produzca una afectación patrimonial en el titular del sistema informático. Situación que en muchas ocasiones no se presenta debido a la complicada “valoración económica” de un sistema informático o de la información que el mismo contiene.

Al igual que con el delito estudiado en el numeral anterior, la reforma al Código Penal español del 30 de marzo de 2015, acarreó la inclusión de varias circunstancias de agravación punitivas. Dichas circunstancias de agravación son las mismas que se refirieron frente al tipo penal de sabotaje informático, las cuales fueron objeto de mención al final del apartado anterior.

3. ITALIA

En la legislación italiana, la protección penal de los datos y los sistemas informáticos se da mediante cuatro figuras típicas. Dos de ellas enfocadas a la protección de los datos y sistemas informáticos privados, y otras dos encaminadas a la salvaguarda de los datos y sistemas informáticos públicos.

3.1. Daño a informaciones, datos y sistemas informáticos ajenos. Artículo 635-bis Código Penal italiano.

Esta primera conducta protege los datos privados contenidos en un sistema informático privado. La conducta en mención castiga al que “destruyere, deteriorase, borrarse, alterase o suprimiese informaciones, datos o programas informáticos ajenos”^{lxxxiii}. Estamos hablando de un auténtico sabotaje informático que no presenta mayores problemas para su estructuración.

Sin embargo, el término “informaciones” contenido en el tipo penal, si representa problemas inocultables. Toda vez que, el Código Penal italiano no especifica qué tipo de información es la que se protege mediante este delito. Y frente a tal indefinición, podría

pensarse que incluye la información contenida inclusive en documentos físicos, como libros o manuscritos.

Este problema es resaltado por Salvadori (2014) quien al respecto manifiesta:

No parece adecuada, sin embargo, la referencia que, junto con los datos y los programas informáticos, se hace a las informaciones, ya que su mención amplía de manera excesiva el ámbito de aplicación del delito, posibilitando la subsunción en el artículo 635-bis del C.P. de los meros daños a informaciones contenidas en un documento de papel o que de todos modos no se puedan tratar mediante un programa informático (p. 90).

Resulta evidente que la inclusión del término genérico “informaciones” en la redacción del tipo penal italiano representa un problema para su aplicación. Por lo que una solución simple pero contundente frente a este problema, sería la aclaración expresa en el tipo penal, de que se hace referencia a “informaciones contenidas en sistemas informáticos”. Tal y como sucede con el delito de descubrimiento de secreto contenido en “archivo o fichero” en el Código Penal español, o en el delito de violación a datos personales “contenidos en ficheros, archivos, bases de datos o medios semejantes” consagrado en la legislación colombiana.

3.2. Daños a sistemas informáticos o telemáticos. Art. 635-*quater*. Código Penal italiano

Esta conducta contempla dos formas distintas de comisión, así como dos resultados distintos. Sin embargo, con la concurrencia de uno de los dos resultados ya es suficiente

para la consumación del tipo penal. Antes de estudiar estos elementos, es necesario remitirnos a la redacción legal:

“quien mediante las conductas mencionadas en el artículo 635-bis, C.P. o a través de la introducción o la transmisión de datos, informaciones o programas informáticos, destruya, dañe o inutilice en todo o en parte sistemas informáticos o telemáticos ajenos, u obstaculice de manera grave su funcionamiento”^{lxxxiv}.

La *primera forma de comisión del delito* nos remite a las conductas del artículo estudiado en el acápite anterior. Es decir, destruir, borrar o alterar datos ajenos. En otras palabras, este segundo tipo penal se materializa cuando, mediante la destrucción, eliminación o alteración de datos contenidos en un sistema informático, **se daña o impide el normal funcionamiento** del sistema informático en el que se encuentra contenida esa información.

La *segunda forma de comisión del delito* consiste en la introducción y transmisión de datos en un sistema informático. Cuando esa introducción de datos genera **el daño o la obstaculización del funcionamiento** del sistema informático se estructura la conducta punible. Para ejemplificar esta modalidad de comisión de la conducta piénsese en aquellos casos en los que se introduce un “virus” o “malware” en un sistema informático con el fin de destruirlo.

Como puede colegirse de los párrafos anteriores, uno de los dos siguientes *resultados* debe producirse: el daño en el sistema informático o la obstaculización grave del funcionamiento del sistema informático o telemático. Un clásico y paradigmático ejemplo

en este sentido son los mencionados ataques de denegación de servicio (*Denial of Service* o *Distributed Denial of Service Attacks*), que impiden el correcto funcionamiento de un sistema informático, si bien no causan, en sentido estricto, ningún daño a los datos y a los programas informáticos (Salvadori, 2014, P. 96).

3.3. Daños a datos y a sistemas informáticos públicos o de utilidad pública. Arts. 635-ter y 635-quinquies del Código Penal italiano.

Las dos figuras típicas estudiadas en los acápites anteriores, se ven reproducidas en los artículos 635-ter y 635-quinquies del Código Penal italiano, con la diferencia de que el objeto sobre el que recae la conducta debe ser de uso del Estado, o de utilidad pública. En otras palabras, se cometen estos delitos cuando se “dañan” sistemas informáticos de utilidad pública, o cuando se “altera”, “elimina”, “deteriora” o “sustraer” datos contenidos en un sistema informático de utilidad pública. De la siguiente forma se han tipificado estas conductas punibles: el que “causare daños ocasionados a informaciones, datos y programas informáticos utilizados por el Estado o por otra entidad pública o que de todos modos resulten ser **de utilidad pública**” (art. 635-ter) y el que causare “daños ocasionados a sistemas informáticos o telemáticos **de utilidad pública**” (art. 635-quinquies)^{lxxxv}.

Entonces, reiteramos, la única diferencia encontrada entre las figuras estudiadas en los dos acápites anteriores y las abordadas en este apartado, es que el objeto material sobre el que recae el delito en estas últimas son los datos o los sistemas informáticos utilizados por el Estado, o que en cualquier modo sean de utilidad pública.

4. CHILE

La tipificación de delitos informáticos se ha dado en la legislación chilena mediante la “ley 19233 relativa a Delitos Informáticos”. En dicha norma, se han establecido 4 conductas punibles, a saber: i) el daño o inutilización en contra de un sistema de tratamiento de datos; ii) el acceso a sistema de tratamiento de datos; iii) el daño en contra de los datos contenidos en el sistema; y iv) la revelación de los datos contenidos en un sistema de información.

Antes de entrar a estudiar las figuras típicas consagradas por la ley en mención, es necesario determinar cuál es el bien jurídico tutelado por esas conductas. Al respecto, Vera (1996) afirma:

Con la entrada en vigencia de esta Ley se establece un nuevo bien jurídico protegido cual es "la calidad, pureza e idoneidad de la información contenida en los sistema de tratamiento de la misma, así como de los productos provenientes de la operación de dichos sistemas". De tal manera que todo atentado que signifique desviar el correcto desempeño del sistema de Tratamiento de Información (automático o manual) con la finalidad de producir un perjuicio que redunde en un beneficio material o moral para sí o para otro, deberá constituir el elemento que dé la característica del delito en su manifestación más común. (p. 190).

Ahora bien, los tipos penales que en Chile atentan contra el bien jurídico de la calidad, pureza e idoneidad de la información contenida en sistemas informáticos, son los siguientes:

4.1. Daño o inutilización en contra de un sistema de tratamiento de datos

El artículo primero de la citada ley señala:

Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Lo primero que debe señalarse es que esta norma distingue entre el daño en contra de un sistema informático, y la inutilización del mismo. Es decir que, “el sistema informático (referido sólo al hardware según la redacción del artículo) puede sufrir un atentado directo que le cause daños permanentes o irreversibles, a través de las acciones destinadas a destruirlo o inutilizarlo. En tal caso, los verbos rectores del tipo serán el "destruir", esto es, el deshacer, arruinar o asolar una cosa material (en este caso el hardware); y el "inutilizar", que significa hacer inútil, vana o nula una cosa, por ejemplo, si luego del ataque el sistema no sirve para el procesamiento de datos o ve limitada su utilidad, sin necesidad de destruirlo.” (Herrera y Nuñez, 1999, p. 253).

Ahora bien, desde la Doctrina chilena, se ha esbozado una crítica a la redacción de este artículo, consistente en que, no se trata de un caso de sabotaje informático, sino simplemente de un delito de “daño” en contra de los bienes corporales muebles que integran el sistema informático. Así, Herrera y Nuñez (1999) señalan:

En primer lugar, a diferencia de lo que se ha escrito hasta ahora respecto a la Ley N° 19.223, nosotros no creemos que este artículo tipifique al sabotaje informático, sino más bien trata un delito de daños convencional sobre los bienes corporales muebles que integran un sistema de tratamiento de información. La razón se debe a que al haber circunscrito el delito informático únicamente para los atentados contra el soporte lógico de un sistema de tratamiento de información, es decir, programas (o sea, instrucciones) y datos relevantes, y al hacer mención expresa a los datos en el inciso 2º, pensamos que el inciso 1º, apunta en dirección del soporte físico, las partes o componentes del sistema, **objeto no comprendido dentro de los delitos informáticos** (p. 253).

Contrario a lo señalado por los autores citados, consideramos que sí es un auténtico caso de sabotaje informático, y por ende, si se trata de un delito informático. Toda vez que, el objeto sobre el cual recae el delito, es el sistema informático, el cual no puede llegar a ser caracterizado (debido a que en ocasiones no lo es) como un bien corporal susceptible de valoración económica. Recordemos que, el concepto que acogimos al momento de tomar postura frente a la discusión terminológica de delito informático *versus* cibercrimen, fue el de delito informático en sentido limitado o restringido. Entendido únicamente como los atentados en contra de **los sistemas informáticos**, y de los datos almacenados en esos sistemas. Así las cosas, consideramos que el delito en mención sí configura un sabotaje informático, y no un atentado meramente patrimonial.

4.2. Acceso a sistema de tratamiento de datos (sistema informático) con fines de espionaje

La conducta tipificada mediante el artículo 2 de la ley chilena 19.233, consagra la punición del “hacking”, pero únicamente cuando el mismo tenga la finalidad de “apoderarse, usar o conocer indebidamente” la información contenida en el sistema informático. Es por esta razón, que hablamos de “hacking” con fines de espionaje^{lxxxvi}. La redacción legal es la siguiente:

Artículo 2. El que con el ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio^{lxxxvii}.

Lo más importante que se debe resaltar frente a este tipo penal, es que contempla un elemento subjetivo especial del tipo, por cuanto para su comisión se requiere en el autor un ánimo de “apoderarse, usar o conocer indebidamente” la información. Así las cosas, los verbos rectores de la conducta son: “interceptar”, “interferir” o “acceder” al sistema informático. Es claro que, aunque no se haya contemplado expresamente, esa interceptación, interferencia o acceso debe ser “no consentido”. Pues de lo contrario, el consentimiento actuaría como causal de justificación.

4.3. Daño en contra de los datos contenidos en el sistema

El artículo tercero de la ley chilena relativa a delitos informáticos establece como conducta delictiva la alteración, destrucción o daño de **la información o los datos** contenidos en el sistema informático.

Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Se trata de un delito típicamente informático, por cuanto lo que pretende proteger es precisamente la información y los datos contenidos en el sistema de procesamiento de datos. Nuevamente debe decirse que, esa destrucción o alteración debe ser no autorizada. Pues, si quien realiza esas conductas, es precisamente el titular del sistema informático, mal se haría al señalar que se trata de una conducta delictiva.

Ahora bien, resulta importante distinguir entre el daño a los datos castigado por este tipo penal, y el daño a los datos tipificado por el inciso segundo del primer artículo de la ley chilena. Al respecto, debe decirse que “esta conducta es claramente distinta de la alteración de datos a que se refiere el inciso 2o del artículo 1, ya que ahora, la acción está dirigida intencionalmente a obtener el resultado y no como en el artículo 1, en que el resultado logrado no es buscado por el agente, sino que se consigue como consecuencia de la comisión de un delito de daños convencional (a sistema informático)” Paréntesis fuera del texto original (Herrera y Núñez, 1999, p. 262).

4.4. Revelación de los datos contenidos en un sistema de información

El último delito consagrado en la ley chilena de delitos informáticos, artículo cuarto, castiga al “que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

Se trata pues, de otro caso de “espionaje informático” en el que lo que se intenta proteger, es la disponibilidad de los datos contenidos en un sistema de información. Es decir, esa potestad que tiene el titular del sistema informático de decir cuáles datos saca a la luz pública, cuáles usa, y cuáles simplemente deja al margen del conocimiento de los demás.

Debe tenerse en cuenta que, este tipo penal de “espionaje” ya no castiga el acceso a la información, como lo hace el delito de acceso con fines de espionaje consagrado en el artículo segundo de la ley chilena de delitos informáticos, sino que, castiga la revelación o difusión de esa información. Es decir, no tipifica el “conocer” la información o el “acceder” a ella, sino los actos posteriores de divulgación de esa información.

Una vez evacuado el estudio de algunos ordenamientos jurídicos, y concretamente de sus disposiciones normativas al respecto, podemos considerar las previsiones y modalidades, así como la técnica y materias aboradas por las legislaciones foráneas estudiadas, con el único propósito de fijar como marco comparativo y tener una base de referencia, que con

criterio de autoridad nos permita el desarrollo y planteamiento de la discusión, y la propuesta que consideramos ofrece solución a la discusión.

Dicho lo anterior, pasaremos entonces al análisis de la discusión nuclear de este trabajo, específicamente el estudio del delito de hurto por medios informáticos, sus elementos, previsiones, ubicación, problemas de aplicación y consecuencias de su tipificación autónoma, para de esta forma ofrecer con fundamento, y recogiendo en su integridad los planteamientos del texto, una propuesta que permita superar la problemática identificada.

CAPITULO III. HURTO POR MEDIOS INFORMÁTICOS.

Hemos llegado entonces, al escenario central y nuclear del objeto de este trabajo de investigación. Para efectos ilustrativos, y con el fin de desarrollar la problemática propuesta, es necesario centrarnos en los elementos de análisis del delito de hurto por medios informáticos.

En primer lugar, estableceremos cual es el objeto de protección, y el bien jurídico tutelado por esta conducta punible. Asimismo analizaremos desde una perspectiva dogmática sus elementos objetivos y subjetivos. A continuación, delimitaremos cuales son los problemas de la tipificación de esta modalidad delictiva, identificaremos los principales problemas de su tipificación en tales condiciones. Todo lo anterior como contextualización y análisis para en el siguiente capítulo poder ofrecer una solución que articule el objeto de este trabajo.

1. Perspectiva general del hurto por medios informáticos

Ya se anticipaba que el hurto por medios informáticos fue tipificado en Colombia mediante la ley 1273 de 2009, en la cual, adicionalmente, se “creó” el bien jurídico de la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Así, el tipo penal de hurto por medios informáticos fue ubicado por el legislador colombiano dentro de los delitos que atentan en contra del bien jurídico ya mencionado. Sin embargo, un sector de la doctrina, al cual nos suscribimos, afirma que el bien jurídico protegido por ese tipo penal no es la información y los datos, sino el patrimonio económico, por lo que simplemente se está contemplando un “nuevo” medio para la comisión del delito de hurto, pero en un tipo penal autónomo. Un ejemplo de lo anterior es el caso en que hipotéticamente se tipificara el homicidio mediante arma de fuego como tipo penal independiente, o el clásico ejemplo del hurto automovilístico, en el cual, se utiliza como medio para cometer el hurto un automóvil.

Esta discusión acerca del bien jurídico protegido por el tipo penal de hurto por medios informáticos será abordada con profundidad más adelante. Por supuesto, al final de la misma, tomaremos postura frente a cuál es el bien jurídico que consideramos debe ser protegido por ese tipo penal, frente a lo cual debemos anticipar que, el objeto jurídico de protección del delito en comento es el patrimonio, y su tipificación autónoma, lejos de resolver cualquier confrontación que se quisiera anticipar mediante su introducción al

mundo jurídico, lo que hizo fue crear problemas de inocultable importancia práctica, los cuales serán objeto de un capítulo aparte.

A renglón seguido, en el siguiente capítulo, se abordará el estudio de la estructura dogmática del novedoso tipo penal, haciendo especial énfasis en sus elementos objetivos. Allí, se analizarán los términos estrictamente informáticos contenidos en el tipo penal, como por ejemplo el término de “medidas de seguridad informática” o “sistemas de autenticación y autorización”. Se trata pues, de un capítulo meramente descriptivo cuyo principal objetivo es poner de relieve los elementos más relevantes de la conducta típica estudiada. Finalmente en este capítulo, elevaremos algunas conclusiones respecto de las peculiares características de este tipo penal.

Por último, se esbozarán los principales problemas derivados de la tipificación autónoma del hurto por medios informáticos. Frente al particular, debe señalarse que en la legislación colombiana existe una circunstancia de calificación específica para el delito del hurto contenida en el numeral 4 del artículo 240, la cual señala que el hurto será calificado cuando se cometa “violando o superando seguridades electrónicas **u otras semejantes**”. La existencia de esta circunstancia de calificación conlleva a una pregunta que no obtiene fácil respuesta: en los apoderamientos que se realizan a través de sistemas informáticos, y se superan las medidas de seguridad contenidas en esos sistemas, ¿Se tipifica el hurto calificado por la causal recién señalada o el hurto por medios informáticos? ¿Por cuál de las dos conductas punibles ha de ser condenado el delincuente? ¿Puede existir concurso de conductas punibles entre el hurto por medios informáticos y el hurto calificado por la causal número 4?

Entonces, en ese último capítulo se explicarán todos los problemas derivados de la tipificación autónoma del hurto por medios informáticos, y se propondrán de forma somera cuáles consideramos las soluciones más viables de cara a la superación de esas dificultades.

2. El bien jurídico protegido por el hurto por medios informáticos

Para iniciar con el estudio del tipo penal de hurto por medios informáticos, resulta necesario delimitar cuál es el bien jurídico que se pretende proteger con su consagración. Partimos entonces de una aproximación al concepto de bien jurídico, entendido como “objetivos político-criminales vinculados a los valores superiores consagrados en la Constitución Política” (Balmaceda, 2014, p. 30), es decir, esos valores esenciales que por su importancia social deben ser objeto de protección mediante el Derecho Penal.

Tres son las posturas que pueden erigirse sobre el bien jurídico protegido mediante el tipo penal de hurto por medios informáticos^{lxxxviii}. En primer lugar, la teoría según la cual, el objeto jurídico de protección en este delito es la confidencialidad, integridad y disponibilidad de la información y los datos. En segundo lugar, la tesis que afirma que el bien jurídico protegido es el patrimonio económico. Y finalmente, aquellas teorías mixtas que sugieren una protección penal dual de los anteriores bienes jurídicos, ya sea como tipos penales pluriofensivos, o en su defecto bajo la tesis de bienes jurídicos intermedios. Desde ya, anticipamos que consideramos correcta la segunda postura. Pero antes de exponer nuestros argumentos, es necesario hacer un breve recuento de los fundamentos de cada una de ellas.

2.1. Primera postura. El bien jurídico protegido es el de la información y los datos

Sea lo primero advertir que no existe un sector representativo en la Doctrina que suscriba esta postura. Pero sí existe una razón (más bien, una falencia legislativa) que podría llevar al intérprete desprevenido a pensar que el bien jurídico protegido en este caso es el de la información y los datos. Esa razón/falencia es la ubicación dada por el legislador al tipo penal de hurto por medios informáticos dentro del título de los delitos contra la información y los datos, además de su inclusión autónoma en el ordenamiento punitivo.

Así lo señalan Manjarrés y Jiménez (2012):

(...)cuando se refiere a los “atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”. Corrobora la importancia de la información como activo de valor para las organizaciones (ISO/IEC 17799/2005), que es necesario proteger adecuadamente para garantizar la continuidad del negocio, la maximización del retorno de la inversión y el aprovechamiento de las oportunidades del entorno, así como para disminuir y contrarrestar los riesgos y delitos que la amenazan. (p. 79)

2.1.1. Ubicación del tipo penal de hurto por medios informáticos

La principal razón que, eventualmente, podría llevar al interprete a afirmar que el bien jurídico tutelado es el de la información y los datos, es la ubicación que se le ha dado al tipo penal objeto de estudio. Como señalábamos con antelación, este tipo penal de hurto por medios informáticos se encuentra consagrado en el capítulo segundo del título VII BIS

del Código Penal. Así, el título VII BIS se creó bajo la rúbrica “de la protección de la **información y los datos**” y el capítulo segundo de ese título, en donde se encuentra el delito en comento, se denominó “de los atentados **informáticos** y otras infracciones”.

Es decir que, haciendo una interpretación exegética del Código Penal colombiano, el hurto por medios informáticos es uno de los “**atentados informáticos** y otras infracciones”. Lo que podría llevar a pensar que es precisamente la información el bien jurídico tutelado con esta tipificación autónoma de hurto.

Esta fue la interpretación que se le dio a este tipo penal por parte de la Sala Penal del Tribunal Superior del Distrito Judicial de Neiva, cuando dicha corporación afirmó que el hurto por medios informáticos no era un delito en contra del patrimonio económico, y por ende no podía ser objeto de la rebaja por reparación integral consagrada en el artículo 269 del Código Penal.

En dicha providencia, fechada del 29 de agosto de 2013, la mencionada sala afirmó que el bien jurídico protegido por ese delito, era el de la información y los datos. Sin embargo, la ubicación dada a un tipo penal no es parámetro definitivo para determinar cuál es el bien jurídico protegido por el delito. Y precisamente por esta razón, la Corte Suprema de Justicia en sentencia 42724 del 11 de febrero de 2015, revocó la decisión del Tribunal Superior del Distrito Judicial de Neiva, afirmando que la rebaja era completamente procedente por tratarse de un delito en contra del patrimonio económico.

En este punto, por ser absolutamente pertinentes, vale la pena traer a colación las afirmaciones de Blanco (2012) cuando se preguntaba cuál era el bien jurídico protegido por el delito de lavado de activos:

Que el art. 301 CP se encuentre ubicado entre los delitos contra el orden socio-económico parece un paso adelante en la consideración económica del blanqueo de capitales. Ello ha de tener un reflejo en el bien jurídico que tal precepto pretende proteger, y puede ser un dato a favor para considerar el orden socio-económico como bien jurídico. **Sin embargo, se ha de advertir que la colocación sistemática no es un dato definitivo, sino «indiciado»; no se han de sobrevalorar las rúbricas clasificatorias puesto que «no necesariamente marcan el bien jurídico protegido a través de los delitos particulares».** Llegados a este punto, es necesario «contrastar la voluntad del legislador con el resultado de su actividad moldeadora en orden a detectar, no sólo el éxito o fracaso de su intervención, sino también el alcance real de la tutela proyectada y del tipo finalmente construido».

Como de forma afortunada lo señala el citado autor, la ubicación del tipo penal no es más que un dato “indiciario” acerca del bien jurídico protegido por el tipo penal específico. Así, si la colocación dada al tipo penal de hurto por medios informáticos corresponde a un auténtico yerro del legislador, mal se haría al afirmar que el objeto jurídico de protección en este caso es la información y los datos.

Esta problemática la expuso la Sala de Casación Penal de la Corte Suprema de Justicia, en sentencia del 11 de febrero del 2015, cuando señaló (arribando a la misma conclusión aquí expuesta) que:

Ciertamente, aunque el legislador fue consciente de la dificultad que comportaba la ubicación del bien jurídico protegido respecto de aquellas acciones antijurídicas reguladas dentro del mentado título, que de manera directa afectaban el patrimonio económico, prefirió atar, de manera anti técnica, como lo aseveró el representante de la fiscalía, la modalidad de la acción típica prohibida —que es el hurto por medios informáticos— al bien jurídico amparado en el referido título VII bis, que adicionar o modificar las circunstancias modales calificantes del artículo 240 del Código Penal, como hubiera sido lo ideal.

De lo hasta aquí dicho, es posible decantar, con meridiana claridad, que pese a la ubicación sistemática del punible de hurto por medios informáticos y semejantes en el título VII bis del Código Penal, rubricado bajo la denominación de la información y los datos, este bien jurídico resulta ser, para el caso concreto — como lo concibió la exposición de motivos del Proyecto de Ley 42 Cámara—, de naturaleza meramente intermedia, pues el interés superior protegido de manera directa es el patrimonio económico, entendido como ese conjunto de derechos y obligaciones, susceptible de ser valorado en términos económicos, más concretamente, en dinero. (CSJ-SP/11-02-2015).

Si bien, consideramos que la ubicación de un tipo penal en efecto es meramente “indiciaria” respecto del bien jurídico que busca proteger, no es posible dejar de lado, la importancia que la ubicación de los tipos penales debe tener al interior de la estructura propia del esquema normativo sustancial.

Es así como desde ya se vislumbra un objeto de crítica importante; pues la ubicación de un tipo penal, dentro de un esquema normativo, no puede ni debe efectuarse de manera caprichosa y aislada, sino por el contrario debe estructurarse bajo un modelo coherente, sistemático y con directa correspondencia con el bien jurídico objeto de protección. Cosa distinta es que existan tipos penales pluriofensivos, cuya ubicación se hará atendiendo la mayor cercanía o proximidad del tipo penal, con el bien jurídico bajo el cual se ubique, sin desconocer que el mismo, o mejor su eventual infracción atente no solo contra uno, sino contra varios bienes jurídicos.

2.2. Segunda postura. El bien jurídico protegido es el patrimonio económico

Más allá de la ubicación dada al tipo penal de hurto por medios informáticos por parte de la ley 1273 de 2009, resulta claro, por varias razones, que el bien jurídico que se pretende proteger mediante su consagración es el patrimonio económico^{lxxxix}, “entendido como ese conjunto de derechos y obligaciones, susceptible de ser valorado en términos económicos, más concretamente, en dinero”^{xc} (CSJ-SP/11-02-2015). Las razones que permiten realizar esta afirmación, pueden sintetizarse brevemente de la siguiente forma:

- i) existe remisión respecto de la conducta a realizar por parte del tipo penal de hurto por medios informáticos al tipo penal básico de hurto; y ii) existe remisión en la sanción a imponer.

2.2.1. Remisión en la conducta

Si se tiene en cuenta que, la conducta típica sancionada por el tipo penal de hurto por medios informáticos remite al tipo penal básico de hurto mediante la fórmula “el que,

superando medidas de seguridad informáticas, realice la conducta señalada en el art 239...”, necesario resulta concluir que se trata del clásico delito de hurto, sólo que cometido a través de un medio novedoso. Y en ese orden de ideas, al tratarse de una modalidad del hurto, el bien jurídico protegido por el tipo penal estudiado es el mismo que protege el hurto básico: el patrimonio económico.

2.2.2. Remisión en la sanción

Cuestión similar a la estudiada en el párrafo anterior, es la que sucede con la pena o sanción que ha de imponérsele a quien lleve a cabo el hurto por medios informáticos. Puesto que, este tipo penal remite a la pena del hurto calificado mediante la fórmula “...incurrirá en las penas señaladas en el artículo 240 de este código”. Y el artículo 240 del Código Penal hace referencia precisamente al tipo penal de hurto calificado.

Así, la inmensa mayoría de la Doctrina que estudia el tema afirma que el tipo penal de hurto por medios informáticos protege el bien jurídico patrimonio económico^{xcii}. Por ejemplo, Grisales (2014) afirma que “encontramos entonces que los delitos que nos ocupan pretenden tutelar el patrimonio económico aunque, como veremos más adelante, de unas específicas y novedosas formas de lesión que implican el empleo de medios informáticos” (p. 131).

Entonces:

(...) natural es concluir, como lo hiciera la demandante y el representante del ente acusador, que el tipo penal de hurto por medios informáticos y semejantes no solo está circunscrito al ámbito de punibles contra la información y los datos, sino,

esencialmente a la esfera de los lesivos del patrimonio económico, pues es el valor ético jurídico que al final resultaría atacado con la sustracción de dineros a través de mecanismos ilícitos de manipulación de los sistemas informáticos, electrónicos, telemáticos o similares, o suplantación de las personas ante los sistemas de autenticación y de autorización. (CSJ-SP/11-02-2015)

De la misma forma, y continuando con la argumentación de cara a la justificación del bien jurídico objeto de protección en punto del hurto por medios informáticos y semejantes, concretamente en lo que hace relación con su objeto de protección tenemos que ““Los atentados informáticos y otras infracciones”; referidos en los artículos 269I “Hurto por medios informáticos y semejantes” y 269J “Transferencia no consentida de activos”, [son] entendidos normalmente como delitos ‘ordinarios’ en cuya realización es importante el uso de recursos tecnológicos contemplados en el capítulo II de la Ley 1273 de 2009 analizada. (Ojeda-Pérez, Arias-Flórez, Rincón-Rodríguez y Daza-Martínez, 2010, p. 57). Lo anterior supone entonces, que finalmente, el objeto de protección lo será entonces, el bien jurídico que como delito común protege, con la consideración especial del uso de recursos tecnológicos.

Asimismo, algunos acuñan conceptos interpretativos más radicales, señalando sin dubitación alguna al patrimonio como objeto de protección, no solo para el hurto por medios informáticos y semejantes, sino en general para los delitos informáticos, al circunscribirlo a un elemento netamente patrimonial, postura que dicho sea de paso rechazamos, pero que para efectos de la discusión es necesario mencionar: “Es de anotar

que los delitos informáticos, en Colombia se encuentran clasificados dentro de los delitos de patrimonio económico, porque esta clase de delitos llegan a ocasionar un detrimento patrimonial, ya sea una persona natural, jurídica o una entidad gubernamental, donde dependiendo de la modalidad la cuantía del delito puede alcanzar cifras astronómicas. (Arzuaga y Guevara, 2013, p. 29).

Así las cosas, y como profundizaremos más adelante, es necesario concluir que el objeto de protección con el ilícito de hurto por medios informáticos y semejantes, lo es justamente el patrimonio económico.

2.3. Posturas mixtas.

Finalmente, la doctrina ha señalado que existen posturas mixtas, que necesariamente atribuyen como objeto de protección, dos bienes jurídicos, el primero de ellos, de carácter individual (patrimonio económico), y el segundo, colectivo (protección de la información y los datos).

Si bien es cierto, existe consenso en los defensores de esta tesis al interior de la doctrina, respecto de la dualidad de protección de estos dos bienes jurídicos; en lo que no hay acuerdo, es en la determinación de su consideración como delito pluriofensivo, o como bien jurídico intermedio.

Como referíamos en precedencia autores como Meek señalan que el tipo penal de hurto por medios informáticos y semejantes, es sin lugar a dudas un tipo penal pluriofensivo, es decir, que protege dos bienes jurídicos, uno de ellos individual y el otro colectivo.

De forma paralela, se destaca la postura de Suárez Sánchez, quien circunscribe el objeto de protección, a la tesis de los bienes jurídicos intermedios, como a continuación se expone:

En el delito de hurto por medios informáticos y semejantes, además del patrimonio económico, se protege otro bien de naturaleza colectiva o supraindividual, dado que la ejecución de tal hecho punible no sólo producirá efectos sobre el patrimonio individual sino también sobre los fundamentos del propio sistema informático. Esta interpretación dual (individual y colectiva) del bien jurídico conduce a admitir que la comisión de un delito de hurto por medios informáticos y semejantes produce, además de la pérdida patrimonial para un individuo, la lesión de la seguridad y la confianza que los ciudadanos deben tener en los sistemas informáticos, las redes de sistemas electrónicos, telemáticos y otros medios semejantes. (Suárez, 2010, p. 237)

No obstante ello, claramente la consideración de Suárez, no se circunscribe al ámbito de los delitos pluriofensivos como destaca Meek, sino que los enmarca en la novedosa tesis de los tipos penales intermedios, esto es que:

Al tenerse al delito de hurto por medios informáticos y semejantes como un delito protector de valores supraindividuales, su estructura ha de consistir en que la conducta se encamina a causar la inmediata lesión de un bien jurídico de naturaleza individual (el patrimonio), y ocasiona, además, la mediata y abstracta puesta en peligro de otro bien jurídico de naturaleza colectiva (el correcto

funcionamiento de los sistemas de información y datos). (Suárez Sánchez, 2010, p. 239)

Como críticas a estas posturas podemos formular las siguientes:

1. Se advierte una esforzada argumentación para soportar la protección de los sistemas de información y datos, al punto de indicar que se trata de bienes jurídicos de peligro abstracto, cuya verificación se da con mayor facilidad, una vez se establece la lesión del bien jurídico individual, concretamente, el patrimonio económico.
2. Esta postura antepone, superpone y prevalece el patrimonio económico. Destaca la posibilidad de la tentativa, por considerarlo delito de lesión, lo que se contradice con su dualidad, pues si admite la tentativa, supone que no se lesionó efectivamente el bien jurídico individual, por lo que mucho menos se habrá de poner en riesgo aunque sea de forma abstracta, el bien jurídico supraindividual o colectivo.
3. La tesis más que determinar con exactitud el bien jurídico objeto de tutela, busca justificar de manera forzada, la ubicación del tipo penal en los delitos informáticos.
4. No explica por qué razón la información y los datos, son considerados como un bien jurídico colectivo, tesis que tampoco compartimos, pero que desborda el objeto de estudio de este trabajo, pero además, deja de lado pronunciarse frente a la necesidad de desbordar la protección del patrimonio, cuando necesariamente en el hurto por medios informáticos y semejantes, la afectación como *conditio sine qua non*, recae sobre el patrimonio económico. Es necesario destacar que el patrimonio de muchos, no deviene el bien jurídico en colectivo, como tampoco la información y datos plurales, desencadena en un objeto de protección supraindividual.

3. Análisis dogmático del tipo penal de hurto por medios informáticos

Habiendo dejado claro que, el bien jurídico protegido por el tipo penal de hurto por medios informáticos no es otro distinto al patrimonio económico, resulta necesario estudiar los demás elementos del tipo penal, tanto desde el plano objetivo, como desde el subjetivo. La redacción legal del hurto por medios informáticos es la siguiente:

Artículo 269I: *Hurto por medios informáticos y semejantes*. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

3.1. Elementos Objetivos

Se trata de elementos “objetivos” del tipo penal, debido a que hacen parte de la cara externa del delito. Son esos elementos que no requieren para su estructuración de la verificación acerca de aquello que quiere o desea el autor. En otras palabras, en el tipo objetivo “debe mirarse la cara “externa”, “objetiva” u “objetivada” de la descripción típica, que no solo contiene objetos del mundo exterior, sino también otros elementos que -por encontrarse situados fuera de la esfera psíquica del autor— pueden comportar una valoración más allá de lo meramente descriptivo, sin que sea viable separar lo objetivo de lo subjetivo con base en una división formal tajante” (Velásquez, 2011, p. 349).

Así, los elementos básicos que componen cualquier tipo penal son: i) sujetos activo y pasivo; ii) acción típica; y iii) el bien jurídico. Sin embargo, debido a la importancia que en este caso ostenta el tema del bien jurídico^{xcii}, dicho tópico fue objeto de estudio en un apartado independiente. Ahora bien, en consideración a las especiales características que presenta el tipo penal bajo estudio, existen otros elementos objetivos que deben ser mencionados, como lo son el objeto material sobre el que recae la acción y los medios determinados para la comisión del delito.

3.1.1. Sujetos activo y pasivo

Los términos “sujeto activo”, “agente”, “actor” o “autor”^{xciii} del delito hacen referencia a la persona que lleva a cabo la conducta contemplada en el tipo penal.

Ahora bien, el sujeto activo puede ser indeterminado o calificado. Será indeterminado cuando el tipo penal no exige ninguna calidad especial en la persona que comete el delito, y calificado cuando la existencia de las calidades sí es exigida por la redacción legal.

Frente al hurto por medios informáticos, debe decirse que se trata de un tipo penal de sujeto activo indeterminado, puesto que, el artículo 269I hace uso de la fórmula “el que”^{xciv}. Lo que permite afirmar que cualquier persona, sin tener que ostentar determinada calidad, puede cometer el delito.

Frente al sujeto pasivo del delito, esto es, el titular del bien jurídico vulnerado o puesto en peligro con la comisión del delito, puede realizarse la misma distinción entre sujeto pasivo indeterminado y calificado.

Respecto del tipo penal estudiado en el presente capítulo, ha de decirse que es de sujeto pasivo indeterminado, pues cualquier persona puede ser el titular del bien jurídico que se ve violentado mediante la comisión del hurto por medios informáticos. Inclusive una persona jurídica. En otras palabras, “el sujeto pasivo de la infracción, por su parte, no está expresamente determinado en la norma, aunque es posible inferirlo de la conjunción de los tipos base y subordinado, de tal suerte, que lo será el titular del derecho patrimonial burlado o poseedor del dinero sustraído, que, según el caso, podrá serlo el usuario financiero y/o la persona jurídica que lo custodia, dependiendo de cuál sea la barrera informática, telemática o electrónica comprometida para acceder al circulante” (CSJ-SP/11-02-2015).

3.1.2. Conducta

Como ya se anticipó, la conducta típica del hurto por medios informáticos no fue contemplada de forma directa en el artículo 269I, sino que el legislador optó por hacer remisión expresa a la conducta del artículo 239, esto es, el tipo penal básico de hurto. Entonces, la acción típica del hurto por medios informáticos la realiza “el que se apodere de una cosa mueble ajena”. Por apoderamiento, debe entenderse el “entrar en dominio de una cosa. Consiste en tener la posibilidad de actuar respecto de un bien como si se fuese señor y dueño de él. El apoderamiento se consuma cuando el agente elude de forma definitiva todas las medidas de custodia del bien de parte de la víctima” (Enciso, 2011, p. 336).

El apoderamiento se dará, por ejemplo, cuando el sujeto activo accede a las plataformas informáticas de una entidad financiera, y traslada los fondos contenidos en una de las

cuentas, pasándolos a otra cuenta de propiedad del delincuente y retirándolos mediante un cajero automático. De igual forma se presenta el apoderamiento, cuando el autor del delito manipula el sistema informático de tal manera que, todas las consignaciones que se realicen en determinada cuenta, sean desviadas a otra cuenta de una entidad financiera distinta, cuyo titular sea el sujeto activo de la conducta criminal.

Sin embargo, si el delincuente no logra superar las barreras de protección del sistema informático, no se habrá dado el apoderamiento, y por ende, la conducta no se habría consumado. Por lo que el sujeto activo deberá responder por el delito de hurto por medios informáticos **en modalidad** tentada.

Para mejor ilustración piénsese en el siguiente ejemplo: el delincuente sustrae determinado monto de una cuenta de una entidad financiera, mediante la instalación de un virus que rompe con las medidas de seguridad del sistema informático, y logra que dicho dinero entre en una cuenta de su propiedad. Sin embargo, el sistema informático cuenta con una alerta de fallas, lo que permite que la entidad financiera bloquee casi de forma inmediata la transacción fraudulenta. Aun cuando el delincuente llegó a tener el dinero en su cuenta por unos instantes, lo cierto es que nunca tuvo la posibilidad real de actuar como señor y dueño de él. Por lo que, podría afirmarse que el apoderamiento nunca se dio, y por ende, que la conducta típica nunca se consumó.

3.1.3. Medios determinados

A lo señalado en el párrafo anterior debe añadirse que, para que se estructure el tipo penal de hurto por medios informáticos, la acción típica debe realizarse a través de unos

medios determinados. Motivo por el cual, resulta imprescindible estudiar cuáles son los medios determinados contemplados en el artículo 269I del Código Penal.

Así las cosas, si el hurto no se comete a través de estos medios determinados se tipificará un hurto ordinario ya sea simple, agravado o calificado, según el caso, pero no un hurto por medios informáticos. Así lo ha manifestado la Sala de Casación Penal de la Corte Suprema de Justicia:

En verdad, el precepto examinado —269I— solamente se ocupa de establecer el sujeto activo indeterminado —no cualificado o común y unisubjetivo⁽⁴⁶⁾— del punible y de consagrar unos específicos ingredientes normativos, que lo identifican como **un tipo de medio concreto o, si se quiere, determinado**, por cuanto estructura una modalidad o mecanismo específico de desapoderamiento de la cosa mueble ajena, a saber, superar las seguridades informáticas mediante i) la manipulación del sistema informático, la red de sistema electrónico, telemático u otro semejante o ii) la suplantación de una persona ante los sistemas de autenticación y de autorización establecidos. (CSJ-SP/11-02-2015).

Así, los medios que deben utilizarse para que se estructure el tipo de hurto por medios informáticos son los siguientes: i) manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante o ii) suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

Cuando se hace referencia a la *manipulación de un sistema informático, una red de sistema electrónico, telemático u otro medio semejante*, hace referencia al grupo de

conductas cometidas por el “cracker” que supera las medidas de seguridad del sistema con el fin de apoderarse de los recursos que se manejan y canalizan a través de ese sistema. Por ejemplo, cuando el delincuente logra controlar de forma cabal las operaciones que se realizan por intermedio de ese sistema informático. Así, desde la comodidad de su casa, el delincuente que manipuló el sistema informático podrá desviar recursos de una cuenta a otra, sustraerlos e incluso eliminarlos a su antojo.

Frente a este primer medio determinado para la comisión del delito, Grisales (2014) ha señalado lo siguiente:

Otro de los ingredientes de la conducta es lo que definiremos como “manipular”, y esto corresponde, según la Real Academia de la Lengua, a “... manejar cosas, controlar cosas, situaciones”. Uniendo así los dos conceptos, tenemos que ese elemento del tipo “manipular un sistema informático”, corresponde al manejo o control del *hardware* que incluye computadores —para este caso los cajeros electrónicos— y sistemas de almacenamiento externo de información —bandas magnéticas o *chips* de las tarjetas electrónicas que almacenan o conservan información—, a través de las cuales se accede a una pequeña parte del sistema o a la información a la que tiene acceso el cliente del banco a quien le hurtaron su “llave” de ingreso a este, permitiendo con ello manipular el sistema con la finalidad de acceder a la cuenta del cliente y desde allí realizar retiros de su dinero a través de cajeros o transferencias electrónicas. (p. 156)

Cuando se habla de *suplantar a un usuario ante los sistemas de autenticación e identificación*, se alude a aquellos casos en los que el criminal logra acceder, de cualquier

forma, a los datos de identificación virtual (usuario y contraseña) de la víctima, y posteriormente ingresa al sistema informático. Pero esta vez no está manipulando el sistema, por lo que el mismo permanece incólume. Simplemente está ingresando al mismo con los datos de identificación genuinos, sólo que sin estar autorizado por el titular de la cuenta en la que se encuentran depositados los fondos.

A modo de ejemplo, puede hablarse del caso en el que un dueño de un “café internet” espía las claves y usuarios que los clientes ingresan en los portales web de las entidades bancarias, y posteriormente procede a ingresar a las cuentas de los clientes utilizando los datos que logró observar.

Otro claro ejemplo, es aquel en el que se clonan las bandas magnéticas o los “chips” de las tarjetas de crédito, y después con la tarjeta “clonada” se retiran fondos de los cajeros automáticos. En este caso, el sistema de autenticación ya no será el compuesto por el usuario y la clave, sino que será la tarjeta (y los datos contenidos en la banda magnética o el “chip”) junto con la clave.

Entonces, ¿Existe diferencia entre autenticación y autorización? Pues bien, el sistema de autorización es entendido como “un proceso digital —una vez digitada la clave o password— por el cual una red de datos autoriza a un usuario previamente identificado a acceder a determinados recursos de esta”. En cambio, la autenticación:

(...) es aquel proceso de verificación de la identidad digital de quien remite una comunicación como una petición para conectarse. El usuario remitente puede ser una persona, un computador o un programa elaborado bajo un lenguaje especial y

enviado desde el computador o dispositivo de comunicación. En un sitio web de confianza —página de banco o de compras—, la autenticación es el modo de asegurar que los usuarios son quienes dicen ser, es decir, que el usuario que intenta ingresar al sistema a realizar funciones es de hecho el usuario que tiene la autorización para hacerlo, si está plenamente identificado por el sistema. (Grisales, 2014, p. 157)

3.1.4. Objeto material sobre el que recae la acción

El objeto material sobre el que recae la conducta es cualquier bien mueble ajeno^{xcv}. Por bien mueble, debe entenderse cualquier objeto susceptible de valoración económica (recordemos que el criterio dominante en Colombia es el del concepto jurídico-económico de patrimonio) que pueda ser trasladado de un lugar a otro. Se requiere entonces que sea un objeto corporal, pues sólo así podrá ser sujeto de un apoderamiento.

No concordamos con un sector de la doctrina que afirma la posibilidad de que el objeto material del hurto por medios informáticos sea la información contenida en las bandas magnéticas de una tarjeta de crédito. Pues el acceso y uso de esa información corresponde simplemente a uno de los “medios determinados” para la comisión del delito^{xcvi}. En ese orden de ideas, el objeto material del delito no sería la información contenida en las bandas magnéticas de las tarjetas de crédito, sino que sería el dinero que después es apropiado por el criminal que utiliza esa información para lograr su cometido.

Resulta entonces desafortunada la afirmación de Grisales (2014) cuando señala:

La redacción del artículo remite a lo descrito en el canon 239 del Código Penal: se hace referencia a una “cosa mueble”, que es aquel bien corporal —como el dinero— o incorporal —como la información privilegiada— que va implícita en la acción del apoderamiento descrita en el artículo 269I del Código Penal (...).

El primero se presenta en el momento en que es copiada la información o se desapodera al titular de la tarjeta débito o crédito y las claves para ingresar a un sistema a fin de suplantar a un usuario, y el segundo, cuando se da el apoderamiento físico de la cosa mueble ajena, que puede ser dinero, retirado previamente de un cajero o transferido a otra cuenta; o en el caso de la información personal o empresarial, al momento de ser recopilada en cualquier medio magnético que sirve para su copiado (p. 160).

Esa “información personal o empresarial” a la que se refiere el citado autor, **no puede ser objeto de un hurto por medios informáticos**, puesto que no es viable un apoderamiento en términos físicos. Además, subsiste el problema de valorar económicamente esa información. Que bien podría tener un gran valor, así como podría no representar un solo centavo.

Ahora bien, esto no significa que la información no sea protegida penalmente, pues, como ya se mencionó en la primera parte de este texto, dichos datos se encuentran tutelados por el delito de “violación de datos personales contenidos en ficheros, archivos o bases de datos...”. Lo claro es que, bajo ninguna circunstancia, esa información puede ser objeto de un hurto.

3.2. Elementos subjetivos del tipo penal

El hurto por medios informáticos únicamente admite la modalidad de comisión dolosa. Esto quiere decir que, el conocimiento y la voluntad del sujeto activo deben estar encaminados al apoderamiento, a través de uno de los medios determinados de comisión del delito. Se excluye de plano entonces la posibilidad de que se cometa el delito a título de culpa.

Adicionalmente, de forma idéntica al tipo básico de hurto, en el hurto por medios informáticos se contempla un elemento subjetivo especial del tipo penal: el propósito de obtener provecho para sí o para un tercero. Es una **finalidad** que debe buscar el sujeto activo, pero no es un resultado que deba concretarse. De lo contrario, si se llegase a exigir la consecución de un provecho patrimonial en quien comete el hurto, no se tipificaría el delito en aquellos casos en los que, por ejemplo, el sujeto activo invierte más dinero en la ejecución del hurto, que lo que efectivamente se apropia. Y no se tipificaría porque no hay un provecho económico en el delincuente. Incluso, por paradójico que suene, podría afirmarse que lo que se presentó fue un perjuicio en el patrimonio del criminal.

3.3. Conclusiones parciales

Del estudio de los elementos típicos del hurto por medios informáticos, pueden esbozarse las siguientes conclusiones respecto de las características del delito objeto de estudio -las críticas al mismo, se elevarán en capítulo aparte junto con las proposiciones para superar los problemas encontrados-:

3.3.1. El hurto por medios informáticos es un delito subordinado

Si bien es cierto que la consagración del artículo 269I supuso una tipificación autónoma del delito de hurto por medios informáticos, no es menos cierto que dicho tipo penal es claramente subordinado. ¿Cuál es la razón de la subordinación? La respuesta es sencilla, por la remisión expresa que hay del hurto por medios informáticos al tipo penal básico de hurto (en cuanto a la descripción típica) y al tipo penal de hurto calificado (en cuanto a la pena). Es y será siempre subordinado mientras que se mantenga la fórmula utilizada, debido a que, cualquier cambio en cuanto a la acción contemplada en el tipo básico de hurto, implica un cambio en la acción del hurto por medios informáticos. Asimismo, cualquier cambio en la pena del hurto calificado, implica un cambio en la pena del hurto por medios informáticos.

En palabras de nuestra Corte Suprema, “se trata de un tipo penal de naturaleza claramente subordinada y compuesta. En efecto, la descripción normativa, en su tipo objetivo positivo y en la consecuencia jurídica, no consagra la conducta reprochada, el objeto material, ni la sanción correspondiente, sino que, en cuanto se refiere al comportamiento antijurídico y al referido objeto sobre el que recae la acción prohibida, efectúa un reenvío normativo al tipo base de hurto (L. 599/2000, art. 239) y a la disposición que lo califica (canon 240 *ejusdem*) para determinar la sanción imponible” (CSJ-SP/11-02-2015).

3.3.2. El hurto por medios informáticos es un tipo penal de medios determinados

Pocos son los tipos penales frente a los cuales se puede afirmar, sin lugar a dudas, que son de medios concretos o determinados. Sin embargo, el tipo penal objeto de estudio es uno de los ejemplos más claros de esa clase de conductas. Es un tipo penal de medios determinados porque para su estructuración el hurto debe ser cometido a través de uno cualquiera de los siguientes medios: i) manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante; o ii) suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos. En cualquiera de los dos casos, superando las medidas de seguridad existentes.

Entonces, sólo a través de estos medios se puede cometer el hurto por medios informáticos. ¿Qué sucede si una persona se apodera de un bien mueble ajeno a través de un medio distinto? Responderá por el tipo penal de hurto, bien sea en la modalidad simple, calificada o agravada según el caso en concreto.

3.3.3. El hurto por medios informáticos no es un delito informático

Al inicio de este trabajo señalamos que existe una tendencia en la Doctrina consistente en afirmar que toda conducta punible que tenga una conexión, mediata o inmediata, con las tecnologías de la información, es un delito informático. Así, la gran mayoría de los autores especializados en el tema señalan que los delitos cometidos a través de sistemas informáticos son delitos informáticos, o en su defecto, cibercrimenes, según el concepto que se adopte. Pues bien, el hurto no ha sido lejano a este fenómeno, y por ello, muchos afirman que el hurto por medios informáticos es un delito informático^{xcvii}.

En contra de esta postura, hemos señalado que sólo son delitos informáticos aquellos atentados en contra de los sistemas informáticos y de la información contenida en esos sistemas. Se trata pues de un concepto restringido o limitado de delito informático. Y es que no podría ser de otra forma, pues si se habla de delito **informático**, resulta claro que el acento se pone en el término **información**. Es esa **información**, y los sistemas encargados de su procesamiento automático, lo que se pretende proteger mediante los delitos **informáticos**^{xcviii}.

Hacemos este recuento no para ahondar en el tema, pues consideramos que la discusión ya se surtió de forma detallada en la primera parte de este trabajo, sino para significar que un delito que no afecte los datos o los sistemas informáticos no puede ser llamado un delito informático. Se tratará simplemente de delitos “comunes u ordinarios” cometidos a través de medios novedosos. Precisamente esto es lo que sucede con el hurto por medios informáticos, debido a que, como quedó claro en el capítulo anterior, su objeto jurídico de protección no es otro diferente al patrimonio económico. Y por ende, ha de catalogársele como un delito “patrimonial” y no como uno “informático”.

4. Problemas derivados de la tipificación autónoma del hurto por medios informáticos. Proposición de solución a esos problemas

Veníamos sosteniendo cómo en efecto no compartimos la tipificación autónoma del delito de hurto por medios informáticos, pues consideramos que si bien es necesario avanzar en la adecuación del derecho penal, a las nuevas formas de criminalidad, y dentro de ellas al espectro de la informática; lo cierto es que esta tesis expansionista -hacemos referencia a

la creación de tipos penales autónomos-, solo puede ser aplicada cuando los tipos penales comunes, clásicos u ordinarios, no son suficientes para castigar problemáticas sociales, que afectan bienes jurídicos de especial importancia para los Estados.

Con antelación se había anticipado que, de la tipificación autónoma del hurto por medios informáticos, surgen varios problemas que constituyen obstáculos relevantes para la aplicación práctica del tipo penal en comento. A continuación se explicarán esas deficiencias.

4.1. Concurso aparente de tipos penales con la circunstancia de calificación del hurto. Art. 240, numeral 4 del Código Penal colombiano.

El numeral 4 del artículo 240 del Código Penal colombiano señala que el hurto será calificado cuando se cometa “con escalamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas **u otras semejantes**”. En este orden de ideas, si se cometiera un hurto superando las medidas de seguridad contempladas en un sistema informático, nada impediría que se tipificara el hurto calificado por la causal mencionada, como quiera que la expresión “**otras semejantes**”, puede abarcar formas de seguridad informática. Lo mismo podría señalarse del hurto por medios informáticos, pues sin duda, se estructurarían todos los elementos típicos de esta última conducta punible^{xcix}.

Para entender los conceptos, podemos acudir a las definiciones que la doctrina construye señalando que: “Son seguridades electrónicas aquellos mecanismo que de manera

automática funcionan ante la presencia de cualquier estímulo, como, por ejemplo, las alarmas”. (Suárez Sánchez, 2010, p. 247). Al punto que destaca igualmente que:

Ante los novedosos y avanzados sistemas de seguridad pueden ser consideradas semejantes a las electrónicas: las informáticas, las electromagnéticas, las elaboradas con fundamento en datos personales de identidad, como el análisis del iris del ojo, la huella dactilar, la identificación de voz humana, etcétera. (Suárez Sánchez, 2010, p. 250)

Entonces, se presenta un concurso aparente de tipos penales entre, por un lado, el hurto calificado por la cuarta causal (específicamente por la expresión lingüística “u otras semejantes”)^c, y por otro, el hurto por medios informáticos. Problemática surgida a raíz de la creación de esta última figura típica, pues, se creó un tipo penal autónomo, ubicado incluso en un título diferente, cuando lo que se debió crear fue una circunstancia de calificación específica que abarcara situaciones como las allí contenidas.

Ahora bien, siguiendo el principio general del derecho de acuerdo al cual, la ley especial prevalece sobre la ley general, resulta evidente que en casos como el señalado debe dársele aplicación al tipo penal de hurto por medios informáticos. Esto nos evita la problemática que representaba la extrema ambigüedad del término “u otras semejantes” utilizado en la circunstancia de calificación del hurto. Sin embargo, todavía subsisten falencias generadas por la tipificación autónoma del hurto por medios informáticos, tal y como ya lo mencionamos. Por lo que, refulge con claridad que la solución más adecuada, desde el punto de vista de la técnica legislativa, es la creación de una causal de hurto que lo califique cuando este se cometa por medios informáticos.

No deja de causar inquietud, el hecho que bajo esta estricta circunstancia, la calificación del hurto común se tornará inoperante, cuando se utilicen medios informáticos en su comisión, pues pasará siempre a considerarse como un hurto por medios informáticos por especialidad, es decir, además de la problemática del concurso aparente, existirá una innecesaria dualidad de tipos penales, que a la postre, redundará en una absoluta inseguridad jurídica, y con ella, la siempre posible arbitrariedad de los operadores judiciales.

4.2. Ubicación deficiente del tipo penal de hurto por medios informáticos

Aunque la ubicación dada a un tipo penal dentro de un capítulo específico del Código Penal no es circunstancia suficiente para afirmar que el bien jurídico protegido se corresponde con la nominación del capítulo, dicha ubicación si resulta ser un dato indiciario sobre cuál es el objeto de protección jurídica del tipo penal. Así, resulta problemático que el hurto por medios informáticos haya sido ubicado dentro de los delitos en contra de la información y los datos.

Tan problemática y deficiente es esa ubicación que, como se mencionó en el capítulo anterior, ya ha obligado a la Sala de Casación Penal de la Corte Suprema de Justicia a pronunciarse al respecto, afirmando que el bien jurídico protegido de forma primordial es el patrimonio económico, y no los datos o los sistemas informáticos allí contenidos. Lo anterior, con el fin de determinar si era viable la rebaja por reparación integral, contemplada en el artículo 269 del Código Penal, para los delitos que afectan el patrimonio económico. Es decir que, la discusión en Colombia, ya superó las barreras de lo

teórico y se posó también en la práctica judicial. Lo manifestado concretamente por la Corte Suprema de Justicia en sentencia del 11 de febrero de 2015 fue lo siguiente:

Ciertamente, aunque el legislador fue consciente de la dificultad que comportaba la ubicación del bien jurídico protegido respecto de aquellas acciones antijurídicas reguladas dentro del mentado título, que de manera directa afectaban el patrimonio económico, prefirió atar, de manera anti técnica, como lo aseveró el representante de la fiscalía, la modalidad de la acción típica prohibida —que es el hurto por medios informáticos— al bien jurídico amparado en el referido título VII bis, que adicionar o modificar las circunstancias modales calificantes del artículo 240 del Código Penal, como hubiera sido lo ideal.

De lo hasta aquí dicho, es posible decantar, con meridiana claridad, que pese a la ubicación sistemática del punible de hurto por medios informáticos y semejantes en el título VII bis del Código Penal, rubricado bajo la denominación de la información y los datos, este bien jurídico resulta ser, para el caso concreto — como lo concibió la exposición de motivos del Proyecto de Ley 42 Cámara—, de naturaleza meramente intermedia, pues el interés superior protegido de manera directa es el patrimonio económico, entendido como ese conjunto de derechos y obligaciones, susceptible de ser valorado en términos económicos, más concretamente, en dinero.

Simplemente con la ubicación adecuada del tipo penal de hurto por medios informáticos (patrimonio económico, más no la información y los datos) se hubiese evitado esa

discusión que, repetimos, ha tenido efectos importantes en la aplicación práctica de estos tipos penales.

Lo más relevante en este punto, es que la propia Corte Suprema de Justicia, tuvo que acudir a un esforzado análisis que en estricto sentido tiene una lógica conclusión, pero que bajo la interpretación derivada de la ubicación del ilícito, debía necesariamente arribar a una consecuencia distinta. Es decir, la alta corporación, reconoció en un delito de hurto por medios informáticos, cuyo bien jurídico es la protección de la información y los datos, que se aplicara un mecanismo de rebaja punitiva postdelictual, propio de los delitos contra el patrimonio económico, arguyendo para ello, la preponderancia de protección del ilícito, no en el marco de la información y los datos, sino del patrimonio económico.

Así las cosas, se concluyó lo que en efecto corresponde, esto es, que el delito de hurto por medios informáticos en verdad es un delito de contenido netamente patrimonial, y que por ende es procedente aplicar la rebaja por la indemnización de los daños causados con el mismo, lo que desborda el escenario de protección de la información y de los datos y lo sitúa en cambio en los ilícitos contra el patrimonio económico.

4.3. Diferenciación en la competencia de tipos penales idénticos

Un último problema derivado de la tipificación autónoma del hurto por medios informáticos, consiste en que, se ha otorgado competencia a Jueces de diferentes categorías, para eventos que son en extremo similares. Específicamente, esa diferenciación se ha dado entre el hurto con cuantía superior a ciento cincuenta (150)

salarios mínimos mensuales legales vigentes, y el hurto por medios informáticos con cuantía similar.

En el primero de los eventos, la competencia la tendrán los Jueces Penales del Circuito. Toda vez que así lo disponen los artículos 36 y siguientes del Código de Procedimiento Penal colombiano. Y en el segundo, es decir en el hurto por medios informáticos (sin importar la cuantía) la competencia será de los Jueces Penales Municipales, tal y como lo preceptúa el numeral 6 del artículo 37 del Estatuto Procesal Penal. Vale la pena destacar que el numeral 6 del artículo 37, fue introducido por la ley 1273 de 2009. Esto es, la misma que tipificó el hurto por medios informáticos.

Entonces, ¿cuál es la falencia que se presenta en este caso? Simple, que a tipos penales semejantes, cuya única diferencia es un medio determinado de comisión del delito, se les ha dado una asignación de competencia judicial diferente. Si se asume que la competencia se atribuye a partir de la gravedad de los delitos, resulta un contrasentido señalar que los Jueces Penales del Circuito conocen del hurto de cuantía superior, mientras que del hurto por medios informáticos, aun cuando tenga una cuantía semejante, además de especificaciones típicas, y técnicas de mayor complejidad, conocerán los Jueces Penales Municipales, máxime cuando se ha reconocido que en los dos eventos, el bien jurídico tutelado es el mismo. Y es un contrasentido puesto que, se terminaría afirmando que el hurto por medios informáticos reviste una menor gravedad que el tipo básico de hurto, lo que por su especialidad, tecnicismo, y forma de criminalidad, resulta una notable contradicción.

4.4. Incoherencia y falta absoluta de razones de política criminal

Si bien la esencia de las modificaciones legislativas en materia penal, parten del presupuesto de un análisis previo de razones de política criminal, lo cierto es que la experiencia en el campo colombiano, y en general latinoamericano, nos ha enseñado que dicho criterio además de tornarse inexistente en la adopción de medidas jurídico penales, es reemplazado por el renaciente y cada vez más utilizado concepto de populismo punitivo.

La ley 1273 del año 2009, no fue ajena a este fenómeno. Basta con acudir al proyecto de ley^{ci} para evidencia como la exposición de motivos está basada en expresiones populistas como afirmar que el proyecto pretende que “el ordenamiento penal colombiano se sume a las políticas penales globalizadas en materia del combate frontal contra la llamada criminalidad del ciberespacio y le brinde herramientas a la comunidad internacional para la persecución de estos flagelos; al mismo tiempo, se busca brindar una adecuada tutela jurídica a un bien jurídico de tanta trascendencia en el mundo de hoy como lo es el atinente a la Protección de la Información y de los Datos”.

Adicionalmente ofrecer el proyecto como un llamado a “modernizar la legislación penal colombiana y a ponerla a la par de la de otros países, como los que integran la comunidad económica europea”, es indudablemente un mercadeo del proyecto, como un avance a la modernización legislativa.

Lo cierto es que ya desde las discusiones iniciales^{cii}, el congresista Parmenio Cuellar, solicitó a la comisión, archivar el proyecto. Basta con revisar los motivos de su ponencia,

para concluir sin mayor asomo de duda, lo que es evidente: a. Que el proyecto es absolutamente populista, y que no obedece a estudios serios y fundados en la materia, buscando una sobre creación caprichosa de tipos penales; y b. Que las conductas allí descritas como novedosas, y concretamente el hurto por medios informáticos, ya está plenamente abarcado con la existencia de la circunstancia calificante del hurto que hemos reiterado en el presente trabajo. Así las cosas, ni siquiera en el marco de una justificación político-criminal, la tipificación autónoma del delito adquiere importancia y relevancia que permita acreditar la consagración autónoma del delito.

CAPÍTULO IV: PROPUESTA PARA SUPERAR ESTAS FALENCIAS

Una vez expuestas las problemáticas derivadas de la consagración autónoma del delito de hurto por medios informáticos, y de la develada duplicidad de conductas punibles, así como la indebida ubicación del tipo penal, en el marco de un bien jurídico tutelado ajeno al objeto de protección de los delitos informáticos, no podemos dejar de abordar la problemática, ofreciendo una propuesta que permita superar las falencias que ofrece la creación, elementos, ubicación, filosofía y en general el delito atrás estudiado.

Es imposible evadir la discusión referida a la necesidad de reprochar penalmente las conductas delictivas que supongan apoderamiento de bienes ajenos, utilizando mecanismos informáticos y telemáticos. Es a su turno un absurdo, negar que el reconocimiento de esta problemática social merece un adecuado, proporcional y estricto reproche penal.

Ya referíamos en el presente estudio, las consecuencias, y paralelamente las bondades que la utilización de este tipo de instrumentos para la comisión de conductas punibles, ofrecen a la criminalidad. No obstante ello, lo cierto es que la necesidad del reproche penal, la gravedad de estas conductas y su necesaria consideración como objetivo de las naciones en materia de lucha y prevención, no pueden ir en contravía de los mas elementales principios del derecho penal, y del establecimiento adecuado y fundamentado del mecanismo que permita hacer frente a esta nueva forma de criminalidad.

De esta forma, identificadas las falencias, pero a su turno reconocida la necesidad de reproche penal, no nos resta más que reestructurar la conducta delictiva, suprimir la duplicidad de tipos penales, reubicar el tipo penal y reformular la consagración del ilícito.

Por simplista que pueda parecer, consideramos que la solución a los problemas resaltados a lo largo de este trabajo, podría darse en dos sencillos pasos: i) la eliminación de la figura autónoma del hurto por medios informáticos^{ciii}; y ii) la creación de una circunstancia de calificación del hurto cuando se cometa a través de sistemas informáticos. Entonces, debería añadirse un numeral 5 al artículo 240 del Código Penal colombiano, que señale que el hurto será calificado cuando el apoderamiento se cometa:

“manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos”.

Siendo coherentes con lo expuesto en este trabajo, el tipo penal, y concretamente la propuesta de calificación del hurto, encuentra justificación en los siguientes puntos:

1. Acogemos el concepto de delito informático en sentido estricto. Es decir, consideramos que los delitos informáticos son solo aquellos que en verdad tienen la potencialidad de afectar el bien jurídico de la protección de la información y de los datos.
2. Reconocemos la necesaria creación de un bien jurídico autónomo, que proteja la información y los datos, así como la preocupación de los estados, por hacer frente a esta nueva forma de criminalidad.

3. Identificamos el hurto informático como una conducta socialmente reprochada, con relevancia social, y merecedora de un verdadero castigo en ejercicio del ius puniendi del Estado.

4. Consideramos que de conformidad con la estructura del delito, la naturaleza del mismo, y su objeto de protección, se trata de un delito que preponderantemente protege el patrimonio económico.

5. De esta forma, la solución adecuada, plasmada en este trabajo, es la eliminación del tipo penal autónomo, la consecuente creación de una circunstancia de calificación que incluya este reproche, y la ubicación necesaria de esta conducta en la estructura del hurto común, con lo que ello supone, particularmente la protección del bien jurídico patrimonio económico.

A modo de conclusión parcial, a través de la consagración de esta circunstancia de calificación del hurto se superará el problema del concurso aparente de tipos penales, la deficiencia en la ubicación sistemática del tipo penal, la ausencia de criterios político criminales que la justifiquen y la odiosa discriminación en la asignación de competencia judicial.

CONCLUSIONES

- I. Los conceptos de cibercrimen y delito informático en sentido amplio, son excesivamente ambiguos, pues en ellos se incluye cualquier delito que haya sido cometido en relación con la informática.

Para mayor ilustración piénsese en el siguiente ejemplo: un hacker entra al sistema informático de un hospital y accede a las historias clínicas de los pacientes. Una vez ha accedido a las historias clínicas, el criminal modifica la información sobre la alergia a la penicilina que tenía un paciente, de tal modo que, en la historia clínica del paciente ya no aparece dicha alerta. Días después una enfermera, ignorando la alergia que presentaba el paciente, le aplicó penicilina por considerar que se trataba del tratamiento adecuado para la infección que sufría el paciente.

Entonces, si acogiéramos el concepto de cibercrimen o el de delito informático en sentido amplio, tendríamos que concluir que en ese caso se presentó un delito informático, concretamente una suerte de homicidio informático inducido. Lo que resulta absolutamente inconveniente si se tiene en cuenta que, en ese caso, no hay un elemento informático que sea objeto de protección. Sino simplemente un nuevo medio (informático) para la comisión de un “viejo delito”.

En cambio, al acoger el concepto de delito informático en sentido estricto, hacemos referencia al delito que afecta los sistemas informáticos y/o los datos contenidos en esos sistemas informáticos. Es decir, sólo en este caso existe una

relación entre lo “informático” y el objeto de protección de los delitos informáticos. Es allí entonces donde verdaderamente surge el delito informático.

- II. El fundamento de la punición de los delitos informáticos se remonta a la importancia que ostentan en la actualidad las redes informáticas y telemáticas. En efecto, en las comunidades modernas resulta inconcebible el funcionamiento cabal de la sociedad sin los sistemas informáticos, y es esa preponderancia innegable que representan las redes telemáticas, como el internet, lo que nos lleva a afirmar que deben ser objeto de protección por parte del derecho penal mediante la institución de los delitos informáticos. Puesto que si el derecho penal no está para proteger aquellos valores fundamentales que permiten el funcionamiento de la sociedad como la conocemos, entonces ¿para qué está?

Ahora bien, el bien jurídico protegido por los delitos informáticos no es otro diferente a la integridad, confidencialidad y disponibilidad de los datos y los sistemas informáticos. No debe entonces pensarse que estos delitos buscan exclusivamente proteger el patrimonio económico o la indemnidad sexual de los menores (afectada por la pornografía infantil), sino que su objeto jurídico radica en la protección de la información automatizada y en los sistemas que permiten el tratamiento de esa información. Esto no excluye el hecho de que los delitos informáticos sirven de “barrera de contención” que impiden la afectación de otros bienes jurídicos como los ya señalados.

No obstante ello, no deben confundirse bajo ninguna circunstancia los delitos informáticos con la criminalidad a través de medios informáticos, como quedara plenamente diferenciado en este trabajo.

- III. Los principales atentados en contra de los sistemas informáticos y los datos allí contenidos son el hacking y el sabotaje informático. El hacking es entendido como el acceso abusivo a un sistema informático sin finalidad distinta a la mera intrusión. Por su parte, el sabotaje informático consiste en la utilización de virus, o cualquier elemento semejante, con el fin de inutilizar, destruir u obstaculizar el funcionamiento de un sistema informático, así como en sustraer, modificar o eliminar la información contenida en el sistema informático.
- IV. Frente al delincuente informático debe advertirse la necesidad de replantear aquella concepción clásica de que solo individuos intelectualmente superiores que tienen profundísimos conocimientos en informática pueden ser criminales informáticos. Dado que, en la actualidad, cualquier persona puede convertirse en un hacker o cracker tan sólo con acudir a uno de los miles de programas disponibles en la web que permiten acceder a sistemas informáticos ajenos, inclusive, la propia forma de crianza y el innegable acceso a la tecnología desde remotas y tempranas edades, desarrolla en la sociedad, una especial facilidad y destreza en el manejo de instrumentos que son medios para la criminalidad informática. En resumen, basta con que, cualquier persona con conocimientos básicos en informática, haga uso de uno de esos “software” para convertirse en un auténtico delincuente informático.

- V. El hurto por medios informáticos no es un delito informático. Simplemente, se trata de un delito clásico (“viejo delito”) cometido por un medio novedoso, en este caso, la informática. Por ende, el bien jurídico protegido por este delito no son los datos o los sistemas informáticos, sino el patrimonio económico. Vale la pena citar una frase simple de Suarez (2010) que concluye que “se trata de una forma especial de hurto que remite a la estructura del tipo básico del hurto” (p. 249).
- VI. La tipificación autónoma del hurto por medios informáticos resulta absolutamente deficiente, puesto que: i) podría llevar al intérprete a pensar que el bien jurídico protegido es el de la informática, lo que a su vez podría producir (como en efecto ya sucedió) problemas en la aplicación de las rebajas propias de los delitos patrimoniales; ii) genera un concurso aparente de tipos penales con la causal de calificación del hurto contemplada en el artículo 240.4, en cuanto esta señala que se calificara el hurto cuando se cometa “superando medidas de seguridad electrónica **u otras semejantes**”; iii) esta tipificación autónoma produce una diferenciación en la competencia de los jueces que conocerán de la comisión de tipos penales idénticos. Así, por un lado, el hurto de cuantía superior a 150 salarios mínimos lo conocerá el Juez Penal del Circuito, y por otro, el hurto por medios informáticos de idéntica cuantía lo conocerá el Juez Penal Municipal.
- VII. No existen razones de política criminal, que permitan justificar la creación e inclusión del delito de hurto por medios informáticos como conducta autónoma, pues no es más que una manifestación adicional del conocido populismo punitivo, con deficiencias y falencias de especial gravedad, que resultan creando mayores

problemas que soluciones a la problemática de la apropiación de bienes por medios informáticos.

VIII. La propuesta para superar estas falencias radica en dos puntos. En primer lugar, la eliminación del tipo penal autónomo de hurto por medios informáticos, y, en segundo lugar, la creación de una causal de calificación del hurto referida a la comisión por medios informáticos.

Con ello se superarían las falencias originadas en la ubicación deficiente del tipo penal, el concurso aparente de tipos penales y la discordancia en la competencia judicial de tipos penales que, en teoría, revisten la misma gravedad.

BIBLIOGRAFÍA

1. Aboso, G; Zapata, M. (2006). *Cibercriminalidad y Derecho Penal*. Buenos Aires: B de F.
2. Alastuey, M. (1994). *Apuntes sobre la perspectiva criminológica sobre la delincuencia informática patrimonial*. En Carrascosa, V. *Informática y Derecho* 4. Merida: Aranzadi.
3. Álvarez Cabrera, C. (2003). *Aspectos penales relativos al uso de honeypots*. Revista internacional derecho penal contemporáneo. Número 5.
4. Álvarez Cabrera, C. (2005). *El arte de la computación forense*. Revista internacional derecho penal contemporáneo. Número 10. Pp. 19-42.
5. Alvarez-Cienfuegos, J. (1996). *Informática y derecho penal. Los delitos relativos a la informática*. Cataluña: Centro de Estudios Jurídicos y Formación Especializada de Cataluña.
6. Anarte, E. (2001). *Sobre los límites de la protección penal a los datos personales*. Derecho y conocimiento, vol. 2, pp. 225-254. Facultad de Derecho. Universidad de Huelva.
7. Anarte, E. (2001-A). *Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la información*. Derecho y conocimiento, vol. 1, pp. 191-257. Facultad de Derecho. Universidad de Huelva.
8. Araujo, J. (1994). *Computer Crimes and Other Crimes against Information Technology in Brazil*. En Sieber, U. (ed) (1994). *Information Technology crime*. Köln; Berlin; Bonn; Munchen: Heymman.

9. Arzuaga Herrada, T; Guevara Medina, L. (2013). *La ley 1273 de 2009 y los delitos informáticos en Santiago de Cali*. Universidad de San Buenaventura.
10. Balmaceda, G. (2009). *El delito de estafa informática*. Santiago: Editorial Jurídica de Santiago.
11. Balmaceda, G. (2014). *Manual de derecho penal. Parte general*. Santiago: Librotecnia.
12. Blanco, I. (2012). *El delito de blanqueo de capitales*. Navarra: Thomson Reuter Aranzadi.
13. Camacho, L. (1987). *El delito informático*. Madrid: editorial desconocida.
14. Choclán, J. (2002). *Infracciones patrimoniales en los procesos de transferencia de datos*. En Morales, O, (Dir). (2002). *Delincuencia informática. Problemas de responsabilidad*. Madrid: Consejo General del Poder Judicial.
15. Davara, M. (2005). *Manual de derecho informático. Séptima edición*. Navarra: Thomson-Aranzadi.
16. Davara, M. (2005). *Manual de derecho informático. Novena edición*. Navarra: Thomson-Aranzadi.
17. Díaz, L. (2003). *El nuevo delito de “contacto TIC preordenado a la actividad sexual con menores” en España*. Revista internacional derecho penal contemporáneo. Número 38. Pp. 5 – 44.
18. Fernández, G. (2001). *Ciberdelincuencia patrimonial e internet. Propiedad intelectual y tarjetas prepago*. En Ministerio Fiscal. *Estudios jurídicos III-2003*. Madrid.

19. Fernández, J. (2007). *Ciberdelincuencia los delitos cometidos a través de internet*. Asturias: Ojanguen.
20. Flores, I. (2012). *Criminalidad informática. Aspectos sustantivos y procesales*. Valencia: Tirant Lo Blanch.
21. Gallardo, A. (1998). *Delincuencia informática: la nueva criminalidad de fin de siglo*. Cuadernos de política criminal, vol. 65, pp: 365-374.
22. Guerrero M., M. (2004). *La ciberdelincuencia*. Bogotá: Instituto de estudios del ministerio público.
23. Gómez, M. (1994). *Los delitos informáticos en el derecho español*. En Carrascosa, V. *Informática y Derecho 4*. Merida: Aranzadi.
24. Gómez Tomillo, M. (2004). *Responsabilidad penal y civil por los delitos cometidos a través de internet*. Navarra: Thomson-Aranzadi.
25. González Rus, J. (2003). *El cracking y otros supuestos de sabotaje informático*. En Ministerio Fiscal. *Estudios jurídicos II-2003*. Madrid.
26. Grisales, G. (2014). *Hurto por medios informáticos y transferencia no consentida de activos en Colombia*. Revista internacional derecho penal contemporáneo. Número 48. Pp. 121-189.
27. Gutierrez, M. (1996). *El intrusismo informático (Hacking): ¿Represión Penal Autónoma?* En *Informática y Derecho 12-13-14-15*. Merida: Aranzadi.
28. Gutierrez, M. (2005). *Reflexiones sobre la ciberdelincuencia hoy (en torno a la ley penal en el espacio virtual)*. Revista electrónica de derecho de la Universidad de Rioja (REDUR). Número 3. Pp: 69-92.

29. Herrera, R; Nuñez, A. (1999). *Derecho informático*. Santiago de Chile: Ediciones Jurídicas La Ley.
30. Hernández Basualto, H. (2001). *Tratamiento de la criminalidad informática en el derecho penal chileno*. Informe solicitado por la División Jurídica del Ministerio de Justicia en el marco de un Convenio suscrito entre esa Secretaría de Estado y la Facultad de Derecho de la Universidad Andrés Bello
31. Huerta, M; Libano, C. (1998). *Delitos informáticos*. Santiago de Chile: Editorial Jurídica Conosur Ltda.
32. Jijena, R. (1992). *Chile, la protección penal de la intimidad y el delito informático*. Santiago de Chile: Editorial Jurídica de Chile.
33. Laso, D. (2002). *Intimidad y protección de datos en derecho penal*. En Morales, O, (Dir). (2002). *Delincuencia informática. Problemas de responsabilidad*. Madrid: Consejo General del Poder Judicial.
34. Lanzos, A. (2003). *Los ilícitos penales cometidos a través de internet*. En Revista Actualidad Penal. Número 15. Pp: 399-413.
35. Manjarrés, I; Jiménez, F. (2012). *Caracterización de los delitos informáticos en Colombia. Pensamiento Americano*.
36. Martin, J. (2001). *La confidencialidad de los datos clínicos en las redes informáticas*. En Lopez, J, (Dir). (2001). *Internet y derecho penal*. Madrid: Consejo General del Poder Judicial.
37. Mata y Martin, R. (2001). *Delincuencia informática y derecho penal*. Madrid: Edisofer S.L.

38. Mata y Martin, R. (2003). *Criminalidad informática: una introducción al cibercrimen*. Revista Actualidad Jurídica. Número 37. Pp. 935-961.
39. Matellanes, N. (2000). *Algunas notas sobre las formas de delincuencia informática en el código penal*. En Diego, M; Sánchez, V (Coordinadoras). *Hacia un derecho penal sin fronteras*. Madrid: Editorial Colex.
40. Maza, J. (2001). *La intervención judicial de las comunicaciones a través de internet*. En Lopez, J, (Dir). (2001). *Internet y derecho penal*. Madrid: Consejo General del Poder Judicial.
41. Meek, M. (2013). *Delito informático y cadena de custodia*. Bogotá: Fondo de publicaciones Universidad Sergio Arboleda.
42. Miro, F. (2012). *El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.
43. Morales, O. (2002). *Apuntes de política criminal en el contexto " tecnológico. Una aproximación a la convención del Consejo de Europa sobre cyber-crime"*. En Morales, O, (Dir). (2002). *Delincuencia informática. Problemas de responsabilidad*. Madrid: Consejo General del Poder Judicial.
44. Morales Prats, F. (2001). *Internet: Riesgos para la intimidad*. En Lopez, J, (Dir). (2001). *Internet y derecho penal*. Madrid: Consejo General del Poder Judicial.
45. Morón Lerma, E. (2002). *Internet y derecho penal: «hacking» y otras conductas ilícitas en la red*. Navarra: Aranzadi.
46. Muñoz Conde, F. (2013). *Derecho Penal. Parte Especial. Edición 19*. Valencia: Tirant Lo Blanch.

47. Ojeda Pérez, J; Arias Flórez, M; Rincón Rodríguez, F; Martínez, L. (2010). *Delitos informáticos y entorno jurídico vigente en Colombia*.
48. Paladines, J. (2012) *La dogmática penal antidrogas en la sociedad del riesgo*. En: Boletín Semestral GLIPGo (Grupo Latinoamericano de Investigación Penal Gottingen).
49. Palazzi, P. (2000). *Delitos informáticos*. Buenos Aires: Ad-Hoc.
50. Pinochet, F. (2006). *El derecho de internet*. Santiago de Chile: Editorial de Derecho de Chile.
51. Piragoff, D. (1994). *Computer Crimes and Other Crimes against Information Technology in Canada*. En Sieber, U. (ed) (1994). *Information Technology crime*. Köln; Berlin; Bonn; Munchen: Heymman.
52. Posada, R. (2013). *El delito de acceso abusivo a sistema informático*. Revista internacional de derecho penal contemporáneo. Número 44. Pp. 97-142.
53. Prias, J. (2006). *Aproximación al estudio de los delitos informáticos*. Revista internacional de derecho penal contemporáneo. Número 17. Pp. 5-78.
54. Reporte Norton sobre Ciberdelitos (2013), elaborado por Symantec. Disponible en formato digital en: <https://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf>. Consultado el 26 de octubre de 2015.
55. Rey, A; Nuñez, C. (2011). *De los delitos informáticos. Ley 1276 de 2009*. En Castro, C. (Coord). (2011). *Manual de Derecho Penal. Parte Especial*. Bogotá: Editorial Temis y Editorial Universidad del Rosario.

56. Rodríguez Medina, E. (2004). *Las tecnologías de la información y las comunicaciones. Nuevos Roles y Escenarios en un Mundo Interconectado*. Bogotá: Ediciones ASUCOM.
57. Romeo Casabona, C. (2006). *De los delitos informáticos al cibercrimen*. En Romeo Casabona, C, (Coord). *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Granada: Editorial Comares.
58. Rueda Martin, M. (2009) *Cuestiones político-criminales sobre las conductas de hacking*. Revista internacional de derecho penal contemporáneo. Número 28. Pp. 151-194.
59. Rueda Martin, M. (2014). *La disponibilidad de la intimidad y la propia imagen del menor de edad en el ciberespacio: riesgos y límites*. Revista internacional de derecho penal contemporáneo. Número 46. Pp. 119-176.
60. Salvadori, I. (2013). *¿El delito de acceso abusivo a un sistema informático se puede aplicar también a los insider?* Revista internacional derecho penal contemporáneo. Número 43. Pp. 5-26.
61. Salvadori, I. (2014). Los delitos de daño en el Código Penal italiano. Revista internacional derecho penal contemporáneo. Número 47. Pp. 87-119.
62. Schick, P; Schmolzer, G. (1994). *Computer Crimes and Other Crimes against Information Technology in Austria*. En Sieber, U. (ed) (1994). *Information Technology crime*. Köln; Berlin; Bonn; Munchen: Heymman.
63. Sieber, U. (1992). *Criminalidad informática: peligro y prevención*. En Mir Puig, S. *Delincuencia informática*. Barcelona: PPU.

64. Sieber, U. (ed) (1994). *Information Technology crime*. Köln; Berlin; Bonn; Munchen: Heymman.
65. Sieber, U. (1998). *Computer Crime and Criminal Information Law*. Documento digital recuperado de: <http://www.jura.uni-muenchen.de/sieber/article/mitis/ComCriCrimInf.htm>.
66. Sieber, U. (2009). *El control de la complejidad en el ciberespacio global: la armonización de los delitos informáticos*. En Delmas-Marty, M; Pieth, M; Sieber, U (eds). (2009). *Los caminos de la armonización penal*. Valencia: Tirant Lo Blanch.
67. Solano, O. (1997). *Manual de informática jurídica*. Bogotá: Ediciones Jurídicas Gustavo Ibáñez.
68. Suárez Sanchez, A. (2010). *El hurto por medios informáticos y semejantes a través de la utilización de tarjeta magnética falsa o ajena en cajero automático*. En Gómez Gonzalez, C; Suárez López, C. (Coords). *Estudios de derecho penal*. Universidad de Bogotá Jorge Tadeo Lozano.
69. Tieddeman, K. (1985). *Poder económico y delitos*. Barcelona: Editorial Ariel S.A.
70. Tieddeman, K. (2000). *Derecho penal y nuevas formas de criminalidad*. Lima: Idemsa.
71. Ubeda, J. (2007). *La persecución de la pornografía infantil. Problemas relacionados con su distribución por Internet*. Revista La Ley Penal. Número 37. Pp. 67-80.
72. Velasquez, F. (2011). *Manual de derecho penal. Parte General. Cuarta edición*. Bogotá: Ediciones Jurídicas Andres Morales.
73. Vera, A. (1996). *Delito e informática*. Santiago de Chile: Ediciones Jurídicas La Ley.

JURISPRUDENCIA

1. Corte Suprema de Justicia, Sala de Casación Penal. Sentencia 42724 del 11 de febrero de 2015. M.P. Eyder Patiño Cabrera.

NOTAS AL MARGEN DE TEXTO

ⁱ La informática es definida como: “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.” Por su parte, la telemática es definida como: “Aplicación de las técnicas de la telecomunicación y de la informática a la transmisión a larga distancia de información computarizada” (RAE, 2012). Esto quiere decir que, la informática hace referencia a la forma como se tratan de forma automatizada los datos, la telemática hace referencia a cómo esos datos tratados de forma automatizada, pueden ser transmitidos a larga distancia. De aquí que, la red telemática por excelencia sea el internet.

ⁱⁱ El Ciberespacio es entendido como el “ámbito artificial creado por medios informáticos” (RAE, 2012). Entonces, cuando hacemos referencia a delitos con contenido cibernético, estamos hablando de los delitos cometidos a través o en contra de ese espacio artificial denominado Ciberespacio.

ⁱⁱⁱ Acogen el concepto de Cibercrimen, entre otros: Miró (2012); Fernández (2007); Romeo Casabona (2006); Mata y Martín (2003).

^{iv} En el acápite de “toma de postura” señalaremos las razones de esta afirmación.

^v Para un análisis detallado del fenómeno de la pornografía infantil, véase, por todos Díaz (2012).

^{vi} Rueda Martín (2014) afirma, respecto del riesgo que representa el intercambio de imágenes e información por parte de los menores, lo siguiente: “La posición de vulnerabilidad en la que se encuentran los menores de edad en contextos relacionados con las TIC se confirma también el estudio sobre hábitos seguros en el uso de *smartphones* por los niños y adolescentes españoles, realizado por Inteco en noviembre de 2011, donde se pone de manifiesto que los menores de edad entre 15 y 16 años sienten preferencia por compartir datos privados en prácticas como el intercambio de fotografías (71%), videos (39%), datos personales que incluyen nombre, dirección o edad (35%) o información sobre sus planes de tiempo libre (34,3%). Esta preferencia expone a los menores de edad a un mayor riesgo de sufrir ataques.” (P. 122)

^{vii} Por ejemplo, Fernández (2001) afirma que: “Podemos definir el delito informático como «la acción u omisión que siendo penalmente relevante, es llevada a cabo utilizando **medios o elementos informáticos** o recae sobre elementos informáticos ajenos»” (p. 470); Similar, Gómez (1994) quien afirma: “Así, con criterio ecléctico y amplio podemos conceptualizarla como el conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto -doble vertiente que después examinaremos- a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos. O centrándonos más en el aspecto patrimonial: el conjunto de acciones dolosas que provoca un perjuicio a personas físicas o entidades, sin que sea necesario que ello conlleve un beneficio material para su autor, o viceversa, produce un beneficio ilícito para su autor aun cuando no perjudique de forma ostensible a la víctima.” (p. 482)

^{viii} En Austria, Schick y Schmölzer (1994) adoptan este concepto cuando señalan: When looking at the “Austrian” definition of “computer crime” it can be seen that it follows for the most part the definition given by the German business consultant von zur Mühlen: “**Computer crime is every criminal act in which a computer is the instrument or target of the act**”. (p. 23); En Alemania, acoge el concepto en mención Tiedemann (1985) quien afirma: “Con la expresión «criminalidad mediante computadoras» se alude a **todos los actos, antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos**. Por una parte, dicho concepto abarca pues el problema de la amenaza a la esfera privada del ciudadano mediante la acumulación, archivo, asociación y divulgación de datos obtenidos por computadoras; de hecho, sin embargo, hasta el momento en Alemania Federal sólo se han conocido pocos casos en que se violaran derechos personalísimos aprovechando abusivamente datos conservados en una computadora. De cualquier forma, el legislador alemán reglamentó en general esa cuestión, denominada equivocamente de «protección de datos», con la «Ley federal de protección de datos», de 27 de enero de 1977, y en concordancia con modelos extranjeros, aunque la reforzó con normas penales poco precisas. Y, por otra parte, el concepto aludido se refiere a los daños patrimoniales producidos por el abuso de datos procesados automáticamente; las consideraciones siguientes se circunscriben pues a este segundo ámbito.” (p. 122)

^{ix} Así, Álvarez-Cienfuegos (1994) agrupa dentro del concepto de delito informático las siguientes conductas: “Para una mayor facilidad expositiva de este capítulo distinguiremos una serie de supuestos, sin ánimo de agotar las posibles hipótesis delictivas: a) Delitos informáticos contra la persona y los bienes y derechos de la personalidad: Intimidación personal y familiar. b) delitos informáticos contra la seguridad jurídica: La falsificación de documentos electrónicos. c)

Delitos informáticos contra la propiedad: la estafa, el hurto y la apropiación indebida. Fraudes informáticos. d) Protección penal de la propiedad del software. e) Delitos informáticos contra la persona y los bienes de la personalidad: intimidad personal y familiar.” (p. 199)

^x No obstante que acoge este concepto, Camacho (1987) parece ligar los delitos informáticos al bien jurídico patrimonio económico, cuando asevera: “En una primera aproximación podríamos definir el delito informático como toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas.” (p. 26)

^{xi} En este sentido, Vera (1996) afirma: De todo lo expuesto, se hace importante recalcar que **no es exacto hablar de "delito informático"**, pues como se puede ver en esta somera exposición, parece bastante dudosa la existencia de la especificidad que se ha pretendido encontrar en algunas conductas. Por eso es que, frente a todo lo expuesto, consideramos que la mejor forma de efectuar un análisis de los hechos delictivos en que toma participación los medios informáticos, **es tomando en consideración el bien jurídico que puede ser transgredido con tales conductas, que, como ya se ha reiterado, puede ser del tipo más variado**. En nuestro estudio nos limitaremos a tratar la protección del "patrimonio", a la "intimidad" y por último, nos abocaremos a analizar la Ley 19.223 que tipifica figuras penales relativas a la informática. Se analizará la protección del patrimonio y de la intimidad, en el Capítulo Tercero y Cuarto respectivamente, por ser los Bienes Jurídicos más vulnerables frente a la utilización de esta nueva tecnología.” (p. 102-103)

^{xii} Haciendo referencia a las causas de la agrupación de delitos informáticos, sin importar cuál sea verdaderamente el bien jurídico protegido, Anarte (2001-A) apunta: “Los inconvenientes de semejantes conceptos, que en definitiva no ofrecen ninguna especificidad, habían sido ya advertidos por la doctrina, que se esforzó en proporcionar, respecto del de delincuencia informática, algún criterio restrictivo, como el hecho de que la conducta se llevara a cabo operando sobre la base de las funciones propias de los ordenadores, a saber, el procesamiento y transmisión automatizados de datos y la confección y/o utilización de programas para tales fines. Por lo demás, parece claro que aquellas opciones conceptuales homogeneizadoras son igualmente disfuncionales desde una perspectiva político-criminal regida por el principio de proporcionalidad. En efecto, si, por una parte, la respuesta penal debe acomodarse a la gravedad de los hechos y si, por otra, aunque haya casos de delincuencia informática (o más específicamente la cibernética) que comparados con otros hechos delictivos similares comportan una lesividad mayor y es más difícil combatirlos, resulta igualmente evidente que esto no se puede predicar de toda la delincuencia informática, entonces, es erróneo destinar indiscriminadamente en el ámbito de la delincuencia informática recursos político-criminales cualificados con fundamento y finalidades específicos. Por otra parte, ante estos inconvenientes conceptuales, han acabado imponiéndose -sobre todo en el ámbito jurídico-penal-, **en lugar de definiciones** o descripciones de la delincuencia informática, **listados** más o menos completos y sistematizados (por ejemplo, según el bien jurídico protegido, el medio de ataque o combinando ambos aspectos) de delitos informáticos o cibernéticos” (p. 199)

^{xiii} Idéntica acepción de delitos informáticos es la acogida por Palazzi (2000): “De allí que estamos frente a un **delito informático en el caso del daño a datos o programas informáticos**, pero no cuando lo atacado es una simple máquina, y como consecuencia de ello se daña la información que ésta contenía. Hay que resaltar, como afirman algunos autores, que las situaciones delictuosas en las que los materiales informáticos no tienen la función más que de un simple objeto no se configura un delito informático. En efecto, dice Jijena Leiva —refiriéndose específicamente al bien “información”—, que al tipificarse un delito informático, lo que se está buscando es tutelar el contenido de información de un sistema informático, y no el hardware en sí mismo. Podremos también hablar de delito informático en el caso de reproducción ilícita de obras de software, de bases de datos o de topografías de semiconductores. Por último encontramos la situación en que se dan ambos supuestos, es decir el ordenador se usa como instrumento y es a la vez el objeto sobre el cual recae la acción delictiva. El caso más elocuente es la destrucción de datos mediante un programa o un virus informático” (p. 36); Adoptan también esta postura Herrera y Nuñez (1999) quienes afirman: En primer lugar, ciertas figuras típicas convencionales han comenzado a realizarse mediante el empleo de las tecnologías de la información, es decir, la informática ha sido utilizada como un medio de comisión específico. Dichas conductas pueden ser comprendidas dentro del tipo penal de delitos que ya están tratados en los Códigos Penales, produciéndose la informatización de un ilícito tradicional, al que llamaremos “delito computacional” para distinguirlo de los “delitos informáticos”. Los delitos computacionales al ser ilícitos que ya están tratados en el Código del ramo, no hacen necesaria la creación de nuevos delitos, y en el caso que no se ajusten completamente a la conducta descrita, bastaría con ampliar el tipo penal para actualizarlo. Pero además han surgido nuevas conductas, impensadas por el legislador de hasta hace medio siglo, que por su especial naturaleza no admiten encuadrarse dentro de figuras convencionales informatizadas sino que es necesario que se creen nuevos delitos. Son estos nuevos delitos a los que con propiedad llamamos delitos informáticos (...) Por lo tanto, una primera conclusión que nos llevará a un concepto de delito informático apropiado es excluir de la definición a los delitos computacionales. Ahora bien, teniendo claro que buscamos conceptualizar a conductas ilícitas nuevas, cometidas a través de equipos computacionales, pero en donde el elemento central no es el medio de comisión sino que **el hecho de atentar contra un bien informático**, debemos distinguir que no todos los bienes informáticos son objeto de estos delitos. (p. 213-216)

^{xiv} A favor de esta postura, Sieber (1994), quien afirma: The historical and empirical background of the newly emerging "criminal information law" - the development of information technology crime - only dates back to the 1960s, when first cases of so-called **"computer crime" appeared in the public press and in scientific literature. These cases included primarily computer manipulations, computer sabotage, computer espionage and illegal abuse of computer systems.** The public and scientific view of computer crime radically changed in the 1980s. A broad wave of program piracy, cash dispenser manipulations, and telecommunication abuses revealed to a broader public the vulnerability of an information society and the need for a new strategy of DP-security and crime control. Furthermore, it appeared that "computer crime" or "information technology crime" was no longer limited to economic crime, but included attacks against all kinds of interests, such as the manipulation of a hospital **computer or computer-related infringements of privacy**, which originally were discussed separately from "computer crime". (p. 5-6); En similar sentido, en Brasil, Araujo (1994) cuando señala: Fundamentalmente, "computer crimes" constitute harmful and fraudulent conducts which do not necessarily have in view the obtention of an illicit advantage. Nevertheless, these conducts must always be practised by means of the use of mechanisms regularly employed in the information activity. Obviously, this concept does not include conducts constituting traditional crimes, such as robberies of hardware, whose material object is a computer and its components. So, if someone steals a personal computer intending to sell it to obtain money to cover his expenses, he will be committing an ordinary robbery, and not a computer crime. (p. 69)

^{xv} Jijena (1992) distingue entre **delitos computacionales** y **delitos informáticos**. Al hablar de éstos últimos acoge el concepto limitado de delitos informáticos: "Utilizamos la primera denominación (delitos computacionales) para aludir a todas aquellas hipótesis delictivas que admiten ser encuadradas dentro de los tipos tradicionales, ya que en ellas los medios informáticos **sólo han sido una específica herramienta** de comisión. **Los delitos informáticos propiamente tales** requieren una configuración distinta, en consideración a las particularidades que ellos envuelven. En esta especie quedarían comprendidas las conductas del denominado hacker, el virus y los bombazos lógicos, entre otros, todos los cuales son hechos característicos del ámbito informático, **único campo en el cual pueden cometerse**. Aquí cabe derechamente el delito tipificado en el artículo 31 del segundo P.CH.L.I. y en el artículo 27 del que se elaboró después de la revisión del anterior, en 1987, figuras ambas que in extenso analizaremos en el Capítulo V. Evidentemente, es esta segunda especie delictual la que justifica el estudio específico de los D.I." (p. 84); En la misma dirección, véase la postura acogida por Pinochet (2006): "es así como entendemos por delito informático a la acción típica, antijurídica y dolosa cometida mediante **el uso normal de la informática, contra el soporte lógico o software, de un sistema de tratamiento automatizado de la información**. Por lo tanto, únicamente estaremos ante un delito informático cuando se atenta dolosamente contra los **datos digitalizados y contra los programas computacionales contenidos en un sistema**; otros casos parecidos, serán sólo delitos computacionales que no ameritan la creación de un nuevo ilícito penal" (p. 485)

^{xvi} Así lo entienden Huerta y Libano (1998) cuando afirman: "Diremos que hay delito informático cuando la acción u omisión típica **sólo puede realizarse por medio, en utilización o en contra de un sistema informático**. Se trata de ilícitos que surgen con el nacimiento de la informática y que no han encontrado, en una época anterior a tal suceso, descripciones típicas en los cuerpos legislativos penales clásicos. Desde este punto de vista, sostenemos que no es sano estimar tales ilícitos como informáticos. **Estimamos que no es buena una técnica legislativa que "informatic" los delitos comunes** ya que de tal forma se menoscaba el carácter especialísimo de los delitos informáticos. Es evidente que algunos delitos comunes se facilitan al cometerse por medios informáticos. En este punto, debemos reparar en la licitud o ilicitud de la acción u omisión informática, herramienta de comisión de un delito como sería, por ejemplo, la estafa. Si la conducta informática es lícita y la estafa se consuma, **habrá pura y simplemente una estafa** que se sancionará de acuerdo a las prescripciones del Código Penal."

^{xvii} En contra de esta postura, Miró (2012), quien señala: Se debe recordar, de nuevo, que al hablar de cibercriminalidad, lo hago en sentido amplio como **concepto englobador de cualquier delito cometido mediante el uso (esencial) de las TIC**. Esto nos debe servir para comprender la variedad de delitos de naturaleza distinta que conforman tal categoría y, por tanto, y a los efectos que ahora nos interesan, la variedad de objetivos sobre los que pueden actuar las, por su parte, diferentes tipologías de ciber- criminales y, por ende, la multiplicidad de víctimas de la cibercriminalidad que existen. (p. 261)

^{xviii} Sieber (1998) define el hacking así: The term "computer hacking" traditionally describes the penetration into computer systems, which is not carried out with the aims of manipulation, sabotage or espionage, but for the pleasure of overcoming the technical security measures. In practice, this kind of offense can be frequently found. (p. 9)

^{xix} A favor de la tipificación autónoma del "hacking directo" véase Huerta y Libano (1998): "Un segundo supuesto motivacional del hacker estará determinado por un ánimo que podríamos llamar "no dañoso". En efecto, es posible, y así ha ocurrido muchas veces, que el delincuente busque la violación de la negativa al acceso, entiéndase códigos, passwords, etc., como una forma de autogratificación de sus capacidades técnicas e intelectuales. El hacker perseguirá la satisfacción de lograr vencer un obstáculo y de demostrar que los programadores que dispusieron las medidas de seguridad no pudieron contra su inteligencia. Asimismo, dentro de esta motivación "no dañosa", se encuentran los hackers que buscan burlar los códigos de acceso con la finalidad del simple divertimento o por razones de curiosidad. Estas conductas, a pesar de no causar un daño directo y tangible, son delitos en sí mismas y deben, necesariamente, estar reguladas y sancionadas" (p. 17)

^{xx} En contra de esta postura, y recalando el papel preponderante de la información, Piragoff (1994) afirma: Even if there is no alteration or destruction of, or interference with the use of data, the intrusion into the computer system, interception

of communications or gaining knowledge of other inner-workings or functions of a computer system represents a serious violation of privacy. (p. 100)

^{xxi} Manifestándose sobre esta dicotomía, Pinochet (2006) ha señalado: En doctrina, el delito de acceso no autorizado o de hacking, consiste, en general, en infringir un sistema de seguridad informático sin autorización. Asimismo, el hacking o el acceso ilegítimo a sistemas de información, como también se le denomina, puede clasificarse, en hacking directo o propiamente dicho y en hacking indirecto (...) Por otra parte, se debe mencionar al delito de cracking, que está relacionado con el hacking o acceso no autorizado, señalando que "en el caso de querer dolosamente dañar el sistema, alterar o suprimir información, se estaría ante un supuesto de cracking, que es una figura que subsume al hacking. O sea, en el cracking, además de configurarse un acceso ilegítimo al sistema de información, se lo daña o se lo altera con voluntad dolosa de provocar dicho daño, sin que se produzca un concurso ideal de figuras" (p. 495)

^{xxii} Respecto a la definición de "virus informático", véase Palazzi (2000) cuando afirma: "Un virus informático no es un organismo con vida propia, a pesar de la analogía que presentan con los virus biológicos: ambos se reproducen engañando el metabolismo del huésped al que infectan; este proceso produce alteraciones en el metabolismo del cuerpo (o en el funcionamiento de la computadora); pueden llegar a tener un tiempo de incubación y finalmente desarrollan su efecto final. En el caso de los virus informáticos este efecto consiste en la destrucción o borrado de las memorias, tanto magnéticas como electrónicas de la misma, o la alteración del normal funcionamiento del sistema. Un virus de ordenador es un programa que tiene la capacidad de hacer copias de sí mismo en otras computadoras y producir un efecto determinado por su autor, que puede ser inofensivo o dañino. Lamentablemente esto último se da en la mayoría de los casos." (P. 145); En similar sentido, Jijena (1998) señala: "No es errado pensar en los virus computacionales como «una especie de plaga electrónica expresada en tenués señales al interior de los computadores», aunque es más preciso concebirlos como programas mal intencionados creados por mentes algo brillantes que han tomado rumbos equivocados. La expresión virus se usa en un sentido analógico, para referirse a programas computacionales que alteran sistemas de tratamiento automatizado de información y sobre los cuales no existiría un mayor control. El virus es —dentro de las modalidades de D.I.— una especie de sabotaje informático, más precisamente un upo de caballo de Troya, porque es un programa aparentemente inofensivo que porta instrucciones que se introducen en un programa de uso normal, las que pueden ser letales. Constituirá una bomba lógica que desencadene un contagio, cuando sea programado para que se active en un momento determinado, permaneciendo inactivo el resto del tiempo." (p.127)

^{xxiii} Al respecto véase Sieber (2009) quien se refiere a los virus como medio idóneo para cometer el sabotaje informático, de la siguiente forma: "Today in the field of computer sabotage, a similar "popularization" as in the field of computer manipulations occurs: Beside the formerly predominant major cases of sabotage which only rarely appear in the today's statistics, there are massive damages to personal computers caused by virus programs and worm programs. These programs are spread especially through illegally copied software or in networks, and therefore constitute a considerable share of the total number of computer crimes. Computer viruses are programs which spread in other programs of a computer system and - possibly with a delay of time - often cause damages. The number and the variety of viruses in circulation has increased in recent years. In some cases, the original software as issued by the producing company was already infected with a virus." (p. 8)

^{xxiv} Pinochet (2006) define el "sabotaje informático" así: Podemos señalar que el sabotaje informático, es conceptualizado como todo ataque que busque borrar, alterar o destruir intencionalmente un sistema o dato informático (...) En este caso, podemos apreciar que el elemento objetivo del delito de sabotaje informático, está constituido por la destrucción o inutilización de un sistema o datos informáticos. Además, el elemento subjetivo del referido delito, consiste en la intención de dañar el sistema o datos de un tercero." (p. 489)

^{xxv} Frente a esta conducta típica, Choclán (2002) señala: "Se trata de un delito que ataca los elementos lógicos de un sistema informático. También en este caso una sola acción puede producir una colectivización del perjuicio (por ejemplo un virus informático). En estos casos en los que pueden verse perjudicados un número indeterminado de sujetos por la acción de sabotaje se justifica una penalidad agravada respecto del tipo básico de daños, pero nuestro legislador ha configurado el sabotaje informático con gran amplitud y como tipo agravado en todo caso. En determinadas hipótesis esta agravación no será plausible, en los casos en que o bien por la poca importancia de los datos alterados, o por la escasa dimensión del perjuicio, no se ha producido un grave perjuicio." (p. 276)

^{xxvi} Frente al *modus operandi* en el sabotaje informático, Sieber (1992) ha señalado: "El *modus operandi* que se utiliza con más frecuencia en el ámbito del sabotaje informático consiste hoy en día sobre todo en la práctica de incendios y atentados con bombas, así como en la introducción de los denominados «programas crash», que borran grandes cantidades de datos en un cortísimo espacio tiempo. Además también deben constatarlas acciones de sabotaje por medio del teleproceso anteriormente indicadas." (p. 25)

^{xxvii} Tiedemann (1985) señala frente al sabotaje informático lo siguiente: "Tanto desde la perspectiva de la envergadura del daño como desde la del modo de realizar el hecho, son dignos de considerar los casos de sabotaje en el procesamiento de datos. También éstos resultan favorecidos por la gran concentración de informaciones en un mínimo espacio. La destrucción total de programas y datos —por ejemplo, mediante atentados con incendio, imanes o «programas borradores» especialmente elaborados— puede poner en jaque la continuidad de toda una empresa. Los servicios secretos de otros países, los fanáticos políticos y los empleados deseosos de venganza deben ser considerados como posibles autores." (p. 128)

^{xxviii} Para Anarte (2001-A) lo que se creó fue una nueva sociedad: la “sociedad de la información”. Así se refiere a este tema el citado autor: “Las innovaciones tecnológicas apoyadas en la informática y en las redes de comunicación mundial, así como su expansión en las últimas décadas, han derivado en un nuevo paradigma sociológico nominado **Sociedad de la Información y/o del Conocimiento**. En este sentido, el conocido Informe Bangemann habla de una «nueva revolución industrial, basada en la información, que se puede procesar, almacenar, recuperar y comunicar de forma ilimitada e independiente de tiempo y distancia». Se trataría, según esto, de nuevos sistemas sociales basados en los servicios, cuyos principios axiales dejarían de ser el capital y el trabajo para centrarse en el “conocimiento teórico”. (p. 191)

^{xxix} Al referirse al cambio de paradigma que ha generado el surgimiento de la tecnología informática, Sieber (1994) señala: In all countries criminal law faces considerable challenges in dealing with computer crime. The common ground for these problems originates from the fact that all criminal codes have, to the present, predominantly protected tangible and visible objects. The protection of information and other intangibles existed, but did not play a dominant role until the middle of the 20th century. However, this situation has changed rapidly during the last decades: The development from industrial to post-industrial society, the increasing value of information (for economy, culture, and politics), as well as the growing importance of computer technology, led to new challenges for "information law". In recent years the resulting wchange ofparadigma" from corporeal to incorporeal objects reached substantive criminal law in various waves of computer crime legislation. (p. 7)

^{xxx} Resaltando la relación de causalidad entre el surgimiento de una nueva tecnología y el correlativo surgimiento de un nuevo riesgo, Sieber (1998) señala: Computer crime and criminal information law are relatively young phenomena. A first historical analysis indicates that each new development of computer technology was followed by a corresponding adaptation of crime as well as by legislative changes. (p. 3); Más de una década después, Sieber (2009) reafirma su postura sosteniendo: Actualmente la tecnología de la información juega un papel central no sólo en la comunidad empresarial, sino en la vida privada y cotidiana de millones de personas. Como consecuencia, los ordenadores y las redes informáticas se utilizan cada vez más como herramienta de auxilio en la comisión de diversos delitos “tradicionales”, como fraude, tráfico de drogas, terrorismo, y otras formas de crimen organizado. (p. 160): En el mismo sentido, véase Aboso (2006): La irrupción del ordenador y la red informática en la vida del hombre moderno representan un giro significativo en el transcurso de su historia, que afectan de un modo positivo su realidad cotidiana. Este fenómeno informático permite fomentar la difusión de ideas entre los individuos, sin depender de la posesión de los medios de comunicación. Los beneficios de la informática pueden percibirse sin mayores explicaciones en el terreno del comercio, la comunicación, el transporte, la educación, la medicina, entre otras áreas. Esta realidad, sin embargo, exige evaluar qué necesidades humanas deben ser satisfechas de modo perentorio, y en qué medida urge diseñar una nueva regulación jurídica para dichas actividades. (p. 5)

^{xxxi} El “cracking” es definido con suficiencia por González Rus (2003): “El término cracking se utiliza para referirse específicamente a los daños informáticos que se producen accediendo a sistemas informáticos ajenos a través de Internet o redes de transmisión de datos. Una referencia tan amplia, sin embargo, es apropiada únicamente si se usa en sentido criminológico o informático, pero resulta menos útil si se pretende aludir con ella a los comportamientos delictivos que con ese nombre se recogen en las distintas legislaciones y en particular en el caso español. Y es que, dado que lo característico de los medios o procedimientos informáticos es que mediante ellos se llevan a cabo las funciones de almacenamiento, procesamiento o transmisión de la información, resultan más exactas las definiciones de sabotaje informático que comprenden únicamente las conductas que, cualquiera que sea el procedimiento a través del cual se produzcan, tienen por objeto preferente de ataque a los elementos lógicos de un sistema informático, como por lo demás, hace la doctrina mayoritaria” (p. 209)

^{xxxii} La telecomunicación es definida como “Sistema de comunicación telegráfica, telefónica o radiotelegráfica y demás análogos” (RAE, 2012). De aquí se desprende que, cuando abordamos la “interceptación de telecomunicaciones” no sólo hacemos referencia a las comunicaciones verbales telefónicas, sino también aquellas no verbales, como los “chats” o los correos electrónicos, entre muchísimas otras formas de telecomunicación.

^{xxxiii} Tan idónea es la red para interceptar comunicaciones que desde un mismo lugar podrían interceptarse las comunicaciones que se realicen alrededor del mundo, sin importar la distancia entre los interlocutores y quien intercepta. Como ejemplo claro de esta afirmación, Maza (2001) trae a colación el programa “ECHELLON”: “El conocido programa ECHELLON, de intervención indiscriminada en las comunicaciones informáticas, aplicado, con fundamento en razones de Seguridad nacional, por el Gobierno de los EEUU de Norteamérica, que representaba la posición de ese Gobierno acerca del criterio aplicable a esta clase de comunicaciones, se ha visto aún incrementado en sus fines por la denominada “Ley Patriota”, aprobada por el Legislativo de ese país, por razones de urgencia, en octubre de este mismo año. Aunque soy de la opinión de que, en el largo plazo, los intereses comerciales y económicos, tan básicos para la existencia misma de la Red, se acabarán imponiendo sobre los criterios políticos, para un reforzamiento de las garantías de privacidad, es lo cierto que, en la actualidad y presumiblemente durante cierto tiempo, esa tendencia “intervencionista”, al menos en EEUU, va a subsistir, con la trascendencia que, en esta materia, **supone la posibilidad de controlar desde un lugar determinado las comunicaciones que se realizan en otros lugares del planeta**. (p. 638)

^{xxxiv} Pues es un riesgo que ha surgido con antelación a los sistemas informáticos. Al respecto ver Aboso (2006) cuando afirma que: Una cuestión íntimamente ligada con la problemática propuesta en este artículo se entremezcla con el pavoroso auge experimentado por la pornografía infantil. Quizás, sin temor a equívoco, pueda afirmarse que este género delictivo ha sido el que más se aprovechó de la utilización abusiva de la red informática, circunstancia que halló eco en los

gobiernos en general, preocupados por poner coto a este auténtico flagelo que tiene por víctimas a los menores de edad, que afecta gravemente su indemnidad sexual, a la par de dejar profundas e indelebles huellas en sus inocentes psiquis. (p. 156-157)

^{xxxv} Rueda Martin (2014) narra un aterrador caso ocurrido en Canadá, en el cual, a partir de la entrega de una imagen donde aparecía semidesnuda a un hombre extraño que la abordó en la red, una menor se vio sometida a toda clase de vejámenes que terminaron por llevarla al suicidio. Así se refiere la citada autora a este suceso: “Por otro, las aludidas manifestaciones causan una gran alarma social cuando sus víctimas son menores de edad, por las dramáticas consecuencias que pueden conllevar, como ha sucedido con el reciente caso de Amanda Todd, una adolescente canadiense de quince años de edad que se suicidó en las siguientes circunstancias, extraídas de la noticia publicada por el diario digital español *El País* el 19 de octubre de 2012, bajo el título “Humillada en la red, humillada en la calle”: “Todo empieza con una imagen, un dato íntimo, una clave entregada a un desconocido al otro lado de la línea. Así comenzó el infierno de Amanda Todd, la joven canadiense de 15 años que se suicidó hace una semana tras haber colgado un mes antes un vídeo en internet en el que contaba su tragedia en pequeñas cartulinas. “Nunca podré recuperar esa foto. Está ahí para siempre”. Es una de las frases de Todd. Se refería a esa primera foto –captura de un vídeo grabado por web cam– con el torso desnudo que su acosador anónimo utilizó para amedrentarla y de la que no pudo huir pese a los sucesivos cambios de colegio.

En este supuesto, la entrega consentida de la imagen de un menor de 12 años de edad, a un extraño con el torso desnudo a través de internet fue utilizada para amenazar y humillar públicamente a la víctima, de modo que le produjo, durante tres años, un gran sufrimiento personal que culminó con su suicidio.” (Pp. 123-124) Para una visión panorámica del caso narrado, véase el video contenido en el siguiente link: <https://www.youtube.com/watch?v=Pc1sK1WX2LA> denominado “Amanda Todd. Stop Bullying.”

^{xxxvi} Frente a la dificultad para sancionar los delitos informáticos, Pinochet (2006) señala: “Existe consenso en la doctrina, en que los delitos cometidos por medio de Internet, son de difícil sanción, debido a la aterritorialidad de las conductas delictuales, es decir, la circunstancia de que se realizan en un país determinado pero se consuman en otro; a la no tipificación de los delitos y la distinta calificación jurídica de una conducta, en la legislación nacional de un país en relación a otro; y finalmente, al rápido avance de las nuevas tecnologías que hace casi imposible, mantener actualizados la regulación de las conductas punibles que van apareciendo.” (p. 477); En el mismo sentido, Vera (1996) señala: “14. LAS PRINCIPALES CARACTERÍSTICAS DE LA ACTIVIDAD INFORMÁTICA QUE INCIDEN EN LA COMISIÓN DE DELITOS SON LAS SIGUIENTES: 1. Concentración de la información. La tendencia a centralizar y consolidar toda la información corporativa en grandes bases de datos, sobre las que interaccionan multitud de usuarios, posibilita considerablemente el acceso a cualquier tipo de información, una vez que se han penetrado las medidas de control de acceso que estén establecidas. 2. Ausencia de registros visibles. La posibilidad de descubrir un hecho fraudulento por simple inspección visual está completamente eliminada al estar la información grabada en forma de impulsos eléctricos sobre soportes magnéticos que no son directamente legibles para el ser humano.” (p. 56)

^{xxxvii} En el mismo sentido, véase: Alastuey (1994) cuando señala: “Por un lado, no existen todavía medios adecuados de detección y control de los hechos. Un sistema complejo de control no resultaría beneficioso a las empresas que precisamente buscaron rentabilidad económica y ahorro de tiempo con la instalación de equipos informáticos”. Por otra parte, la víctima desconoce el hecho la mayoría de las veces o, aun conociéndolo y sospechando fundadamente quién lo cometió, tiene dificultades para probar ambas cosas (tanto la perpetración del hecho como su autor). **Ciertamente, descubrir el hecho no resulta fácil**; las propias características del mismo lo impiden: los medios complejos de comisión del hecho que son conocidos exclusivamente por especialistas en sistemas informáticos, la facilidad del autor de borrar toda huella que pueda inculparle, **la separación temporal entre lugar de comisión del hecho y de producción de los efectos, etc.**” (p. 457)

^{xxxviii} Frente a la necesidad de estructurar una cooperación internacional de cara a las problemáticas que genera la comisión de delitos informáticos, Núñez y Rey (2011) afirman: “Por lo anteriormente expuesto, es de vital importancia elaborar nuevos planteamientos dogmáticos y político criminales tendientes a crear mecanismos eficaces para obtener mayor cooperación entre los Estados y así poder sancionar, mediante el uso del derecho penal la delincuencia consumada en el ciberespacio” (p. 625)

^{xxxix} Respecto del procedimiento forense para la investigación de delitos informáticos, véase Álvarez Cabrera (2005), quien señala: “El proceso forense en materia de evidencia digital, a muy grandes rasgos, se divide en tres momentos: la recolección de la evidencia, su análisis y su presentación. En la recolección, antes que nada, el investigador debe asegurarse de no modificar la información contenida en el medio magnético (...) En este punto se da inicio a la segunda parte del procedimiento forense: el análisis del medio magnético (...) En la etapa de presentación el investigador, el abogado y el fiscal deben tener en cuenta normas de estrategia como las presentadas por el *National Center For Forensic Science*, debiendo para el efecto determinar hasta qué punto debe capacitar a la audiencia en temas técnicos –al juez, por ejemplo–, decidir sobre la conveniencia de pedir el testimonio de un experto, etc.” (p. 22)

^{xl} A favor de esta afirmación, véase Vera (1996) quien afirma: “3. Los programas (35) y los datos pueden alterarse sin dejar rastro. En tanto la manipulación de registros escritos es bastante difícil y suele dejar evidencias, la alteración de programas o datos grabados en soportes magnéticos puede hacerse sin dejar rastro, salvo que se hayan adoptado las adecuadas medidas de control.

4. Fácil eliminación de pruebas. Es extremadamente fácil en caso de peligro, hacer desaparecer programas manipulados o ficheros completos de datos alterados, desde la consola del computador o desde un terminal tan sólo pulsando una tecla o emitiendo una instrucción de borrador, lo cual, posteriormente, puede hacerse pasar por un error fortuito.” (p. 57)

^{xli} ***Nota sobre la responsabilidad de los prestadores del servicio de internet.** Si bien este tema no encuadra dentro de la perfilación criminológica del delincuente informático, sí es importante señalar simplemente que, los prestadores del servicio de internet pueden llegar a incurrir en responsabilidad penal cuando a través de sus plataformas se cometen delitos en contra de la información y los sistemas informáticos. Para tal efecto, como es apenas obvio, deberá acreditarse el dolo en su actuar (cuando menos el dolo eventual) así como los requisitos exigidos en torno a la imputación objetiva, lo que presenta no pocos problemas. Más allá de esa dificultad, la potencial responsabilidad de las personas naturales encargados de la prestación del servicio es un tema que no debe perderse de vista por parte de los operadores judiciales y que deberá ser objeto de un desarrollo doctrinario suficiente. En similar sentido, Gómez Tomillo (2004) afirma: “Con independencia de lo expuesto, cabe hacer una mínima reflexión en torno a la responsabilidad del resto de potenciales intermediarios que intervienen entre la confección de la información ilícita y la recepción de ésta por parte de una pluralidad indeterminada de destinatarios. En primer lugar, analizamos la de quien se limita a facilitar el acceso a internet, esto es, quien tan sólo posibilita a un usuario entrar en la red, hecho que es utilizado por aquél para llevar a cabo el comportamiento antijurídico, por ejemplo, depositar pornografía infantil accesible a terceros en un servidor. Desde nuestro punto de vista, tales proveedores de acceso difícilmente se puede sostener que lleven a cabo una actividad punible. Ciertamente acceder a la red es el presupuesto necesario para cometer los delitos a los que nos referimos. Asimismo, en las excepcionales hipótesis en las que medie dolo, cuya prueba es realmente compleja, en abstracto cabría estimar que se realiza una conducta de cooperación, necesaria o no” (p. 107).

^{xlii} No obstante, hay quienes asemejan a los delincuentes informáticos con los defraudadores patrimoniales. Al respecto, véase Camacho (1987) quien asevera: “¿Qué es un defraudador? Alguien que roba desde una posición de confianza. No utiliza una pistola. No toma riesgos. Conoce a sus jefes y sabe que confían en él. Y a pesar de ello, roba. Sabe que no está corriendo grandes riesgos. Los autores de la mayoría de los grandes fraudes no acabaron en la cárcel.» A pesar de que este comentario se refería a los llamados delincuentes de «cuello blanco» y no a los delincuentes informáticos de forma específica, creo que es totalmente aplicable a nuestro caso ya que aquellos defraudadores son el más claro antecedente de éstos, y sus características son bastante similares. En cualquier caso, e independientemente de las motivaciones que pueda tener para cometer el delito, es un empleado que por su trabajo tiene acceso al sistema informático y conoce suficientemente sus debilidades como para permitirle realizar el hecho delictivo.” (p. 84)

^{xliii} Así, Jijena (1998) señala sobre el delincuente informático: “a) Se trata de una persona con **niveles de inteligencia y conocimiento superiores**. b) Posee óptima preparación en el manejo de la tecnología informática (se afirma que la preparación indiscriminada de expertos de alto nivel técnico sin la adecuada preparación ética, «ha democratizado el delito en las oficinas»). c) No es de extrañar que se trate de profesionales del área y de personal calificado de las empresas informáticas d) Ratificando nuestra afirmación anterior, según estadísticas publicadas en 1985 por el National Bureau of Computer Crime, en EE.UU. el típico delincuente informático tiene entre 18 y 30 años de edad, no posee actividad delictiva previa, es de sexo masculino y tiene **características de empleado sobresaliente**. e) El delincuente actúa confiando en la ignorancia de la eventual víctima sobre la vulnerabilidad de los computadores” (p. 110)

^{xliv} Singular resulta la acepción de “hacker” que presenta Gallardo (1998): “¿Cómo es realmente un delincuente informático? Si bien no se puede generalizar y menos en el terreno de las motivaciones, donde ni siquiera los psicólogos logran ponerse de acuerdo respecto a las razones que pueda haber tras esta clase de conductas antisociales, estos piratas suelen ser personas de entre 15 y 30 años, varones, blancos, con amplios conocimientos de comunicación e informática y versados en el manejo de sistemas operativos (los programas que gestionan los ordenadores). Ahora bien, ¿de dónde salen y qué buscan estos delincuentes? Los hackers de viejo cuño procedían, en su mayoría, de aquella generación hippie de los años sesenta y tenían motivaciones filosóficas con un cierto sentimiento anarquista, pero con un código de honor que siempre trataban de respetar. Los actividades hackers, los de nueva escuela, no se merecen este nombre, sino que se trata de criminales informáticos, vándalos, descreídos o delincuentes juveniles en los que no se puede encontrar ningún tipo de ética.” (p. 372)

^{xlv} Los resultados de estas búsquedas incluyen tutoriales web, manuales en PDF, e incluso videos acerca de cómo acceder, paso a paso, a un sistema informático ajeno. En apoyo a esta afirmación, véase Morales (2002) cuando asevera: “Ciertamente, en materia de acceso ilegal la decisión política criminal de tutelar o no penalmente el intrusismo informático sin otra finalidad es compleja. La vertiginosa evolución del mundo Internet ha eclipsado el romanticismo inherente a aquellas conductas consistentes en acceder a sistemas ajenos e informar al administrador de los déficits de seguridad, sugiriendo alternativas para preservar la integridad del sistema frente a posibles ataques; **además, cualquiera puede ser ahora un intruso con los programas de entorno gráfico de acceso ilegal que pueden obtenerse gratuitamente en Internet...**” (p. 27)

^{xlvi} A favor de esta afirmación, véase: Tiedemann (2000) “Dos procesos penales de la Fiscalía de Stuttgart, todavía en curso, atestiguan sobre el hecho de que los ataques a sistemas informáticos también siguen siendo practicados **desde adentro, es decir por trabajadores desleales de una empresa** (o de la administración): una oficinista que liquidaba los pagos de la empresa a través del tráfico BTX (Online), giró en 134 oportunidades a su hijo un total superior a 500,000 DM [aproximadamente 250,000 dólares]; y un cocinero de la cantina de Telekom, al calcular la garantía por botellas de las

bebidas, descontaba de las tarjetas-chip, en vez de 0.30, 5 marcos alemanes por pieza, obteniendo una ganancia total de más de 40,000 DM” (p. 89)

^{xlvii} Para un estudio completo de los *insiders*, véase: Salvadori (2013), quien señala con especial énfasis: “No hay duda de que este delito se puede aplicar respecto a las introducciones en un sistema informático realizadas por parte de personas no autorizadas a acceder a este (*outsider*). Sin embargo, en los últimos años ha aumentado de manera considerable el número de accesos realizados por parte de empleados (*insider*) que utilizan el sistema informático, al que han accedido de manera legítima para finalidades contrarias o diferentes a las autorizadas. Cada día son más frecuentes en la práctica los casos de empleados que aprovechan de la posibilidad de acceder a los sistemas informáticos de las empresas en las que trabajan para copiar o dañar datos o programas informáticos.”² (p. 7)

^{xlviii} Similar, Camacho (1987): “En el párrafo citado encontramos un primer elemento de interés: (los delincuentes informáticos) suelen ser empleados de confianza, bien por el tiempo que llevan en la empresa, o bien por el tipo de trabajo que realizan. Este elemento común, la confianza depositada por la empresa en el autor del fraude, se repite inexorablemente en la historia de la delincuencia informática. No podemos olvidar que de acuerdo con los estudios estadísticos disponibles el 70% de los riesgos proceden de personal perteneciente a la empresa, en tanto que sólo el 5% proceden de personal externo.” (p. 84)

^{xlix} A favor de esta afirmación, véase Alastuady (1994) quien apunta: “Los autores del «delito» no suelen ser personas con una inteligencia superior a la media que poseen conocimientos cualificados en el campo de la informática y que por ello llevan a cabo manipulaciones sofisticadas en los sistemas informáticos, sino más bien personas con un coeficiente intelectual medio, **que tienen la «oportunidad» de realizar el hecho y la aprovechan**” (p. 459)

ⁱ Ahora bien, no podemos culminar el análisis del criminal informático sin hacer una breve referencia a la prevención del surgimiento de delincuentes informáticos. Para tal efecto, consideramos necesario, desde el punto de vista criminológico, señalar que la educación se constituye en el primer mojón para evitar que los niños se conviertan en “hackers”. Así, Álvarez (2003) afirma: “En la era actual, dada la conectividad en la cual la mayoría de negocios está inmersa, vía internet o intranets (en términos generales), y puesto que cualquier adolescente con conocimientos básicos puede utilizar herramientas gratuitas de software, descargables desde miles de sitios en la red, que permiten realizar intrusiones no detectadas, robo de información, alteración no autorizada de sitios web, desciframiento de claves de correo electrónico o de comunicaciones o documentos protegidos, entre otros, se ha hecho evidente que, frente a tal nivel de riesgo, cualitativo y cuantitativo, conviene tomar medidas proactivas que impidan a esos niños cometer sus fechorías.” (P. 114)

ⁱⁱ En este sentido se pronuncian Herrera y Núñez (1999): “Se considera a estos ilícitos como delitos de “cuello blanco”, exigiendo en el sujeto activo una calificación especial, un cierto nivel de conocimientos informáticos. Sin embargo, creemos que esta característica no es relevante, ya que cada día se está avanzando en dirección a hacer más fácil, comprensible y accesible la computación a todas las personas, ya que es imprescindible para poder informatizar nuestras actividades cotidianas. Por ello, **desde un niño a un anciano podrán realizar estas acciones ilícitas**. Sin perjuicio de lo anterior, existen algunos delitos informáticos que sí requieren conocimientos más profundos.” (p. 224)

ⁱⁱⁱ Dicho en otras palabras por Gutiérrez (2005): “Por lo mismo, cabría afirmar que todos y cada uno de nosotros, individual o colectivamente, estamos implicados en el «gremio de afectados». Ninguno de los ciudadanos de una sociedad incorporada al tren de la era digital puede considerarse «no aludido» en este tema. (En la medida en que realizamos todo tipo de actividades usuales como adquirir bienes en supermercados que fijan sus precios en códigos de barras, es decir, electrónicamente, por ejemplo, podemos ser víctimas de fraudes informáticos; en la medida en que usamos teléfonos con tarjetas electrónicas, eventualmente podemos ser víctimas de manipulaciones en las mismas para que se nos cargue mayor costo en cada llamada; en la medida en que usamos Internet, podemos estar siendo víctimas de programas espías contra nuestra intimidad, o podemos sufrir las consecuencias de un virus informático que dañe todo nuestro sistema, o destruya nuestra valiosa información... etc.)” (p. 70)

^{liii} Ver *infra*, capítulo VI: el hurto por medios informáticos.

^{liv} Al respecto, ver: Moron Lerma (2002) p. 74 y ss. Para un estudio detallado de esta discusión, ver: Rueda Martin (2009) p. 174 y ss.

^{lv} Ley cuyo artículo primero, al referirse sobre el objeto de la misma, señala: “La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”.

^{lvi} En Colombia, la ley 1581 de 2012 relativa a la protección de datos personales, contempla como objeto “La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.” Sin embargo, aun cuando esta ley contempla sanciones para quienes violen los datos o archivos personales, lo cierto es que no es viable dejarle a ella la sanción de quienes los infringen. Pues, a diferencia de España, en Colombia solo pueden ser sancionados “los responsables y encargados del tratamiento de datos personales. Es por esto que, el artículo 23 de la precitada norma establece que se podrán imponer sanciones a los “responsables y encargados del tratamiento de datos. Pero no a cualquier sujeto que, sin ser responsable o encargado, decida violentar los datos personales –como sería el caso del “hacker”-. Lo preceptuado por el artículo 23 de la ley 1581 es lo siguiente:

“Artículo 23. Sanciones. La Superintendencia de Industria y Comercio **podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento** las siguientes sanciones: a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó; b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar; c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio; d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles; Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva”.

^{lvii} Adoptan esta postura, por todos, Rueda Martín (2009); Posada (2013); Herrera y Nuñez (2001); Meek (2013); Aboso (2006).

^{lviii} En este sentido, véase Herrera y Nuñez (2001) para quienes la existencia de un bien jurídico es innegable: “En definitiva, el tema de los bienes jurídicos protegidos por los delitos informáticos necesita abordarse en primer lugar, desde un concepto unívoco de éstos, que sólo incluya a los nuevos delitos incapaces de encuadrarse en las figuras tradicionales. Y luego, reconociendo como único objeto afectado por tales conductas al soporte lógico, sean programas o datos, es conveniente establecer parámetros claros para proteger penalmente sólo cierta información, que destaque por su finalidad, su naturaleza o importancia. Aquí dejamos una puerta abierta para la doctrina en primer lugar, y luego la jurisprudencia y el legislador, respecto a señalar qué elementos se considerarán para determinar la relevancia de una información.” (p. 223-224).

^{lix} Para un análisis detallado de la normatividad chilena sobre los delitos informáticos y su bien jurídico: ver *supra*., El Delito Informático en el Derecho comparado, Legislación Chilena.

^{lx} En este sentido, Martín (2001) recalca la importancia de la historia clínica digitalizada(HC): “Si bien no es objetivo de esta breve exposición, sí conviene en mi opinión recordar a los legos del mundo asistencial médico, que en una HC, se contienen datos susceptibles de una especial vigilancia, a este respecto ya existen diversas normativas nacionales y autonómicas, que definen el contenido de la HC así como su uso excepcional para otras actividades de tipo formativo, de investigación clínica, de control de calidad asistencial y por supuesto de investigación ante un Proceso Judicial, Penal, Civil, Laboral etc., siendo en este caso de gran valor probatorio para el Jurista y la esencia para la elaboración de la Prueba Pericial Médica, que origina no pocas controversias, que no procede analizar aquí, especialmente cuando la HC es requerida por la Autoridad Judicial y sale de recinto hospitalario. **Así pues el contenido de la HC que sucintamente exponemos, va a permitir deducir la necesidad de su custodia, dado que en ella se incluyen datos protegibles que constituyen uno de los bienes jurídicos que pueden ser vulnerados, la intimidad de las personas.**” (p. 246)

^{lxi} Continúa señalando Martín (2001): “Los que por razones profesionales manejamos continuamente Historias Clínicas en el soporte papel, nos parece en principio muy lejano el que pueda caer en manos intrusas estos datos, sin embargo esta cuestión se agudiza cuando **la HC en soporte magnético pueda ser limpiamente manipulada, copiada, o vertida en una red informática**, cuando todavía no existe una normativa de medidas de seguridad de alto nivel en ficheros automatizados.” (p. 247)

^{lxii} Similar, Laso (2002) quien afirma: “Ha llovido ya bastante desde que diera comienzo la protección institucionalizada de los datos de carácter personal. En este sentido desde sus orígenes, y con la finalidad de modernizar la Administración, todo Gobierno y todo Estado ha pretendido emplear para ello la ayuda de los tratamientos automatizados de datos. Pero este tratamiento automatizado de los datos de carácter personal no debería ni podría realizarse, en ningún caso, sin **una protección eficaz de dichos datos**. La intensificación del poder que otorga el manejo de los datos personales deberá así de estar siempre equilibrado normativamente mediante una consolidación de los derechos de los ciudadanos.” (p. 38)

^{lxiii} Davara (2007) define así las bases de datos: “Una base de datos es un depósito común de documentación, útil para diferentes usuarios y distintas aplicaciones, que permite la recuperación de la «información»1 adecuada, para la resolución de un problema planteado en una consulta. Todas las bases de datos deben partir de un fondo documental seleccionado, al que se somete a un proceso con objeto de que se pueda recuperar la información orientada a la solución de un problema. Así, consideramos la base de datos como un almacenamiento de documentación, organizada y estructurada de forma que permita recuperarla como información. Esto es, que dé respuesta a una consulta, a un problema.” (p. 165)

^{lxiv} Frente al significado de “tratamiento de datos personales”, la Directiva 46 de 1996 del Parlamento Europeo afirmó que se trata de “cualquier operación o conjunto de operaciones, efectuadas o no, mediante procedimientos automatizados, y aplicados a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, etcétera”.

^{lxv} Es de señalar que, en Colombia la legislación sobre la protección de sistemas informáticos se encuentra, apenas, en una etapa de formación y maduración absolutamente inacabada. Así lo señala Prias (2006) cuando afirma: “Quizás en esta materia como en ninguna otra, resulta evidente la incapacidad del derecho para adaptarse a las nuevas situaciones con la celeridad requerida, la cual es más significativa en el sistema del derecho continental por la formalidad y rigidez de sus fuentes. No obstante lo anterior, lo cierto es que las primeras manifestaciones de legislación en materia de sistemas e

informática cuentan ya con al menos dos décadas de desarrollo, si bien en países como Colombia, solamente hasta ahora se comienza a elaborar alguna legislación sobre el particular.” (p. 10)

^{lxvi} Por parte del derecho administrativo sancionador, específicamente mediante la ley 1581 de 2012, se ha dado un avance importante en la protección de los datos personales. Sin embargo, como ya mencionamos, dicha disposición se queda corta al sancionar únicamente a los “responsables y encargados de la protección de datos”. Por lo que, el problema de los “hackers”, desde el punto de vista del derecho administrativo sancionador, permaneció incólume.

^{lxvii} A favor de esta afirmación, véase Hernández (2001) cuando afirma: “El Código Penal no define en qué consiste el delito de daños, pero inequívocamente se entiende por tal la destrucción dolosa de cosas corporales (v. por todos *Etcheberry*, cit., p. 478). Por tal razón no son subsumibles en los respectivos tipos penales del § 10 del Título IX del Libro II del Código las conductas destructivas que tengan por objeto soportes lógicos (programas) o información virtual (en rigor la distinción no es esencial, porque los programas a su vez son un conjunto de datos).” (p. 8)

^{lxviii} En contra de esta postura, véase Palazzi (2000) quien señala: “Entonces, la información contenida en una computadora (ya sea en un diskette, en el disco rígido o en la memoria) llega a poseer la entidad suficiente para ser reputada cosa a los efectos de aplicarles las mismas disposiciones. Por otro lado la doctrina moderna le atribuye a la información un valor en sí misma como mercancía, y la posibilidad de un derecho de propiedad sobre ella” (p. 134)

^{lxix} Para un estudio detallado de la protección penal a los derechos de autor, ver por todos: Muñoz Conde (2013) p. 454.

^{lxx} En contra de esta afirmación, véase: Davara (2007): “La tendencia actual, en nuestra opinión acertada, es que **esta protección jurídica se lleve a cabo bajo la figura, sobradamente conocida, de los derechos de autor**; independientemente, ya que se trata de algo distinto, de las relaciones contractuales entre creador y distribuidor, o entre distribuidor y usuario que, dentro del principio de la autonomía de la voluntad de los contratantes, pueden establecer cláusulas que protejan y cubran más sus propias relaciones que el contenido de la información de la base (...) Consideramos una base de datos como «un depósito común de documentación, útil para diferentes usuarios y distintas aplicaciones, que permite la recuperación de la «información» adecuada en la resolución de un problema planteado en una consulta». Los tres apartados básicos de esta definición -depósito común de documentación, útil para diversos usuarios y permitir la realización de una consulta- deben ser interpretados **en su carga intelectual**, orientados a la comprensión a la que nos referimos. **No cabe duda de que las bases de datos exigen y desarrollan una creatividad**, tanto en el almacenamiento de la información y su relación e interoperabilidad con los diferentes sistemas lógicos y físicos que la tratan, como en la recuperación de dicha información de acuerdo con una consulta planteada.” (p. 176-177)

^{lxxi} Así, Gutiérrez (1996) afirma: “que castigando el hacking **se adelanta la barrera de protección** frente a hechos más graves, bien sean provocados de propósito (se accede subrepticamente sin otra intención que el jugar o el “poner a prueba” a la máquina, y de forma sobrevenida se decide la comisión de un fraude, o se copia información secreta, o se falsifican datos informatizados...), bien de forma no intencional (sin perseguirlo, el hacker que accede sin autorización modifica o borra, datos, provocando perjuicios de entidad, o se imposibilita el acceso al sistema a otro usuario del mismo con autorización...)” (p. 1179)

^{lxxii} Anarte (2001) se opone a que el bien jurídico sea denominado “libertad informática”, y señala que debe hacerse referencia a la “protección de datos personales”: “Más que la libertad informática, el artículo 197.2 protege el llamado **derecho a la protección de datos personales**, como se advierte en el hecho de que la conducta típica se cumple también cuando los datos apoderados, utilizados, modificados o a los que se accede, se hallan registrados, no en ficheros o soportes «informáticos, electrónicos o telemáticos», sino «en cualquier tipo de archivo o registro público o privado»” (p. 251).

^{lxxiii} Al pronunciarse sobre el bien jurídico protegido por los delitos informáticos Jijena (1998) afirma: “Nosotros creemos que la información, **el conjunto organizado de datos o el soporte lógico informático**, constituye el objeto material del D.I., no obstante ser intangible e incorporeal, con lo cual, acogiendo la configuración genérica que recién formulamos y para mantener la coherencia con la misma, tenemos que plantear un doble alcance para ella: sería un bien jurídico esencial para la sociedad y, además, los datos organizados en un sistema de tratamiento automatizado de los mismos se verían afectados directa y materialmente por los ilícitos informáticos. (...) En consecuencia, si observando empíricamente la realidad sabemos que el objeto material de un delito es la persona o cosa que constituye la materia sobre la cual recae la conducta del delincuente; que pertenece al mundo fáctico; que es un elemento del tipo, y que no existe en los delitos formales o de mera actividad (v. gr., falso testimonio), no dudamos en afirmar que en un DI el objeto material del mismo es un intangible, es inmaterial, es inapropiable directamente, es la información (...) Concluimos, en lo que al objeto jurídico respecta, que para la criminalidad informática la información se presenta como un bien genérico, proyectable, y que dentro de los bienes jurídicos específicos que de ella se desprenden a no dudar el más relevante es la información de tipo nominativa, es decir, la intimidad. (p. 93-94)

^{lxxiv} Como antecedente normativo relevante de esta consagración del bien jurídico tenemos lo preceptuado en el artículo 3 de la ley 1341 de 2009. Este artículo señala: “El Estado reconoce que el acceso y uso de las tecnologías de la información y las comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal son pilares para la consolidación de las sociedades de la información y del conocimiento.”

^{lxxv} A favor de esta afirmación véase Pinochet (2006): “Previamente, debemos definir el concepto de delitos informáticos o “ciberdelitos”, entendiéndose por tales a aquellas acciones típicas, antijurídicas y culpables, que recaen **sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien jurídico de naturaleza colectiva o macrosocial** (abarcativo de otros intereses, v.gr., propiedad común, intimidad, propiedad intelectual,

seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos), en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas" (p. 484)

^{lxxvi} En contra, afirmando que el bien jurídico se reduce necesariamente al patrimonio, Solano (1997). Quien afirma: "La criminalidad mediante el uso de computadores se realiza a través de conductas dañosas **sobre un bien jurídico tutelado por la ley que hace parte de un patrimonio**. El delito informático es toda acción dolosa que cause un perjuicio a personas naturales y jurídicas que puede producir o no un beneficio material para su autor, pudiendo o no perjudicar de forma directa o inmediata a la víctima, caracterizándose dicha acción por ser realizada mediante dispositivos habitualmente utilizados en actividades informáticas." (P. 277)

^{lxxvii} En contra, Morales Prats (2001) para quien el bien jurídico protegido por los cibercrmenes es la intimidad. Así lo señala el citado autor: "El estudio **sobre los riesgos para la intimidad que suscita Internet**, requiere previamente la elucidación del contenido de este bien jurídico en el ciberespacio, puesto que, como se expondrá, este objeto jurídico de protección se muestra como una realidad jurídica en constante evolución. En efecto, **el bien jurídico intimidad** va mutando su contenido y las facultades jurídicas que derivan del mismo al compás del desarrollo tecnológico." (p. 65), Similar, véase Matellanes (2000): La preocupación por la protección jurídica de la intimidad se ha visto acrecentada en los últimos decenios al comprobar la multiplicación y potencialidad de los procedimientos susceptibles de vulnerarla, como son los medios técnicos de captación y transmisión de la imagen y del sonido, así como de acumulación y procesamiento de información en general y de los datos de carácter personal. (p. 136)

^{lxxviii} En contra de esta afirmación, Lanzos (2003) señala: "Parece difícil entender cometido el delito o la falta de daños informáticos cuando simplemente advertimos **la mera inclusión de nuevos documentos** junto a los ya existentes o cuando se produce una perturbación temporal de la operatividad del sistema." (p. 407)

^{lxxix} Al respecto Anarte (2001) señala: "Por otra parte, brevemente, de un lado, como se ha indicado, la libertad informática (o ese nuevo derecho fundamental a la protección de datos), aún como poder de disposición sobre los datos personales, no es un todo homogéneo, sino que abarca diversas facultades. Dejando de lado precisiones, el artículo 197.2 no las protegería todas, al tiempo que, las que se tutelan, cristalizan de modo diverso según la conducta típica en él contemplada, pero también en otras formas típicas del Capítulo Primero del Título X. Y así, apoderarse y utilizar, como acceder y utilizar, representan un atentado a la intimidad del sujeto pasivo; mientras que modificar o alterar atentan contra un bien jurídico diferente, «la identidad informática o integridad de los datos, sin perjuicio de que en el segundo supuesto está también implícito en principio el acceso no autorizado»" (p. 236)

^{lxxx} Adoptando una postura "particular" Meek (2013) afirma: "ahora bien, debe decirse que un usuario en ejecución del delito informático atenta contra la incolumidad de la información y los datos informáticos en sus tres únicos posibles estadios: información tratada, almacenada y transmitida, que pudiendo representar cualquier objeto presente en la realidad viajan al interior de un sistema de procesamiento de información y se encuentra en alguno de los estadios acabados de mencionar" (p. 72)

^{lxxxi} Convenio que han ratificado los países miembros de la Unión Europea. Asimismo, sólo 5 países que no son miembros de la Unión Europea se han adherido al Convenio: Estados Unidos, Canadá, Japón, República Dominicana y, recientemente, Argentina. Por su parte, en el 2013 Colombia fue invitada por parte del Consejo de Europa a adherirse al Convenio de Budapest. Adhesión que deberá llevarse a cabo dentro de los cinco años siguientes a la invitación.

^{lxxxii} Prias (2006) reconoce expresamente el impacto persuasivo que tienen este tipo de convenciones internacionales respecto de las decisiones político criminales de los Estados. Dicho autor manifiesta: "Dado el carácter transnacional de este tipo de delincuencia, muchas veces la decisión de penalizar determinadas conductas no depende de la determinación autónoma de cada país. Quizás la manifestación reciente más significativa de este orden la constituye la "Convención del Consejo de Europa sobre la Delincuencia Informática", suscrita en Budapest el 23 de noviembre de 2011. Ciertamente cabe hablar de una globalización de la criminalidad –global crime– cuyo curso más eficiente se realiza a través de las grandes redes de la información y que ha motivado, ante eventos de tal gravedad como los del fatídico 11 de septiembre, reacciones tan discutidas como el *patriot act* americano que tipifica con todas las previsibles para el libre funcionamiento de la red el delito de "ciberterrorismo"." (p. 13)

^{lxxxiii} Traducción del italiano al español realizada por Salvadori (2014).

^{lxxxiv} Traducción del italiano al español realizada por Salvadori (2014)

^{lxxxv} Traducción del italiano al español realizada por Salvadori (2014)

^{lxxxvi} Herrera y Núñez (1999) señalan frente a este tipo penal: "En primer lugar, es interesante mencionar el desconocimiento del legislador respecto de la trascendencia de un "hurto" de datos, ya que en el primer informe de la Comisión se le consideró un delito de menor relevancia que el anterior, porque en él "no se destruye nada. Por otra parte, en este artículo encontramos la exigencia, para la perfección subjetiva del tipo, de un elemento motivacional necesario en el agente comisivo: la intención o ánimo de apoderarse, usar o conocer, indebidamente, la información contenida en un sistema de tratamiento de la misma. Por tal razón, no bastaría con el cumplimiento de alguna de las conductas tipificadas (interceptar, interferir o acceder al sistema), sino que es necesario este ánimo en el agente." (p. 258)

^{lxxxvii} Al estudiar los verbos rectores contenidos en este tipo penal, Vera (1996) señala: "Interferir (el sistema de tratamiento de información): es "causar interferencia, que en términos generales "es interponer o mezclar una acción o movimiento en otro" y debe ser entendido como la interposición o superposición de señales (ópticas, acústicas, electrónicas, magnéticas, etc.) u ondas de que resulta en ciertas condiciones, aumento, disminución o neutralización de los

impulsos magnéticos". En inglés el término es sinónimo de GLITCH, que es cualquier mal funcionamiento temporal o aleatorio en el hardware, y que a veces es provocado por un programa (Software). Accesar (el sistema de tratamiento de información): debe ser tomado en un sentido técnico y que "es la acción de ingresar al sistema de tratamiento de información desde un disco o desde cualquier otro periférico, lo que permitirá dependiendo de la parte del sistema al cual se ha accedido, sólo conocer datos o información, o además modificar o ingresar o sacar datos o información contenida en él. En inglés "ACCESS". (p. 202)

^{lxxxviii} Adicionalmente, un sector minoritario, entre el que encontramos a Meek (2013), afirma que son dos los bienes jurídicos protegidos por el tipo penal de hurto por medios informáticos. Por un lado, el patrimonio económico, y por el otro, la información y los datos informáticos. Así lo expone el mencionado autor "Como ya se dijo, tanto el patrimonio económico (bien jurídico individual) como la información y los datos informáticos (bien jurídico colectivo) son el objeto de tutela; esto indica, pues, que se trata de un tipo penal pluriofensivo." (p. 120)

^{lxxxix} Para Aboso (2006) el patrimonio económico: se puede definir el patrimonio, a priori, como la suma de todos los bienes pecuniarios correspondientes a una persona. El concepto de patrimonio incluye los bienes materiales y los inmateriales, ambos de necesaria apreciación económica y de pertenencia ajena. Se incluyen, por ende, los derechos reales, la posesión, la tenencia, incluso derechos personales de carácter patrimonial, y los créditos (p. 76-77)

^{xc} La concepción jurídico-económica del patrimonio es la mayormente acogida por la Corte Suprema de Justicia Colombiana.

^{xc i} Partidario de esta postura es Aboso (2006) quien al referirse acerca de los "fraudes informáticos" acota: En este apartado nos detendremos en el estudio de las formas que adoptan las conductas fraudulentas que atentan contra el patrimonio de terceros. Pero, además, es menester efectuar una aclaración que se relaciona con la denominación en sentido estricto de "delitos informáticos", y que alcanza únicamente aquellos comportamientos ilícitos vinculados a la información y su transmisión o comunicación en general. Acá el bien jurídico afectado es el patrimonio en general, y lo que se castiga en particular son las conductas que afectan el patrimonio mediante el uso de sistemas informáticos por parte del agente (p. 71). Continúa señalando, de forma aún más concluyente: Sin perjuicio de la terminología que en definitiva se utilice, sea la de propiedad o la de patrimonio, el contenido y el alcance de estas expresiones son más generosas en su concepción y aplicación en la ley penal que en la civil. El ámbito y el alcance de tutela de este delito, en particular, son los intereses pecuniarios ajenos de carácter personal, es decir, esta norma penal es un típico modelo de una cláusula de protección de derechos individuales, en contraposición a la corriente supra-individual que se verifica en la actualidad en el derecho penal y en el penal económico (p. 76).

^{xc ii} Tema de enorme relevancia debido a que, al constatar que el bien jurídico protegido por el tipo penal de hurto por medios informáticos es el patrimonio económico y no la información y los datos, se pudo concluir que dicho tipo penal **no es un delito informático**. Puesto que, reiteramos, no atenta en contra de los sistemas informáticos o de la información allí contenida.

^{xc iii} El término "autor" es criticado por un sector de la Doctrina por cuanto parece llevar inmersa una adjudicación de responsabilidad penal. Así, Velasquez (2011) sintetiza esta crítica de la siguiente forma: "la equiparación entre sujeto activo y autor es, sin embargo, criticada por quienes aducen que la calidad de autor supone la responsabilidad penal, mientras que la de sujeto activo no" (p. 350)

^{xc iv} No obstante, existen tipos penales que utilizan la fórmula "el que" y aun así son de sujeto activo calificado. Ejemplo claro al respecto, son los delitos en contra de los Bienes y Personas Protegidas por el Derecho Internacional Humanitario, los cuales, a pesar de utilizar la fórmula "el que", sólo pueden ser cometidos, por regla general, por quien ostente la calidad de combatiente.

^{xc v} Según Tiedemann (1985) el dinero contenido en los bancos no es una "cosa" susceptible de apropiación. Por lo tanto, no podría darse el hurto por medios informáticos en los casos en los que se sustraigan los fondos depositados en las entidades financieras. Así lo afirma el autor: Éstas originan problemas penales específicos en materia de criminalidad mediante computadoras. Contrariamente a lo que ocurre con los sistemas penales de Francia y Suiza, la doctrina alemana dominante considera que el dinero en bancos o escrituras no constituye una «cosa», en el sentido de los parágrafos 242 y 246 del Código Penal. Por consiguiente, acreditar o adeudar un importe en una cuenta bancaria como resultado de un acto indebido y doloso no constituye hurto ni apropiación indebida. Además, dado que el autor se convierte en propietario de los importes acreditados, al serle abonados, las normas penales que protegen el derecho de propiedad no le son aplicables. Los problemas penales de la criminalidad mediante computadoras, por tanto, se concentran alrededor de los hechos punibles contra el patrimonio (en especial la estafa y el abuso de confianza), así como sobre las falsificaciones (de documentos y de reproducciones técnicas). (p. 132)

^{xc vi} En apoyo a esta afirmación, véase Palazzi (2000) cuando cita una jurisprudencia en Argentina en 1997: "Por su parte, el Tribunal Oral N°9," en un caso idéntico sostuvo que las conductas que analizamos debían ser consideradas bajo **el tipo penal de hurto**." (p. 113); En el mismo sentido, Hernández (2001) En síntesis, a juicio del suscrito, en el derecho chileno la obtención de dinero en cajeros automáticos por personas no autorizadas constituye en principio **hurto**. Por otra parte, entender tarjetas de acceso como llaves para los efectos del robo con fuerza resulta plausible en cuanto lo esencial del concepto radica en la idoneidad del instrumento para abrir del modo *normal* una cerradura, siendo indiferentes las características técnicas de una y otra." (p. 14); En contra, Palazzi (2000) cita otra jurisprudencia del mismo país dictada en 1996: "El Tribunal Oral N° 19 en el caso "Gómez Olivela", con una base fáctica similar, sostuvo que: "...medió un ardid

idóneo, tal como fue la obtención del plástico y código personal de 8...) para luego utilizarlo en las maniobras fraudulentas...". En base a tales consideraciones adoptó también la calificación de **estafa**" (p. 112).

^{xcvii} En apoyo a esta postura, por todos, ver: Miró (2012); Grajales (2014); Camacho (1987); Romeo Casabona (2006).

^{xcviii} Para una explicación detallada de la postura, ver *supra*: capítulo I, precisión terminológica, adopción del concepto de delito informático en sentido limitado.

^{xcix} Haciendo referencia a un precepto similar contenido en la legislación española, Davara (2007) señala: "No podemos hablar del delito de robo ya que, como sabemos, el robo exige, de acuerdo con lo especificado en el Código Penal (art. 237), apoderarse de las cosas muebles ajenas empleando fuerza en las cosas para acceder al lugar donde éstas se encuentran o violencia o intimidación en las personas. Evidentemente, no necesita más comentario, y está claro que la acción realizada por medios informáticos, en los que se accede a un programa o tratamiento de la información para llevarla a cabo, dista mucho de llevar aparejada violencia, intimidación o empleo de fuerza en las cosas. Sin embargo, el artículo 238 abre una puerta interpretativa favorable al indicar que «son reos del delito de fuerza en las cosas los que ejecuten el hecho» con la utilización de «llaves falsas», entendiendo como llaves (art. 239), «a los efectos del presente artículo», las «tarjetas magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia».

Además, cuando estas tarjetas, por ejemplo, contengan un chip o una banda magnética, con un procesamiento informático que efectúa la función de llave y permite su utilización como tal, tendrá un tratamiento especial respecto al delito y estaríamos -cosa impensable en la legislación penal anterior- ante un delito de robo -que exige fuerza en las cosas- cometido «limpiamente» por medios informáticos." (p. 387)

^c Meek (2013) va más allá y señala que el problema concursal se presenta respecto del término "seguridades electrónicas": "Por supuesto, dificultades adicionales genera también el artículo 240.4 porque, de ser estrictos, la conducta prevista en este dispositivo es básicamente la misma de la cual se ocupa el artículo en estudio (hurto por medios informáticos) lo cual obliga a acudir de nuevo al tipo más especial que pareciera ser el que se examina." (p. 121) Se trata de una postura errada, debido a que, los mecanismos de seguridad electrónica y los de seguridad informática no pueden ser por completo asimilables. Sin embargo, como se mencionó, sí existe un concurso aparente de tipos penales, pero únicamente respecto de la expresión "u otras semejantes" del artículo 240 numeral 4 del Código Penal colombiano.

^{ci} Proyecto de Ley No. 042 de 2007 Cámara y 123 de 2007 Senado. Gaceta del Congreso 528 de 2007.

^{cii} Ver ponencia de Parmenio Cuellar, publicada en la Gaceta No. 275 de 2008, en la cual sugiere el archivo de la iniciativa.

^{ciii} En contra de esta postura, y señalando la necesidad de la tipificación autónoma del hurto informático, véase Flores (2012) cuando afirma: A una conclusión muy similar arribó Flores (2012), cuando afirma: "En otros casos, sin embargo, el proceder del legislador puede resultar más discutible, bien por la nueva tipificación de conductas informáticas contra el patrimonio para las que habría bastado el tipo genérico (defraudaciones en el gasto de servicios de telecomunicaciones), bien por la ausencia de tipificación expresa de conductas que sí debían haber previsto la utilización de tecnología digital (insolvencias punibles, hurto informático, uso indebido de tarjetas de crédito). (P. 191-192)