Página inicial: 79 Página final: 88

LA TIPICIDAD DE LA REVELACIÓN DE SECRETOS INFORMÁTICOS

Alberto H. González Herrera*

Resumen:

La tipicidad contribuye a establecer claramente qué puede ser objeto de sanción jurídico-penal. La intimidad como uno de los derechos más importantes para el efectivo desarrollo de la persona, merece tutela; desde su proclama en la carta constitucional, se hace imperativo que el Derecho penal contribuya a su observancia plena. En el presente trabajo, la tipicidad de la revelación de secretos informáticos es examinada, la que por la legislación vigente propugna por la tutela de la misma por afectar la seguridad informática.

Palabras Clave:

Tipicidad; Delitos Informáticos; Derecho a la Intimidad; Derecho Positivo; Protección de Datos Personales.

Abstract:

Typification contributes to clearly establish the actions which may be subjected to a criminal legal action. Intimacy, as one of the most important rights for personal development, deserves protection; and since its proclamation in the Constitution, criminal law must contribute to its protection. This article examines the typification of the disclosure of computerized confidential information, since the current legislation advocates for its protection.

Keywords:

Typification; Cybercrime; Right to Intimacy; Positive Law; Personal Data Protection.

Sumario:

*Licenciado en Derecho y Ciencias Políticas por la Universidad de Panamá. Docente de la Universidad de Panamá y defensor de oficio del Instituto de Defensoría de Oficio de Panamá. Actualmente es candidato a Doctor en Derecho Penal y Criminología de la Universidad Pablo de Olavide Sevilla – España. Ha ocupado diversos cargos en la Rama Judicial de Panamá. E-mail: agonzalezherrera26@yahoo.com

I. Aspectos Generales.

a. La Tipicidad.

La tipicidad supone que el legislador ha considerado delito la conducta que lesiona o pone en peligro intereses o bienes de relevancia para la sociedad. El artículo 2 del Código penal panameño de 2007 indica: "En este Código sólo se tipifican aquellas conductas y comportamientos cuya incriminación resulte indispensable para la protección de bienes jurídicos tutelados y los valores significativos para la sociedad, y de acuerdo a la política criminal del Estado." Por su parte, claramente exponía el insigne maestro REYES ECHANDÍA que la tipicidad es: "Fenómeno en virtud del cual el legislador concreta en normas legales aquellos comportamientos humanos que considera lesivos de intereses jurídicos fundamentales y predicables del individuo, de la sociedad y del propio Estado.[1]" A la vez, el impulsor del funcionalismo penal JAKOBS sostiene: "...se pone de manifiesto que no cualquier objeto de regulación de una norma es un bien jurídico, sino sólo aquel que ha de desempeñar alguna función para la sociedad o para uno de sus subsistemas, incluido el ciudadano.[2]" El catedrático de Derecho Penal de la Universidad de Panamá, MUÑOZ POPE señala: "Misión fundamental de la tipicidad, por tanto, es describir todos los elementos esenciales del comportamiento punible, de modo que si no se describe tal cual comportamiento, punible, el mismo será impune toda vez que no se adecua a un tipo en particular.[3] Actualmente, apunta FERNÁNDEZ CARRASQUILLA, que la doctrina plantea la existencia o no de injusto penal, y que no es posible el mismo sin afectación real al bien jurídico.[4]

La Constitución Política de la república de Panamá, dispone en el artículo 3, lo siguiente: Sólo serán penados los hechos declarados punibles por Ley anterior a su perpetración y exactamente aplicable al acto imputado."

Por ende, en Panamá, el mandato de determinación o de tipicidad de los delitos, como en otros países, requiere que la conducta sea previamente descrita en forma expresa y taxativa por la ley, como delito, para que pueda ser objeto de sanción luego de su realización.[5]

[1] REYES ECHANDÍA, Alfonso, Diccionario de Derecho penal, 5ª edición, Temis, Bogotá, 1990, p. 45.

[2] JAKOBS, Gunther, Derecho Penal, Parte general, Fundamentos y teoría de la imputación, Marcial Pons, Madrid, 1995, p. 52.

[3] MUÑOZ POPE, Carlos Enrique, Teoría del Hecho Punible, Inédito, Panamá, 2000, p. 39.

[4] FERNÁNDEZ CARRASQUILLA, Juan, Derecho penal liberal de hoy, Introducción a la dogmática axiológica jurídico penal, Gustavo Ibañez, Bogotá, 2002, p. 167.

[5] El inciso segundo del artículo 29 de la Constitución colombiana lo acoge: "Nadie podrá ser juzgado sino conforme a leyes preexistentes al acto que se le imputa, ante juez o tribunal competente y con observancia de la plenitud de las formas propias de cada juicio." El artículo 39 de la Constitución costarricense destaca: "A nadie se hará sufrir pena sino por delito, cuasidelito o falta, sancionados por ley anterior y en virtud de sentencia firme dictada por autoridad competente, previa oportunidad concedida al indiciado para ejercitar su defensa y mediante la necesaria demostración de culpabilidad." La Constitución dominicana en el artículo 40.13 establece: "Nadie puede ser condenado o sancionado por acciones u omisiones que en el momento de producirse no constituyan infracción penal o administrativa." El artículo 25.1 de la Constitución española señala: " Nadie puede ser condenado o sancionado por acciones u omisiones que en el momento de producirse no constituyan delito, falta o infracción administrativa, según la legislación vigente en aquel momento." El artículo 15 del Pacto internacional de derechos civiles y políticos expone: "1. Nadie será condenado por actos u omisiones que en el momento de cometerse no fueran delictivos según el derecho nacional o internacional. Tampoco se impondrá pena más grave que la aplicable en el momento de la comisión del delito. Si con posterioridad a la comisión del delito la ley dispone la imposición de una pena más leve, el delincuente se beneficiará de ello. 2. Nada de lo dispuesto en este artículo se opondrá al juicio ni a la condena de una persona por actos u omisiones que, en el momento de cometerse, fueran delictivos según los principios generales de derecho reconocidos por la comunidad internacional." La Convención americana sobre Derechos humanos en el artículo 9 indica: "Principio de Legalidad y de Retroactividad Nadie puede ser condenado por acciones u omisiones que en el momento de cometerse no fueran delictivos según el derecho aplicable. Tampoco se puede imponer pena más grave que la aplicable en el momento de la comisión del delito. Si con posterioridad a la comisión del delito la ley dispone la imposición de una pena más leve, el delincuente se beneficiará de ello."

De esa previsión típica, se genera una triple función según MUÑOZ CONDE, a saber:

> "a. Una función seleccionadora de los comportamientos humanos penalmente relevantes.
>
> b. Una función de garantía, en la medida en que sólo los comportamientos subsumibles en él pueden ser sancionados penalmente.
>
> c. Una función motivadora general, ya que, con la descripción de los comportamientos en el tipo penal, el legislador indica a los ciudadanos qué comportamientos están prohibidos y espera que, con la conminación penal contenida en los tipos, los ciudadanos se abstengan de realizar la conducta prohibida."[6]

La tipicidad o precisión del injusto penal, reviste mucha importancia, al punto que la Corte interamericana de Derechos humanos, en el año 1999, en el caso de Castillo Petruzzi y otros contra la república de Perú haya sostenido lo siguiente: "La Corte entiende que en la elaboración de los tipos penales es preciso utilizar términos estrictos y unívocos, que acoten claramente las conductas punibles, dando pleno sentido al principio de legalidad penal. Este implica una clara definición de la conducta incriminada, que fije sus elementos y permita deslindarlas de comportamientos no punibles o conductas ilícitas sancionables con medidas no penales. La ambigüedad en la formulación de los tipos penales genera dudas y abre el campo al arbitrio de la autoridad, particularmente indeseable cuando se trata de establecer la responsabilidad penal de los individuos y sancionarlas con penas que afectan severamente bienes fundamentales, como la vida o la libertad."[7]

Pues bien, orientada la determinación de conductas punibles por el mandato de determinación, tenemos que la tutela o protección recaerá sobre valores fundamentales conocidos como bienes jurídicos, cuyo reconocimiento está contenido en la Constitución.[8]

b. El Derecho a la Libertad Informática.

La vida actual se caracteriza por hacer un uso continuo y permanente de la tecnología; desde las redes de sistemas computacionales que operan en todas las empresas, cadenas comerciales, entes estatales y en la internet, hasta dispositivos y equipos portátiles de comunicación como teléfonos móviles y ordenadores portátiles. En estos instrumentos y en los buzones de correos electrónicos, se suele almacenar gran cantidad de documentos y datos sobre trámites mercantiles, laborales, sociales y personales. Estos últimos, deben manejarse con suma diligencia y cuidado por parte de quienes manejan en un momento dado los mismos, a fin de no afectar ni lesionar a nadie en su honra, patrimonio, imagen e intimidad.

Sobre este último precisa FROSINI, el derecho al secreto o reserva a la intimidad es: "...el derecho personal a mantener inviolada la propia esfera de vida íntima en una sociedad como la tecnológica, en la cual todo se vuelve objeto de información."[9] Al respecto, PÉREZ LUÑO afirma: "Esta proyección de los efectos del uso de la informática sobre la identidad y dignidad humanas, incide también en el disfrute de los valores de la libertad y la igualdad."[10]

[6] MUÑOZ CONDE, Francisco, Teoría general del delito, 4ª. edición, Valencia, 2007, p. 56.

[7] Citado por REMOTTI CARBONELL, José Carlos, La Corte interamericana de Derechos humanos, estructura, funcionamiento y jurisprudencia, Barcelona, 2003, p. 326.

[8] ROXIN, Claus, Derecho penal, parte general, Tomo I, Fundamentos. La estructura de la teoría del delito, Civitas, Madrid, 2006, Pp. 57-58.

[9] FROSINI, Vittorio, Informática y Derecho, Temis, Bogotá, 1988, p. 22.

[10] PÉREZ LUÑO, Antonio, "Intimidad y Protección de Datos personales: Del Habeas Corpus al Habeas Data" en Estudios sobre el Derecho a la Intimidad, Tecnos, Madrid, 1992, p. 40.

Como quiera que la era informática con sus avances ha impactado la vida de todos, ha tenido que considerarse el derecho a la libertad informática, que FROSINI define como: "el derecho a poder disponer de los datos de información personal propios y, por tanto, a permitir o rehusar su uso por parte de las agencias de información que manejan los bancos de datos; derecho a controlar la veracidad de los datos, el acceso a su conocimiento por parte de terceros, el uso que de ellos se haga con finalidades sociales, económicas, políticas."[11]

A continuación se examinará el orden punitivo panameño para comprobar si es precisa y conveniente la tipificación de las conductas que implican la revelación de secretos informáticos.

II. Tipicidad o Atipicidad en la Revelación de Secretos Informáticos.

a. Consideraciones Previas.

Como ya advertimos, la tipicidad implica que una conducta es considerada delito, se encuentra descrita en la ley penal, y, ello, es previo a la realización del acto que se estima lesivo al interés o bien jurídico protegido. En tanto, la atipicidad es la falta de consideración como delito por parte de la ley penal de una conducta. Es la no adecuación del hecho, a los presupuestos contenidos en la ley. FERNÁNDEZ CARRASQUILLA refiere de la atipicidad que: "En general se habla de ella cuando el hecho externo que se imputa en un caso determinado no está previsto como delito por la ley, es decir, ni siquiera genéricamente y en abstracto se acomoda a un tipo de injusto,..."[12]

Antes de abordar el delito de revelación de secretos, es conveniente reconocer lo que significan los vocablos "revelación" y "secretos". La voz revelación en uno de los significados que contempla el Diccionario de la Lengua Española significa:"Manifestación secreta y oculta."[13] Mientras que el secreto conforme al Diccionario de la Lengua Española es: "Lo que cuidadosamente se tiene reservado y oculto."

Los secretos constituyen una de las manifestaciones del derecho a la intimidad, y sobre ellos destaca JIJENA LEIVA: "...como pilar fundamental está el secreto o reserva (secreto absoluto), conjuntamente con el derecho al control de la utilización y circulación de la información que sobre su persona ha sido confiado a un tercero (secreto relativo), la tranquilidad o ausencia de perturbación física o psicológica y la autonomía."[15]

Por consiguiente, los datos personales que se manejen en un sistema computacional o base de datos no pueden tratarse a la ligera, porque podrían causar perjuicios graves e irreparables a sus titulares si dichos datos llegaren a conocimiento del público sin su consentimiento o autorización.

Además, los secretos o datos personales que de cada persona son manejados a diario por el Estado, los bancos, las tiendas, los centros médicos, los hospitales, los hoteles, los centros de diversión

[11] FROSINI, Ob. Cit. p. 23.
[12] FERNÁNDEZ CARRASQUILLA, Juan, Derecho Penal Fundamental, Tomo II, Segunda edición, Temis, Bogotá, 1998, p. 321.
[13] DICCIONARIO DE LA LENGUA ESPAÑOLA, Real Academia Española, Tomo II, 21º edición, Madrid, 1992, p.1792.
[14] Ibídem, p.1853.
[15] JIJENA LEIVA, Renato Javier, La protección penal de la Intimidad y el Delito Informático, Editorial Jurídica de Chile, Santiago, 1992, p. 42.

y demás sitios de concurrencia pública, no pueden escapar a una regulación o restricción legal y es necesario limitar su utilización, para evitar que por mal empleo de los mismos, seamos afectados si se dispone de ellos sin nuestra autorización.

Antes de verificar si es típica la revelación de secretos informáticos en la legislación panameña, trataremos de precisar lo que es el delito informático, el cual guarda relación directa con el objeto de estudio.

b. Concepto de Delito Informático.

La doctrina sobre el tema no adopta una posición uniforme en cuanto al concepto de delito informático, y, mucho menos, en cuanto a la tipificación de la revelación de secretos informáticos.

La Organización para la Cooperación Económica y el Desarrollo (OCDE) lo define como: "...cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el proceso automático de datos y las transmisiones automáticas de datos."[16]

OSSA ROJAS se refiere al delito informático como: "...cualquier conducta ilegal, no ética o no autorizada atentatoria tanto contra bienes propiamente informáticos como tradicionales, que se realice mediante el uso y/o la aplicación de tecnologías informáticas."

Sin ahondar en múltiples concepciones, consideramos que el delito informático es un hecho que se realiza vulnerando los sistemas de seguridad de una o varias unidades de una red computacional, mediante el empleo de un ordenador o de una computadora personal, con el fin de utilizarla como medio de ejecución de un delito convencional u obtener de la base de datos de dicha red, la información que sobre un tema, una actividad o varios sujetos reposa en el mismo.

c. La Revelación de Secretos en la Legislación Panameña.

El jus puniendi se utiliza para evitar la lesión de bienes jurídicos o de derechos fundamentales como el derecho a la intimidad, que es uno de los derechos que permiten la realización y satisfacción de necesidades de las personas.

Sin embargo, pese a que la Constitución política reconozca tácitamente el derecho a la intimidad personal, ni en el texto de Código penal derogado ni en el nuevo Código penal de 2007, se cuenta con Título o un capítulo dentro del Libro segundo que prevea su completa tutela. No obstante, existen algunos tipos penales que en forma dispersa e indirecta la protegen.

Preceptúa el artículo 29 de la Constitución panameña lo siguiente: "La correspondencia y demás documentos privados son inviolables y no pueden ser examinados ni retenidos, sino por mandato de autoridad competente y para fines específicos, de acuerdo con las formalidades legales. En todo caso, se guardará absoluta reserva sobre los asuntos ajenos al objeto de examen o de la retención.

El registro de cartas y demás documentos o papeles se practicará siempre en presencia del interesado o de una persona de su familia o, en su defecto, de dos vecinos honorables del mismo lugar.

[16] Citado por RIQUERT, Marcelo Alfredo, "Delitos informáticos" en www.delitos informáticos.com.

[17] Ibídem.

Todas las comunicaciones privadas son inviolables y no podrán ser interceptadas o grabadas, sino por mandato de autoridad judicial.

El incumplimiento de esta disposición impedirá la utilización de sus resultados como pruebas, sin perjuicio de las responsabilidades penales en que incurran los autores."

Como bien jurídico, la intimidad también encuentra respaldo en el artículo 17 del Pacto internacional de Derechos Civiles y políticos que preceptúa:

"1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

La Convención Americana sobre Derechos humanos, de igual forma, estima la intimidad como elemento integrante de los derechos fundamentales a la honra y la dignidad humana, al disponer en el artículo 11 lo siguiente: "Protección de la Honra y de la Dignidad.

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

Si bien estas normas no hacen referencia a la intimidad informática o derecho al secreto informático, al abarcar los derechos personales a la privacidad, a la inviolabilidad del domicilio y a la correspondencia, se deben extender a la esfera o ámbito de las tecnologías como la informática, bases de datos digitales o de correos electrónicos, para no dejar desprotegidos a los ciudadanos. Pero, ¿qué se entiende entonces, por secretos informáticos? Los secretos informáticos comprenderán aquellos informes que reposan en un banco de datos, en un sistema computacional o dirección de correo electrónico, donde constan detalles particulares de una persona natural o jurídica, de una actividad estatal, de una empresa, de una organización no gubernamental, de una institución pública o privada, de una representación diplomática, entre otros. Tenemos entonces, que todo secreto revestirá el carácter de informático si se encuentra contenido no sólo en una base de datos o sistema informático, sino también en los mensajes de correo electrónico y en los dispositivos o memorias de almacenamiento portátiles como los USB, los discos compactos, entre otros.

1. Código Penal de 1982

El derogado Código Penal de 1982, en su momento inspirado en el Código penal tipo para Iberoamérica, a diferencia de los códigos modernos, aprobados en el último decenio del siglo pasado, no contempló un título o capítulo dedicado a los delitos contra la intimidad, sin embargo, en el Título II de los delitos contra la libertad, tanto en el capítulo III de los delitos contra la libertad individual, como en el capítulo V de los delitos contra la inviolabilidad del domicilio y en el capítulo VI de los delitos contra la inviolabilidad del secreto, tutelan en forma tímida, los secretos y el derecho personal a la

intimidad. Del examen de estos tipos penales, advertimos que las únicas conductas en las cuales podrían subsumirse las violaciones o afectaciones a los secretos informáticos, serían las contenidas en el capítulo VI de los delitos contra la inviolabilidad del secreto, Título II de los delitos contra la libertad. En virtud de ello, el secreto, como bien jurídico tutelado, forma parte de la libertad personal del individuo, que puede resultar afectada o menoscabada, si una persona conocedora de sus datos o información, por razón del empleo que realiza, termina descubriéndolos o dándolos a conocer sin consentimiento previo. Por un lado, el artículo 170 tipifica la divulgación de secretos a quienes por razón de su oficio, empleo, profesión o arte, tenga conocimiento de los mismos y los revele sin autorización de su titular. Al no hacer la norma referencia a la forma como llega a conocimiento del sujeto activo la noticia de secretos, ni el tipo de secretos, da lugar a que pueda subsumirse la violación de secretos informáticos si la lleva a cabo algún sujeto en el desempeño de su oficio, empleo, profesión o arte.[18] Parece que el sujeto activo al entrar en conocimiento de secretos, cuya publicación puede causar daño y los revela sin consentimiento del afectado o sin necesidad de salvaguardar un interés superior. La calidad de servidor público servía como circunstancia agravante de responsabilidad penal si se incurría en el tipo, aprovechándose del acceso a la información para alguna medida relativa a la medida de prevención de del delito de blanqueo de capitales.

A pesar del importante objeto de tutela, la norma no resultó aplicada, constituyendo como otros tipos penales, una mera legislación simbólica. Así mismo, el artículo 171-A del Código penal, prevé la sanción por la divulgación de la información que tenga una persona por conocimiento en el ejercicio de sus funciones; la norma dispone: "El servidor público o el particular que como empleado, directivo o miembro de una junta u órgano de administración de cualquier entidad pública o privada en que el Estado tenga participación económica, haga uso indebido de información que haya conocido por razón o con ocasión de sus funciones, con el fin de obtener provecho para sí o para un tercero, incurrirá en prisión de 2 a 6 años e inhabilitación para ejercer funciones públicas por el mismo término de la pena principal." Este precepto introduce por vez primera en Panamá, una figura parecida al "insider trading" o abuso de información privilegiada.

Conviene destacar que la doctrina reconoce otras conductas no tipificadas que afectan los secretos informáticos como: "la introducción de datos falsos (data diddling) en bancos de datos personales; la fuga de datos (data leakage) o revelación dolosa de informaciones concernientes a la vida personal, familiar o del patrimonio económico o individual; el uso de llaves maestras (superzapping) o utilización de programas no autorizados con la finalidad de modificar, destruir, copiar, insertar, o impedir el uso de datos archivados en los sistemas de información; y el intrusismo informático."[19] Las conductas mencionadas son solamente algunas de las nuevas manifestaciones delictuales que se vienen dando en el mundo y que tienen repercusiones de magnitudes insospechadas en la esfera de la intimidad, la economía y la seguridad informática.

---

[18]Dispone el artículo 170 lo siguiente: "El por razón de su oficio, empleo, profesión o arte, tenga noticia de secretos cuya publicación pueda causar daño y los revele sin consentimiento del interesado o sin que la revelación fuere necesaria para salvaguardar un interés superior, será sancionado con prisión de 10 meses a 2 años o de 30 a 10 días-multa, e inhabilitación para ejercer tal oficio, empleo, profesión o arte, hasta por 2 años.

La sanción antes descrita será aumentada al doble, cuando el que viole el secreto sea un servidor público que haya tenido acceso a la información, en razón de una de las medidas de prevención del delito de blanqueo de capitales previstas por la ley."

[19]CASTRO OSPINA, Sandra Jeannette, Delitos Informáticos, www.delitosinformaticos.com/delitos/colombia2.shtml, 2002.

2. Código Penal de 2007

A diferencia del texto anterior, el nuevo Código Penal panameño, vigente desde el 23 de mayo de 2007 (Texto único, G.O. D. Nº26519 de lunes 26 de abril de 2010), en el Título VII de los Delitos Contra Seguridad Jurídica de los Medios Electrónicos, en el Capítulo I, establece los denominados Delitos contra la Seguridad informática. En cuatro artículos que van del artículo 289 al artículo 292, se contempla más allá de los secretos y la intimidad, conductas dirigidas a proteger las bases de datos, redes, programas y sistemas informáticos.

Destaca GUERRA de VILLALAZ que el objeto de protección es: "...la seguridad informática que comprende la protección a la privacidad, a la fe pública, a la economía, a la propiedad intelectual, a las comunicaciones, los medios de transporte y la seguridad pública."[20]

El artículo 289 prohíbe el ingreso indebido o la utilización indebida de base de datos, red o sistema informático, se prevé la pena de dos a cuatro años de prisión. Preceptúa dicho precepto: "Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenido en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión será sancionado con dos a cuatro años de prisión."

El sujeto activo puede resultar cualquier persona, no exige una calidad especial, basta con que realice uno de los verbos rectores. La penalidad es única y no presenta alternativas.

Así mismo, el artículo 290 sanciona el apoderamiento indebido, la copia, la utilización o la modificación de los datos en tránsito (vía correo electrónico) o contenidos en una base de datos o sistema informático, que los interfiera, los intercepte, los obstaculice o impida su transmisión. La sanción prevista va de dos a cuatro años de prisión.

Las conductas anteriores conforme al artículo 291, implican aumento a las penas de una tercera a una sexta parte si se cometen afectando los datos que estén contenidos en bases de datos o sistemas informáticos de: oficinas públicas; instituciones públicas, privadas o mixtas que prestan un servicio público; bancos, aseguradoras, y demás instituciones financieras y bursátiles; si se cometen con fines lucrativos. Estas sanciones se pueden aplicar sin perjuicio que los datos sean de información confidencial, acceso restringido, referente a la seguridad del Estado, según lo dispuesto en el Capítulo I, Título XIV del Libro Segundo del Código penal. Lo antes visto constituye una condición objetiva de punibilidad de la circunstancia agravante, al prever un sujeto pasivo específico o un fin concreto (lucro).

Establece el artículo 292 que si las conductas las perpetra un sujeto activo con calidad de encargado o responsable de la base de datos o sistema informático. Si la persona autorizada para acceder a estos datos, al sistema o a la red, lo hacía por su posición actúa en forma similar a quien ostenta la información privilegiada (ejemplo del insider trading), la sanción se agravará entre una sexta y una tercera parte.

Sobre estas modalidades delictivas advierte MUÑOZ CONDE: "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 solo se limiten a las

[20]GUERRA de VILLALAZ, Aura E., Compendio de Derecho penal, parte especial, Chen, Panamá, 2010, p. 254.

consistentes en apoderamiento, utilización o modificación de los datos, sino que incluyen también el acceso a los mismos."[21]

Es necesario, que a corto plazo se capaciten tanto a investigadores como juzgadores en torno a la ejecución y consumación de este tipo de conductas que ya están dando mucho que hacer a nivel supranacional y urge adoptar estrategias conjuntas entre los países para combatirlas.

III. Conclusiones.

La nueva legislación penal panameña, en materia de delitos contra la inviolabilidad del secreto es insuficiente para frenar las nuevas modalidades de delitos cometidos en la esfera informática.

Urge la adopción de una ley de protección de datos personales, que tutele eficazmente la garantía fundamental del derecho a la intimidad personal.

La tipificación de los delitos que evitan la revelación de los secretos informáticos es de vital importancia para la seguridad de la economía, el Estado y la intimidad.

[21] MUÑOZ CONDE, Francisco, Derecho penal, parte especial, 15a. edición, Tirant lo Blanch, Valencia, 2004, p. 263.

Bibliografía

CASTRO OSPINA, Sandra Jeannette, "Delitos Informáticos" (2002), disponible en: ‹http://www.delitosinformaticos.com/delitos/colombia2.shtml›

DICCIONARIO DE LA LENGUA ESPAÑOLA. Real Academia Española, Tomo II, Vigésima primera edición, Madrid, 1992.

FERNÁNDEZ CARRASQUILLA, Juan. Derecho Penal Fundamental, Tomo II, Segunda edición, Temis, Bogotá, 1998.

_____. Derecho Penal Liberal de Hoy, Introducción a la dogmática axiológica jurídico penal, Gustavo Ibañez, Bogotá, 2002.

FROSINI, Vittorio. Informática y Derecho, Temis, Bogotá, 1988.

GUERRA de VILLALAZ, Aura E. Compendio de Derecho penal, parte especial, Chen, Panamá, 2010,

JAKOBS, Günther. Derecho Penal, Parte general, Fundamentos y teoría de la imputación, Marcial Pons, Madrid, 1995.

JIJENA LEIVA, Renato Javier. La protección penal de la Intimidad y el Delito Informático, Editorial Jurídica de Chile, Santiago, 1992.

MUÑOZ CONDE, Francisco. Derecho penal, parte especial, 15a. edición, Tirant, Valencia, 2004.

MUÑOZ CONDE, Francisco. Teoría general del delito, 4ª. edición, Valencia, 2007.

MUÑOZ POPE, Carlos Enrique. Teoría del Hecho Punible, Inédito, Panamá, 2000.

PÉREZ LUÑO, Antonio. "Intimidad y Protección de Datos personales: Del Habeas Corpus al Habeas Data" en Estudios sobre el Derecho a la Intimidad, Tecnos, Madrid, 1992.

REMOTTI CARBONELL, José Carlos. La Corte interamericana de Derechos humanos, estructura, funcionamiento y jurisprudencia, Barcelona, 2003.

REYES ECHANDÍA, Alfonso. Diccionario de Derecho penal, 5ª edición, Temis, Bogotá, 1990.

RIQUERT, Marcelo Alfredo. "Delitos informáticos" en ‹http://www.delitos informáticos.com›

ROXIN, Claus. Derecho penal, parte general, Tomo I, Fundamentos. La estructura de la teoría del delito, Civitas, Madrid, 2006.