



PRESENTACIÓN

En este, nuestro primer boletín sobre cybercriminalidad, trataremos de dar un enfoque general sobre Derecho Penal y Nuevas Tecnologías - prefiero denominarlo de esta manera, a fin de no caer en la discusión de si se trata delitos informáticos o delitos cometidos a través del internet - y cómo se viene desarrollando en nuestro país.

En ese sentido, le presentamos una relación de normas de carácter nacional que van desde la Ley que incorpora los delitos informáticos al Código Penal, así como normativa de carácter internacional como el Convenio sobre Cybercriminalidad o Convenio de Budapest, hasta el último pronunciamiento por parte de nuestro legislador en el Dictamen de la Comisión de Justicia y Derechos Humanos recaído en los Proyectos de Ley 034/2011-CR, 037/2011-CR y 1136/2011-CR con un texto sustitutorio por el que se propone la Ley de los delitos informáticos del pasado veinte de julio, también denominada por los medios de comunicación como Ley Beingolea. Legislación que nos permitirá orientarnos en el tema, además de ver cuál ha sido o es la tendencia que viene asumiendo nuestro legislador respecto al cibercrimen.

Y para culminar, le presentaremos las noticias y casos más recientes asociados a la cybercriminalidad, así como una serie de eventos que se vienen realizando o están próximos a realizarse.

Esperamos que la información que le proporcionamos le resulte útil y de su agrado.

Fabiola Villanueva Del Busto
División de Cibercrimen
Iriarte & Asociados



SUMILLA

TEMA PRINCIPAL:

DERECHO PENAL Y NUEVAS TECNOLOGÍAS: ESTADO ACTUAL

SELECCIÓN DE NORMAS:

NORMAS INTERNACIONALES

- RESOLUCIÓN 55/63 DE LAS NACIONES UNIDAS - LUCHA CONTRA LA UTILIZACIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN CON FINES DELICTIVOS
- RESOLUCIÓN 56/121 DE LAS NACIONES UNIDAS - LUCHA CONTRA LA UTILIZACIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN CON FINES DELICTIVOS
- CONVENIO SOBRE LA CIBERCRIMINALIDAD DEL CONCEJO DE EUROPA O CONVENIO SOBRE CIBERCRIMINALIDAD DE BUDAPEST
- PROTOCOLO ADICIONAL A LA CONVENCION SOBRE CIBERCRIMINALIDAD
- RESOLUCIÓN AG/RES 2004(XXXIV-O/04) – DE LA ASAMBLEA GENERAL DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. “CIBERCRIMEN – CIBERDELINCUENCIA”

NORMAS NACIONALES

- CONSTITUCIÓN POLITICA DEL PERÚ DE 1993
- CODIGO PENAL
- LEY 27309 QUE INCORPORA AL CÓDIGO PENAL DEL PERÚ LOS DELITOS INFORMÁTICOS (PROMULGADA EL 15 DE JULIO DEL AÑO 2000)
- DICTAMEN DE LA COMISIÓN DE JUSTICIA Y DERECHOS HUMANOS RECAÍDO EN LOS PROYECTOS DE LEY 034/2011-CR, 037/2011-CR Y 1136/2011-CR CON UN TEXTO SUSTITUTORIO POR EL QUE SE PROPONE LA LEY DE LOS DELITOS INFORMÁTICOS

SECCIÓN DE NOTICIAS:

- CIBERDELINCUENTES OPERAN EN PERÚ A TRAVÉS DE FRAUDES VÍA E-MAIL
- ALERTAN POR PEDÓFILOS EN INTERNET
- INVESTIGAN A PERIODISTA DE ECONOMIA DE “PERU 21” POR PRESUNTO DELITO INFORMÁTICO



e-boletín legal de Derecho Penal
Informático
Boletín Legal sobre Cibercrimen

PERÚ

CYBERCRIMEN

Año I, N° 1
Septiembre, 2012

- LA LEY DE DELITOS INFORMÁTICOS
- “LEY BEINGOLEA” SERÍA REEMPLAZADA POR EL CONVENIO DE BUDAPEST

SECCIÓN DE EVENTOS:

- II CURSO DE CAPACITACION EN INVESTIGACION DE DELITOS INFORMATICOS EN EL MARCO DEL NUEVO CODIGO PROCESAL PENAL 2012.
- FORO ANUAL DE INTERNET



DERECHO PENAL Y NUEVAS TECNOLOGIAS: ESTADO ACTUAL

El Derecho Penal es, por excelencia, el medio de control social más efectivo con el que cuenta el Estado, pues mediante su potestad punitiva, materializada en la norma penal, sanciona a aquel individuo o colectivo que va contra las normas, manteniendo y asegurando, de esta manera, la coexistencia en sociedad. Pero el Derecho Penal es, también, un sistema discontinuo de ilicitudes, pues no puede prever todas las conductas humanas que van apareciendo, las nuevas modalidades delictivas que cada día son más sofisticadas, ello gracias a los avances de la tecnología. Es así pues que surge esta amalgama Derecho Penal y Nuevas Tecnologías, o denominados por algunos Cyberdelincuencia.

Es pues, que con la finalidad de resolver los problemas que se producen dentro de una convivencia social, que surgen elementos normativos como Convenio sobre La Cybercriminalidad del Consejo de Europa o Convenio sobre Cybercriminalidad de Budapest, que tienen por finalidad instar a los Estados miembros a combatir estas nuevas modalidades delictivas como el Acceso ilícito, la Interceptación ilícita, la Interferencia en los datos, que tienen como fin la protección de bienes jurídicos como la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, bienes jurídicos que han surgido con las nuevas tecnologías. No olvidemos que los bienes jurídicos no son otra cosa que aquellos presupuestos indispensables o condiciones fundamentales para la realización de la persona y la vida en común; por ende, no son estáticos, y por lo tanto en la medida que gocen de relevancia para la convivencia en sociedad requerirán de una protección por parte del Estado.

Claro está que dicha norma no se limita a la parte sustantiva, sino que por el contrario, y acorde al avance de las nuevas tecnologías, propone mecanismo procesales interesantes a fin de combatir estos ilícitos, además de invitar a la cooperación internacional para la solución de este problema: la cybercriminalidad, que nos obliga a replantearnos la concepción de criminalidad bipolar que se manejaba, para orientarlo hacia una criminalidad de grupo, además de renovar nuestro concepto de jurisdicción, sin dejar ser un Derecho Penal protector de los derechos fundamentales.

Nuestro país no es ajeno al asunto, así tenemos la Ley 27309 del 15 de julio del año 2000, mediante la cual se incorporan al Código Penal los Delitos Informáticos, modificándose de esta manera el Título V del Libro Segundo del Código, incorporando los siguientes artículos:

- **Artículo 207-A - Interferencia, acceso o copia ilícita contenida en base de datos:**

“El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos,



será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas”.

- **Artículo 207-B - Alteración, daño o destrucción de base de datos.**

“El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.”

- **Artículo 207-C - Circunstancias cualificantes agravantes**

“En los casos de los artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

- 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función de su cargo.*
- 2. El agente pone en peligro la seguridad nacional”.*

Si bien es cierto, estos artículos se encuentran ubicados dentro de los delitos contra el Patrimonio, aunque en realidad se encuentran asociados a la protección de otros bienes jurídicos, como son la integridad, confidencialidad y disponibilidad de los datos o sistemas informáticos. Sin embargo, hay que destacar la intención del legislador de poner solución al problema de la cybercriminalidad y no dejar paso a la impunidad.

El pasado mes de julio, la Comisión de Justicia y Derechos Humanos del Congreso de la República, bajo la presidencia del congresista Alberto Beingolea emitió un dictamen, en el cual se buscaba poner fin a este problema y regular las conductas ilícitas asociadas al empleo de nuevas tecnologías, o delitos informáticos, como lo denomina el propio dictamen, sin embargo de la redacción del documento se observa que éste no se adecúa a los parámetros de un Derecho Penal garantista y preventivo, no cabe duda que todas las intenciones para combatir este mal son buenas, solo que lucha tiene que realizarse con el debido respeto y protección de derechos fundamentales.

Consideraciones Finales:

El Perú necesita, con suma urgencia, de una legislación adecuada a combatir la cybercriminalidad, pero respetando los derechos fundamentales, a efectos de evitar la impunidad frente a este tipo de



conductas que emplean de manera inequívoca las nuevas tecnologías y ponen en peligro la vida en sociedad. Una legislación acorde al Convenio sobre la Cybercriminalidad de Budapest, respetuoso de las garantías fundamentales de la persona, que, a la fecha está resultando un instrumento eficaz para combatir este mal que nos afecta a todos: La Cybercriminalidad.

SELECCIÓN DE NORMAS

NORMAS INTERNACIONALES

- **4 de Diciembre de 2000**

RESOLUCIÓN 55/63 DE LAS NACIONES UNIDAS

La Asamblea General de la Naciones Unidas mediante esta resolución la lucha contra la utilización de la tecnología de la información con fines delictivos, por lo cual invita a los Estados Miembros a que tomen en cuenta las medidas propuestas para combatirla utilización de la tecnología de la información con fines delictivos.

- **19 de Diciembre de 2001**

RESOLUCIÓN 56/121 DE LAS NACIONES UNIDAS

La Asamblea General de las Naciones Unidas mediante esta resolución invita a los estados miembros a luchar contra la utilización de las tecnologías de la información con fines delictivos, en tal sentido Invita a los Estados Miembros a que, al elaborar leyes y políticas nacionales y al adoptar prácticas para luchar contra la utilización de la tecnología de la información con fines delictivos.

- **23 de Noviembre de 2001 (Entra en Vigor el 1 de Julio de 2004)**

CONVENIO SOBRE LA CIBERCRIMINALIDAD DEL CONCEJO DE EUROPA O CONVENIO SOBRE CIBERCRIMINALIDAD DE BUDAPEST

El Concejo de Europa y los Estados que suscriben el convenio con la finalidad de luchar contra la cyberdelincuencia , conscientes de los cambios que trae consigo la tecnología pretende, a través de los artículos de dicho instrumento internacional, otórgale a los Estados partes mecanismos efectivos para combatir este mal, es así que define conceptos como “sistemas informáticos” o “datos informáticos”, plantea aspectos de Derecho Penal Sustantivo definiendo tipos penales como la Interceptación Ilícita , Fraude Informático,



Falsificación Informática; asimismo presenta aspectos de carácter procesal y mecanismos de cooperación internacional. Lo que la convierte en una de las normas de carácter internacional más completas.

- **28 de Enero de 2003 (Entra en vigor el 1 de Marzo de 2006)**

PROTOCOLO ADICIONAL A LA CONVENCIÓN SOBRE CIBERCRIMINALIDAD

Por su parte este protocolo aborda temas de racismo y xenofobia cometidos a través de medios informáticos, mediante esta norma se busca que los Estados miembros incorporen a su legislación interna como delito la difusión de material de índole racista y xenófobo.

- **08 de Junio de 2004**

RESOLUCIÓN AG/RES 2004(XXXIV-O/04) –ASAMBLEA GENERAL DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. “CIBERCRIMEN – CIBERDELINCUENCIA”

La Asamblea General de la Organización de los Estados Americanos mediante sesión plenaria decide adoptar medidas respecto a las amenazas en el ámbito de la seguridad cibernética, en tal sentido insta a los Estados miembros a adoptar la Estrategia Interamericana Integral de Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética

NORMAS NACIONALES

- **29 de Diciembre de 1993 (Entra en vigor el 1 de Enero de 2004)**

CONSTITUCIÓN POLITICA DEL PERÚ de 1993

Nuestra Carta Magna en el Título I, Artículo 2° inciso 6 precisa:

“A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar”.

De la lectura del texto constitucional se aprecia que la intención del legislador de proteger los derechos fundamentales, como es la intimidad de las personas, precisando los medios a través de los cuales ésta puede ser vulnerada, como lo son los servicios informáticos computarizados o no.

- **08 de Abril de 1991**

DECRETO LEGISLATIVO 635 – CÓDIGO PENAL



El Código Penal desde su promulgación ha sufrido diversas modificatorias en relación al uso de nuevas tecnologías, un ejemplo de ello son los siguientes delitos: Pornografía Infantil(Artículo 183-A), Hurto en su modalidad agravada (Artículo 186), Organización y uso indebido de archivos computarizados (Artículo 157°); entre otros.

- **15 de Julio de 2000**

LEY 27309

Mediante esta norma se incorporan al Código Penal los Delitos Informáticos, modificándose de esta manera el Título V del Libro Segundo del Código, incorporando los siguientes artículos:

Artículo 207-A: Interferencia, acceso o copia ilícita contenida en base de datos:

Artículo 207-B: Alteración, daño o destrucción de base de datos.

Artículo 207-C: Circunstancias agravantes

Evidentemente el Título V del Libro Segundo del Código Penal está referido a los Delitos contra el Patrimonio, la pregunta es si los Delitos informáticos se encuentran asociados al bien jurídico Patrimonio, es discutible este punto, si solo responden a una naturaleza patrimonial o si por el contrario son de carácter pluriofensivo, sobre ello tocaremos en nuestros próximos boletines.

- **20 de Julio de 2012**

DICTAMEN DE LA COMISIÓN DE JUSTICIA Y DERECHOS HUMANOS RECAÍDO EN LOS PROYECTOS DE LEY 034/2011-CR, 037/2011-CR Y 1136/2011-CR CON UN TEXTO SUSTITUTORIO POR EL QUE SE PROPONE LA LEY DE LOS DELITOS INFORMÁTICOS.

Debemos precisar que se trata de un Dictamen y no una norma, solo que para efectos didácticos y con la finalidad de apreciar el punto de vista del legislador, se le ha ubicado en la sección de norma de nuestro boletín.

Pues bien el pasado 20 de Julio la Comisión de Justicia y Derechos Humanos emitió dicho dictamen, el cual ha sido denominado por los medios de comunicación como “Ley Beingolea”, ello en virtud a que el presidente de dicha comisión era el congresista y abogado penalista Alberto Beingolea. Pues bien, a través de este dictamen se materializa, por decirlo de alguna forma, la intención del legislador regular sobre aquellas conductas desviadas llevadas a cabo mediante el empleo de nuevas tecnologías, así se desprende de la lectura del análisis técnico de dicho



documento, así como del artículo 1° del Texto Sustitutorio. Dicho documento muestra no solamente aspecto sustantivos en materia sancionatoria como es el caso de las figuras de Sabotaje Informático, Fraude Informático entre otros, sino también aspectos procesales como los institutos procesales de Colaboración Eficaz y Agente Encubierto. Sin duda alguna la intención del legislador de regular sobre estos temas, es buena, solo que dicha intención debe estar orientada no solo a cuestiones de política criminal, sino también hacía un Derecho Penal Garantista.

NOTICIAS

CIBERDELINCUENTES OPERAN EN PERÚ A TRAVÉS DE FRAUDES VÍA E-MAIL

16 DE SEPTIEMBRE

El Perú se ha convertido en un buen lugar de acción para los delincuentes informáticos, que a través de e-mails de remitentes desconocidos, logran que incautos cibernautas -movidos por atractiva información- hagan clic en el archivo adjunto sin medir las consecuencias.

Esta forma de estafa se puede presentar a través de mensajes que llegan al correo electrónico, unos que invitan a ver fotos o videos íntimos de modelos y conocidas artistas. También se presentan como falsos e-mails de entidades bancarias o juegos de lotería provenientes del extranjero, entre otros.

Según el especialista Jorge Mieres, analista de malware de Kaspersky Lab, este tipo de delito informático se ha incrementado considerablemente en los últimos dos años en el Perú, ante el crecimiento económico que experimenta nuestro país.

Fuente: http://www.rpp.com.pe/2012-09-16-ciberdelincuentes-operan-en-peru-a-traves-de-fraudes-via-e-mail-noticia_522179.html

ALERTAN POR PEDÓFILOS EN INTERNET

18 DE SEPTIEMBRE

Más de 120 denuncias de pedofilia han sido presentadas en lo que va del año, según cifras policiales. El comandante Daniel Hernani, miembro de la División de Investigación de Delitos de Alta Tecnología (Divindat), pidió a los padres a mantenerse alertas con el Internet.

Fuente: <http://iblnews.com/story/67891>



INVESTIGAN A PERIODISTA DE ECONOMIA DE “PERU 21” POR PRESUNTO DELITO INFORMÁTICO

28 DE ABRIL

A pedido de la fiscalía, el 53° juzgado penal de Lima autorizó la detención preventiva del periodista del diario Perú21, Rudy Palma Moreno durante tres días, para ser investigado por presunto hackeo de correos electrónicos

Las autoridades se centran en saber dónde y cómo obtuvo las claves de acceso a los correos electrónicos intervenidos y determinar cuál era su motivación para cometer el delito.

Fuente: <http://www.larepublica.pe/28-04-2012/investigacion-periodista-de-economia-de-peru-21-por-presunto-delito-informatico>

LA LEY DE DELITOS INFORMÁTICOS

02 DE AGOSTO

Diversas organizaciones de la sociedad civil, como la Red Científica Peruana, Ipys y la Asociación Pro Derechos Humanos y especialistas se han dirigido al Congreso para alertar sobre el dictamen de la Ley de Delitos Informáticos aprobado por la Comisión de Justicia a raíz de una iniciativa del PPC. Los firmantes avalan la preocupación del Legislativo por actualizar el catálogo de delitos informáticos del Código Penal, pero sostienen que varios de los artículos vulneran derechos fundamentales y demandan la apertura de un diálogo nacional que esclarezca que los DDHH deben ser protegidos tanto en el ámbito de las comunicaciones offline como online.

El Perú requiere modernizar su legislación sobre los delitos informáticos y protegerse de las amenazas a su ciberespacio. Esta tarea debe ser acometida con responsabilidad. Los antecedentes del dictamen observado van en un sentido distinto

Fuente: <http://www.larepublica.pe/politica/editorial-12-08-2012>

“LEY BEINGOLEA” SERÍA REEMPLAZADA POR EL CONVENIO DE BUDAPEST

15 DE SEPTIEMBRE

El cuestionado proyecto de ley contra los delitos informáticos denominado 'Ley Beingolea' debido a su principal impulsor podría ser reemplazado debido a las fuertes críticas surgidas en internet, desde activistas web hasta la Asociación Nacional de Periodistas del Perú y varios organismos públicos.

Por este motivo, los directores de las entidades gubernamentales correspondientes planearían crear una comisión de ciberseguridad encargada de buscar soluciones a los robos a través de la banca online.



Otra medida sería adscribir al país a la Convención de Budapest o Convenio del Consejo de Europa sobre el Cybercrimen, al igual que hicieron más de 40 países para regular adecuadamente las leyes que se emitan.

Fuente: <http://www.larepublica.pe/15-09-2012/ley-beingolea-seria-reemplazada-por-el-convenio-de-budapest>

|

EVENTOS

II CURSO DE CAPACITACION EN INVESTIGACION DE DELITOS INFORMATICOS EN EL MARCO DEL NUEVO CODIGO PROCESAL PENAL 2012.

Fecha: Octubre a Diciembre de 2012

URL: <http://www.dirincrim.com/cursos.html>

FORO ANUAL DE INTERNET

Fecha: Miércoles 3 de Octubre.

Lugar: AmCham

URL: <http://www.amcham.org.pe/eventos/invitaciones/2012/Octubre/e0874.htm>



IRIARTE & ASOCIADOS

Jr. Miró Quesada 191 - Of. 510. Lima 01 – Perú.

Telefax (+511) 427 0383

<http://www.iriartelaw.com>

contacto@iriartelaw.com

©2012 Iriarte & Asociados.