CAPÍTULO I

FINALIDAD DE LA LEY DE CIBERCRIMEN

1. BIENES JURÍDICOS TUTELADOS

El espíritu del Proyecto de Ley de Delitos Informáticos o Cibercrimen, identificado con el número 4055 del Congreso de la República, entendido éste como la "*ratio legis*"[9], lo encontramos en la parte considerativa de la misma, en la cual se establece que es necesario proteger lo siguiente:

a. Los derechos de la persona en cuanto a la *integridad, disponibilidad* y *confidencialidad* de los sistemas que utilicen tecnologías de la información y sus componentes, a fin de garantizar certeza jurídica en las transacciones propias del comercio electrónico y, así, armonizar y contribuir con las disposiciones internacionales relacionadas con la prevención y sanción de los delitos informáticos.

---

9 DU PASQUIER, Claude, Introducción al Derecho, Editorial Jurídica Portocarrero S.R.L. 5ta edición. Traducción del francés por Julio Ayasta González. Lima, Perú. 1994. Pág.151. Este autor afirma que "según el punto de vista en que uno se coloque, la *ratio legis* puede ser considerada como el fin realmente querido por el legislador en la época de elaboración de la ley..."

b. Contrarrestar los ataques cibernéticos de conformidad con la normativa nacional e internacional.

Fundamentalmente, del análisis del contenido del citado Proyecto de Ley, entendemos por bienes jurídicos tutelados los siguientes:

1.1 La información: Se protege la información en cuanto a sus atributos consistentes en la integridad, disponibilidad y confidencialidad.

1.2. El Patrimonio: Se protege el patrimonio toda vez que se sancionan todos aquellos actos de transferencia patrimonial no consentida por el propietario, así como lo relativo al daño informático.

Así también, se incluyen normas relativas a la seguridad del Estado, y se regulan delitos contra el pudor y el honor de las personas.

Es importante que los Estados pongan la debida atención a los asuntos de ciberseguridad, toda vez que los ataques cibernéticos pueden afectar a la infoestructura estratégica de los Estados relacionada con: sector de electricidad, transporte, financiero, telecomunicaciones, suministro de agua, entre otros. Los delitos cibernéticos pueden trascender el mundo virtual y afectar en el mundo físico, como lo hemos visto cuando un *malware* denominado "*stuxnet*" fue capaz de crear una alteración en el mundo físico con relación a las centrífugas de enriquecimiento de uranio en la planta iraní de Natanz. Para no pensar en asuntos que podrían parecer extremos, pensemos en que, por medio de un ataque cibernético, se podría alterar la red de control de semáforos de una ciudad o

el sistema financiero de un país. Por ello la importancia de crear una regulación de protección de los bienes jurídicos tutelados antes indicados.

2. ÁMBITO DE APLICACIÓN DE LA LEY

Se vuelve compleja la aplicación de una normativa que sanciona actos realizados en un espacio virtual o, que en la jerga cibernauta, se denomina "*ciberespacio*", debido a que no constituye un espacio físico o geográfico. Marc Goodman define al ciberespacio diciendo que: "*se trata de un ambiente intangible; no es un mundo de átomos y células, sino digital. Los bytes no tienen peso, olor ni color y viajan a la velocidad de la luz.*"[10]

La Internet, entendida como una red informática mundial utilizada como un medio internacional de comunicación, no tiene límites políticos; sin embargo, todos los actos realizados a través de esa red no deben vulnerar los derechos de las personas, tales como la propiedad, la dignidad o el honor, entre otros, ni entrañar violación de la ley, la moral o las buenas costumbres.

El autor, Ramón Gerónimo Brenna, al comentar sobre la Internet explica que: ésta consiste en un espacio no territorial, no geográfico y que, por su sola existencia genera interrogantes y problemas al mundo legal conocido, fuertemente atado a lo geográfico por la cuerda de las soberanías.[11]

---

10 GOODMAN MARC, Cibercriminalidad. Instituto Nacional de Ciencias Penales. México 2003, pag. 8.

11 BRENNA RAMÓN, Informática y Derecho, Buenos Aires, 2001, pág. 37.

Al final de cuentas, Internet es una red de informática mundial que se utiliza como un "***medio de comunicación***", formada, tal como la define el Diccionario de la Real Academia Española, por la conexión directa entre computadoras u ordenadores, mediante un protocolo especial de comunicación.

Debe tenerse presente que, jurídicamente, *territorio* no es sinónimo de *espacio geográfico*, debido a que el territorio comprende todos los lugares a los que se extiende la soberanía del Estado, lo que debe incluir las redes, sistemas y ordenadores vinculados al Estado de Guatemala.

Consideramos que, para los efectos del presente trabajo, no es conveniente profundizar en la interminable discusión de los alcances extensivos de la soberanía del Estado sobre la Internet, o sobre la existencia de una "*soberanía digital*", que algunos atribuyen a los Estados, debido a las asignaciones de dominios para cada país (lo cual, a nuestro juicio, no puede utilizarse como referencia para establecer límites en esta materia). Algunos Estados como Colombia, por ejemplo, han declarado que los dominios con el sufijo de su país (por ejemplo: ***.co*** para Colombia, ***.gt*** para Guatemala) constituyen bienes de ***interés público***, para que los mismos no sean comercializados, por considerar que identifican a un país o región.

Lo que realmente trasciende, en la esfera jurídica, es la determinación del lugar de **origen** y de **producción** de las consecuencias jurídicas del acto ilícito, debido a que, esos lugares, sí constituyen parte de un espacio territorial, donde existen normas de Derecho emanadas por el Estado a través de un ente legislativo. El único aspecto que sí merece atención, en cuanto a los límites de la soberanía de un Estado, es cuando un investigador, por sus buenos oficios, profundiza en las redes o sistemas de otro Estado; por

ejemplo, a raíz de la investigación de un ataque cibernético, DDoS (Ataque de Denegación de Servicio Distribuido), que en ocasiones utiliza *botnets* (*malware*), el investigador debe accesar a sistemas o redes que pueden estar ubicados en otro territorio. Todos estos inconvenientes podrían solucionarse con una adecuada normativa en materia de "cooperación internacional" o "asistencia jurídica mutua", tal como se indica más adelante.

El concepto de Ciberespacio no debe crear confusión en cuanto a la determinación del lugar de origen del delito o del lugar donde surte sus efectos. Internet tiene, obligadamente, una infraestructura física ubicada en determinado lugar, y es precisamente en ese lugar de ubicación donde podemos establecer el origen del delito o sus consecuencias.

Dentro de la Teoría General de la Ley Penal, que nuestro Código Penal regula, específicamente en los artículos 4 y 5, y que constituye el ámbito espacial de validez de la ley penal, se estudia el ámbito de aplicación de la ley por actos realizados dentro y fuera del territorio nacional, por parte de autores o cómplices, como una manifestación de la soberanía del Estado.[12]

12 El artículo 4 del Código Penal de Guatemala, Decreto 17-73 del Congreso de la República, regula la "***territorialidad de la ley penal***", de la forma siguiente: "Salvo lo establecido en tratados internacionales, este Código se aplicará a toda persona que cometa delito o falta en el territorio de la República o en lugares o vehículos sometidos a su jurisdicción." Asimismo, el artículo 5 del mismo cuerpo legal, al regular la "***extraterritorialidad de la ley penal***" establece: "Este Código también se aplicará: 1º. Por delito cometido en el extranjero por funcionario al servicio de la República, cuando no hubiere sido juzgado en el país en el que se perpetró el hecho. 2º. Por delito cometido en nave, aeronave o cualquier otro medio de transporte guatemalteco, cuando no hubiere sido juzgado en el país en el que se cometió el delito. 3º Por delito cometido por guatemalteco, en el extranjero, cuando se hubiere denegado su extradición. 4º. Por delito cometido en el extranjero contra guatemalteco, cuando no hubiere sido juzgado en el país de su perpetración, siempre que hubiere acusación de parte o del Ministerio Público y el imputado se hallare en Guatemala. 5º. Por delito que, por tratado o convención, deba sancionarse en Guatemala, aun cuando no

En ese sentido, en materia de Delitos Informáticos o Cibercrimen, debe tomarse en consideración el siguiente ámbito de aplicación de la ley:

2.1 Cuando el sujeto activo origina u ordena la acción delictiva dentro del territorio nacional. En este caso, el sujeto activo se ubica dentro del territorio nacional y origina la acción delictiva haciendo uso de redes y sistemas que utilizan tecnologías de la información, independientemente del lugar en el cual surta efectos.

En este caso, corresponderá a los expertos o peritos que participen en la investigación criminal, con la colaboración de los respectivos proveedores de servicio de Internet, determinar el lugar físico en el cual se originó la acción delictiva. Actualmente, la ubicación del lugar físico se podría establecer por diferentes métodos o formas de seguir el trazo o ruta utilizada por el perpetrador, pudiendo ser mediante un informe de la IP, utilizada en el caso concreto.[13]

hubere sido cometido en su territorio. 6º Por delito cometido en el extranjero contra la seguridad del Estado, el orden constitucional, la integridad de su territorio, así como falsificación de la firma del Presidente de la República, falsificación de moneda o de billetes de banco, de curso legal, bonos y demás títulos y documentos de crédito."

13 Cisco Certified Network Associate, quinta edición, pág. 86. Indica que una dirección **IP** es un número identificador designado a cada computador en una red, ésta designa de forma específica la localización de este computador dentro de la red. Una dirección IP es una dirección lógica no física, y es usada para localizar *hosts* (*) locales en la red. Una dirección IP, fue diseñada para permitir, a un *host* en una red, comunicarse con un *host* de una red diferente. Una dirección IP, está dividida en 32 bits de información. Estos *bits,* a su vez, son subdivididos en cuatro secciones referidos como octetos o *bytes*, cada uno contiene un *byte* (8 bits). Se puede designar una dirección IP por uno de tres métodos: por **notación decimal** (172.16.16.30.56), de **forma binaria** (10101 100.00010000.00011110.00111000) o de **forma hexadecimal** (AC.10.1E.38). Todos estos ejemplos representan la misma dirección IP. La ventaja de utilizar 32 bits para una dirección IP, es que permite una estructura de direcciones jerárquica y un largo número de direcciones, cerca de 4.3 billones.

2.2 Cuando el sujeto activo origina u ordena la acción delictiva desde el extranjero, produciendo efectos en el territorio nacional. En este caso, la acción delictiva opera a la inversa del caso anterior, surtiendo efectos en el territorio nacional. Como ejemplo de este caso sería, cuando se conozca de una acción delictiva de fraude informático originada en el extranjero, pero afectando patrimonio ubicado en el territorio nacional.

2.3 Cuando el origen o los efectos de la acción se produzcan en el extranjero, utilizando medios que se encuentren en el territorio nacional. En este caso, el origen o los efectos de la acción delictiva se producen en el extranjero, pero se utilizan medios o equipos ubicados en el territorio nacional. Como ejemplo citamos el caso de las redes robóticas (*botnets*)[14], donde las instrucciones o programas pudieran tener origen en el extranjero, utilizando computadores o equipos ubicados en Guatemala, para cometer delitos que surten efectos en el extranjero.

---

14 http://www.microsoft.com/protect/terms/botnet.aspx, consultado el 16 de julio 2010, 10:15 horas. El término **bot** es la abreviatura de *robot*. Los ciberdelincuentes distribuyen *software* malintencionado (también conocido como *malware*) que puede convertir un ordenador en un *bot* (conocido también como un *zombi*). Cuando esto ocurre, el ordenador puede realizar tareas automatizadas a través de Internet, sin que el usuario tenga conocimiento de ello. Los ciberdelincuentes suelen utilizar *robots* para infectar un gran número de computadoras. Estos equipos forman una red, o una ***botnet***. Los ciberdelincuentes usan *botnets* para enviar *spam* (mensajes de correo electrónico masivo), propagan virus, usan las computadoras y los servidores como arma de ataque, y para cometer otros tipos de delitos y el fraude. Si el equipo pasa a formar parte de una *botnet*, el equipo puede disminuir la velocidad y es posible que ayude a los delincuentes sin darse cuenta.

2.4 **Cuando se caracterice cualquier tipo de complicidad desde el territorio guatemalteco**. La ley penal establece que son cómplices, entre otros, quienes proporcionaren informes o suministraren medios adecuados para realizar el delito o quienes sirvieren de enlace o actuaren como intermediarios entre los partícipes, para obtener la concurrencia de éstos en el delito. De manera que, para poder caracterizar cualquier tipo de complicidad desde el territorio guatemalteco, debemos sujetarnos a lo que establece el artículo 37 del Código Penal.[15] Como ejemplo de complicidad en materia de Cibercrimen, podemos citar las "alianzas" para ataques cibernéticos que promueven los hacker-activistas para dañar sistemas informáticos, tal como sucedió en el ataque de *Anonymous* denominado "*The Internet Strikes Back*", donde fueron duramente afectados los sistemas informáticos de la Oficina Federal de Investigación –FBI-, entre otros entes, y donde participaron cerca de 10,000 personas o atacantes de diferentes países, haciendo uso de más de 27,000 ordenadores.

En el contenido del Proyecto de Ley, en mención, se establece que, cuando el origen o los efectos hayan sido producidos en el extranjero, serán competentes los Tribunales guatemaltecos en caso de que en el extranjero no se hubiere dictado sentencia firme por el mismo hecho o el sujeto activo hubiere evadido la persecución penal en tribunales extranjeros.

15 El artículo 37 del Código Penal de Guatemala, establece que son **cómplices**: "1º Quienes animaren o alentaren a otro en su resolución de cometer el delito. 2º Quienes prometieren su ayuda o cooperación para después de cometido el delito. 3º. Quienes proporcionaren informes o suministraren medios adecuados para realizar el delito; y, 4º Quienes sirvieren de enlace o actuaren como intermediarios entre los partícipes para obtener la concurrencia de éstos en el delito."

3. DELITOS DE ACCIÓN PÚBLICA

Los delitos regulados en el Proyecto de Ley de Cibercrimen, se consideran de ***acción pública***, es decir, son hechos ilícitos que deben ser investigados *de oficio* por el Ministerio Público, siendo innecesario cualquier acto introductorio, como denuncia o querella, de parte de determinada persona.

Inicialmente se estableció que los delitos informáticos serían de acción pública *a instancia privada*; sin embargo, para lograr una mejor persecución penal, por parte del Ministerio Público, se concluyó que era necesario que los delitos cibernéticos fueran considerados de *acción pública*, ya que, tal como veremos más adelante y específicamente en el caso del fraude informático, el ciberdelincuente afecta patrimonios colectivos que, considerados de manera individual, no tienen mayor trascendencia.

4. DEFINICIONES UTILIZADAS EN EL PROYECTO DE LEY DE CIBERCRIMEN

Para facilitar la comprensión del contenido del Proyecto de Ley, se incluyeron las definiciones de los términos que se utilizan en el articulado.

Por técnica legislativa se trató de evitar el empleo de términos en idioma extranjero. Sin embargo, existen algunos términos que por su carácter técnico, de conocimiento en el medio informático y por su difícil traducción al idioma español, quedaron en idioma inglés. Así tenemos, entre otros, los términos *HASH, INTERNET, WEB, SOFTWARE*, entre otros.[16]

16 Dentro de las definiciones utilizadas en el Proyecto de Ley de Delitos Informáticos

se encuentran: (a) **Confidencialidad**: Constituye un atributo de la información para prevenir su divulgación a personas o usuarios no autorizados; (b) **Correo electrónico**: Es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos; (c) **Datos informáticos**: Toda representación de hechos, instrucciones, caracteres, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función; (d) **Datos de tráfico**: Designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente; (e) **Disponibilidad**: Constituye una característica de la información para garantizar que ésta se encuentre disponible, en cualquier momento, para quien tiene la autorización de acceder a ella, sean personas, procesos o aplicaciones; (f) **Documento electrónico**: Registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contengan información acerca de hechos o actos capaces de causar efectos jurídicos; (g) **Hash:** Se refiere a una función o método para generar claves o llaves que representen de manera unívoca a un documento, registro y/o archivo; (h) **Hipertexto**: Texto que contiene elementos a partir de los cuales se puede acceder a otra información; (i) **Infoestructura**: Son infraestructuras reconocidas como el medio generador por el cual una nación convierte los activos, ya sea materiales en bruto, tecnologías o ideas, en productos de valor y servicios; (j) **Integridad**: Constituye un atributo de la información para asegurar que ésta, al almacenarse o al ser trasladada, no sea modificada de ninguna forma no autorizada; (k) **Internet**: Conjunto descentralizado de redes de comunicación interconectadas , que utilizan el protocolo de control de transporte y el protocolo de Internet, según sus siglas en inglés: TCP/IP; garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial; (l) **Página Web**: Documento situado en una red informática, al que se accede mediante enlaces de hipertexto; (ll) **Proveedor de servicio**: Toda entidad pública o privada que ofrece, a los usuarios de sus servicios, la posibilidad de comunicar a través de un sistema informático; Cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios; (m) **Sistema informático**: Dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos; (n) **Sistema operativo:** Programa especial que se carga en un computador luego de ser encendido y cuya función es gestionar los demás programas o aplicaciones, que se ejecutarán en dicho computador, como por ejemplo, un procesador de texto, una hoja de cálculo, la impresión de un texto en una impresora o una conexión a Internet; (ñ) **Software**: Se refiere al equipamiento lógico o soporte lógico de un computador digital, que comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica; (o) **Correo electrónico masivo**: Constituye todos aquellos mensajes no solicitados o no deseados por el destinatario y de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican, de alguna o varias maneras, al receptor; (p) **Tarjeta inteligente**: Es una tarjeta con circuitos integrados la que permite la ejecución de una lógica programada, para proveer servicios de

5. CONVENCIÓN SOBRE LA CIBERDELINCUENCIA

Debido a la necesidad de aplicar una política penal común a nivel internacional para proteger a la sociedad frente a la ciberdelincuencia, y para crear un marco regulatorio uniforme y mejorar la cooperación internacional, el 23 de noviembre del año 2001, los Estados miembros del Consejo de Europa formalizaron la Convención sobre la Ciberdelincuencia, también conocida como Convenio de Budapest.

Las conductas ilícitas, reguladas en el Convenio de Budapest, son: el acceso ilegal, interceptación ilegal, interferencia de los datos, interferencia de sistema, uso erróneo de dispositivos, falsificación del ordenador, fraude del ordenador, pornografía infantil. También se establecen disposiciones de índole procesal para la preservación de datos almacenados, y todo lo relacionado a los actos procesales para producir prueba y aislar todo acto de cibercrimen.

Actualmente, Guatemala no es parte de la Convención sobre Ciberdelincuencia, sin embargo, nuestro país daría un paso trascendental para el combate del cibercrimen y para su futura adhesión a la referida Convención, cuando la Iniciativa de Ley de Delitos Informáticos, número cuatro mil cincuenta y cinco, llegue a formar parte del ordenamiento jurídico guatemalteco.

seguridad de la información; (q) **Tecnologías de la información**: Rama de la tecnología que se dedica al estudio, aplicación y procesamiento de información, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, protección, procesamiento, transmisión y recuperación de información, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso de equipos y programas, cualesquiera de sus componentes y todos los procedimientos vinculados con el procesamiento de información.

No obstante que el Convenio de Budapest fue celebrado a nivel del Consejo de Europa, no existe ningún impedimento legal para que otros países, como el caso de Guatemala, puedan adherirse a dicha normativa. Al contrario, tanto para Europa como para los países de América Latina y todos los países del mundo, debido a la naturaleza "transfronteriza" de los delitos informáticos, la normativa se convierte en Derecho positivo cuanto mayor sea el número de países que se adhieran a la citada Convención. Ejemplo de ello ha sido la ratificación, por parte del Senado de Estados Unidos, en el mes de agosto del año dos mil seis. Así también, la Cámara de Diputados de México ha exhortado, a su organismo Ejecutivo, para que se adhiera formalmente al Convenio de Budapest.[17] Argentina, al igual que otros países de América Latina, actualmente se encuentra en el procedimiento previo a la adhesión a la Convención.

Recientemente, España ratificó el Convenio sobre la Ciberdelincuencia del Consejo de Europa siendo, de esta forma, el trigésimo país en ratificar este Convenio y el décimo séptimo Estado Miembro de la Unión Europea en hacerlo.

Son muchos los organismos internacionales que se han preocupado por crear leyes uniformes en materia de ciberdelincuencia, así tenemos a la Organización de los Estados Americanos (OEA), ente que, a través de REMJA[18], ha realizado distintos foros y

17 La Comisión Permanente del Senado, en México, emitió un comunicado con un punto de acuerdo, en el que exhorta al Ejecutivo Federal para que México se adhiera formalmente a la Convención Sobre Ciberdelincuencia (Convenio de Budapest). Dicho comunicado fue publicado en la Gaceta No. 10 del Senado, del 7 de julio del 2010. La exposición de motivos del comunicado hace referencia a la importancia de la adopción del Convenio de Budapest, para facilitar la cooperación a nivel internacional y para la aprobación de una legislación adecuada que permita combatir delitos tales como fraudes informáticos y pornografía infantil.

18 Según el sitio web de la Organización de los Estados Americanos, http://www.oas.org/es/sla/dlc/remja/, el proceso de las REMJA constituye el foro político y técnico de

talleres de discusión y aplicación de técnicas para combatir el delito cibernético. También tenemos a la División sobre Aplicaciones TIC y Ciberseguridad, de la Unión Internacional de Telecomunicaciones (UIT), que ha emitido publicaciones sobre cibercrimen y que han sido de mucha utilidad para crear las leyes ordinarias internas de cada país.

mayor importancia, a nivel hemisférico, en temas relacionados con el fortalecimiento y acceso a la justicia y la cooperación jurídica internacional, en áreas relacionadas con la asistencia mutua en materia penal, extradición, políticas penitenciarias y carcelarias, delito cibernético y ciencias forenses, entre otras.