DOCUMENTOS DE TRABAJO 01

RICARDO ELÍAS PUELLES

Luces y sombras en la lucha contra la delicuencia informática en el Perú

hiperderecho

Hiperderecho
Organización civil peruana sin fines de lucro dedicada a investigar, facilitar el entendimiento público y promover el respeto de los derechos y libertades en entornos digitales. Fundada en el 2012, ha estado involucrada en el debate público de diferentes asuntos de interés público como libertad de expresión, derechos de autor, privacidad y delitos informáticos.

Ricardo Elías Puelles
Abogado por la Pontificia Universidad Católica del Perú. Se graduó con mención sobresaliente por la tesis "Los fines constitucionales de la pena como fundamento para la derogación de las gracias presidenciales". Es especialista en Teoría del Delito por la Universidad Nacional de Buenos Aires así como en Política Criminal y Derecho Procesal Penal por la Universidad Nacional Mayor de San Marcos. Ex miembro de la Asociación Civil Themis.

Esta publicación es parcialmente resultado de un proyecto de investigación financiado por Google Inc.

Esta publicación fue terminada en junio del 2014.

Hiperderecho
http://www.hiperderecho.org
hola@hiperderecho.org

I. INTRODUCCIÓN

En la primera mitad del Siglo XIX, Adolfe Quetelet y André-Michel Guerry impulsaron el estudio científico de la *estadística moral* con el fin de comprender la relación entre la cantidad de delitos producidos y la ubicación geográfica de su comisión. Estas técnicas para representar la distribución de los delitos a través de mapas fueron retomadas más adelante en Estados Unidos por la Escuela de Chicago, principalmente por Burguess (1925) y Shaw & McKay (1942). Todo ello sentó las bases de la Criminología Ecológica y de lo que, a mediados de los setenta y ochenta, se conocería como *Crime Prevention Through Environmental Design.* A partir de ello, muchos estudios se han centrado en comprender y estudiar el espacio físico donde ocurren los delitos para buscar mecanismos para su prevención y lucha. Así, para los criminólogos, un delito tiene lugar cuando concurren cuatro elementos: una ley, un infractor, un objetivo y un lugar.[1]

Con la aparición de Internet y de los delitos informáticos, los criminólogos han comenzado a anunciar que la concepción del delito debe replantearse pues estos nuevos crímenes vienen siendo cometidos en "no lugares". Estos cambios han abierto nuevas líneas de estudio. Mientras que el miedo al delito tradicional se asociaba a experiencias emocionales, el miedo al delito informático está vinculado a un componente cognitivo, ya que el usuario de Internet hace una valoración puramente racional del riesgo que corre con determinadas conductas en la red. Sin embargo, es poco probable que navegar por la red le genere la misma sensación que cuando pasa por una calle oscura, por un lugar inhóspito o por uno poco controlable.[2] Frente al rápido e inminente avance de la criminalidad informática no sólo es necesario criminalizar estas nuevas conductas sino también estudiarlas de manera detallada para buscar mecanismos de prevención, pues como la Asociación Mundial de Derecho Penal reconoció en el XV Congreso Internacional de Derecho Penal realizado hace ya veinte años:

> La comunidad académica y científica, conjuntamente con los gobiernos deben comprometerse a realizar más investigaciones sobre el delito de la tecnología informática (…) La teoría y política jurídica debe prestar especial atención al estudio y desarrollo de la ley informática, tomando en consideración las características específicas de la información, al compararla con los objetos tangibles, e investigar los probables cambios que afectan los principios generales y paradigmas.[3]

Lamentablemente, durante muchos años, esta labor académica no se implementó en el Perú.

El problema no incide únicamente en el aumento de este tipo de criminalidad sino en las consecuencias que traen consigo. A nivel mundial, por ejemplo, el FBI IC3 - *Internet Crime Complaint Center* reportó que en el 2013 se produjeron 262,813 denuncias por

---

1 *Vid.* VOZMEDIANO SANZ, Laura y César SAN JUAN GUILLÉN. "Criminología ambiental. Ecología del delito y de la seguridad". Barcelona: Universidad Oberta de Catalunya, 2010.

2 Ibid. p. 164.

3 Recomendaciones del XV Congreso Internacional de Derecho Penal. Sección II – Sobre delitos informáticos y otros delitos cometidos contra la tecnología informática. Evento realizado entre el 04 y 10 de setiembre de 1994 en Río de Janeiro - Brasil. Recomendación No. 24.

cibercrímenes que representaron pérdidas económicas ascendentes a US$ 781'841,611 dólares. Debo precisar que si bien el número de incidentes fue menor al del 2012, lo cierto es que las pérdidas representaron un incremento del 48,8% respecto al año anterior.[4] En el mismo sentido, de acuerdo al *Global Economic Crime Survey 2014*, elaborado por PricewaterhouseCooper, la percepción de los delitos informáticos se ha incrementado del 39% (2011) al 48% (2014) a nivel mundial. Incluso, según el mismo estudio, los delitos informáticos representan uno de los cinco fraudes más comunes al interior del sector empresarial (24%).[5]

Pese a que nuestro país no cuenta con cifras oficiales que demuestren el perjuicio económico que representan los cibercrímenes, sí es necesario indicar que en los últimos diez años este tipo de delitos se ha incrementado de manera considerable a nivel nacional, siendo Lima la ciudad con el mayor número de incidentes reportados:

Tasa por 100,000 habitantes	2002	2007	2012
Menor a 0.1	Todo el país	Amazonas, Ancash, Apurímac, Ayacucho, Cajamarca, Callao, Cañete, Cusco, Huánuco, Huancavelica, Huaura, Lima Norte, Lima Sur, Madre de Dios, Moquegua, Pasco, Santa, San Martín, Tacna y Ucayali	Amazonas, Ancash, Apurímac, Cañete, Lima Norte y Pasco
0.1 – 1.8 (Baja)	-	Arequipa, Ica, La Libertad, Lambayeque, Loreto, Piura, Puno y Tumbes	Arequipa, Ayacucho, Cajamarca, Callao, Cusco, Huánuco, Huaura, Huancavelica, Ica, Junín, La Libertad, Lambayeque, Lima Sur, Loreto, Piura, Puno, Santa, San Martín, Sullana, Tacna, Tumbes, y Ucayali
1.9 – 3.6 (Media)	-	Junín y Lima	Madre de Dios y Moquegua
3.7 – 5.3 (Alta)	-	-	Lima

Cuadro 1
Evolución de los delitos informáticos por distrito fiscal.
Fuente: Mapas Temáticos del Observatorio de la Criminalidad del Ministerio Público del Perú. Elaboración propia.

En este trabajo analizaré la respuesta que progresivamente ha implementado nuestro Legislador frente a este tipo de ilícitos. Además, plantearé algunas recomendaciones que

---

4 Fuente: <http://www.ic3.gov/>. Consultado: 19 de mayo de 2014.

5 PricewaterhouseCooper. *Global Economic Survey 2014*. Fuente: <http://www.pwc.com/gx/en/economic-crime-survey/>. Consultado: 19 de mayo de 2014.

permitirán, de un lado, fortalecer nuestro sistema punitivo y, de otro, salvaguardar los derechos y garantías que como ciudadanos nos asiste.

II. LA RESPUESTA DEL ESTADO PERUANO FRENTE A LOS DELITOS COMETIDOS A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS

Si bien el Código Penal peruano (CP) fue promulgado el 03 de abril de 1991, este cuerpo normativo ya avizoraba la importancia de sancionar los delitos cometidos a través de medios electrónicos por lo que tipificó el delito de *hurto telemático*. Así, el artículo 186 CP, castigaba el hurto agravado con pena privativa de libertad no menor de 3 ni mayor de 6 años y con 180 a 365 días-multa, cuando el autor "*usa*[ba] *sistemas de transferencia electrónica de fondos, de la telemática en general, o viola*[ba] *el empleo de claves secretas.*"[6] Poco tiempo después, mediante la Ley No. 26319 del 27 de mayo de 1994, la sanción fue incrementada a pena privativa de libertad no menor de 4 ni mayor de 8 años, manteniéndose sin modificación sustancial alguna hasta que fue derogada mediante la Ley 30096 del 22 de octubre de 2013. Sin embargo, pronto el legislador cayó en cuenta de que este tipo penal sólo castigaba un escaso número de conductas delictivas y dejaba impunes muchos ilícitos en los que se empleaban mecanismos informáticos.

En menos de una década, el problema del empleo indebido de las Nuevas Tecnologías ocasionó que el Congreso decidiera sancionar a quienes las empleaban con fines ilícitos. La primera respuesta de nuestro Legislador fue la tipificación de los Delitos Informáticos. Posteriormente, al no ser suficiente, se crearon nuevos delitos o se agravaron los ya existentes con la finalidad de perseguir a aquellos delincuentes que empleaban este tipo de tecnologías como un medio para la perpetración de otros (turismo sexual, pornografía infantil, fraude electrónico, apología al terrorismo, etcétera).

2.1. La incorporación de los Delitos Informático al Código Penal de 1991 (Arts. 207-A, 207-B, 207-C y 207-D CP)

Perú comenzó a participar en Internet en diciembre de 1991, siendo la Red Científica Peruana precursora de este fenómeno. Sin embargo, no fue sino hasta 1994, gracias a la RCP, Infovía y la aparición de los primeros centros proveedores de Internet, que su uso se comenzó a masificar.[7] Si bien en los años siguientes no se conocieron en nuestro país mayores crímenes cibernéticos, el sector empresarial sí se mostró preocupado pues, de un lado, el nivel de protección de los correos electrónicos, bases de datos y pioneras páginas

---

[6] Salinas Siccha apunta sobre este tipo delictivo: "Esa postura asumió el legislador y optó por introducir los mal llamados delitos informáticos como modalidades de comisión de conductas delictivas ya tipificadas. De ese modo encontramos reunidas tres circunstancias que agravan que agravan la figura del hurto: primero, cuando la sustracción se realiza mediante la utilización de sistemas de transferencia electrónica de fondos; segundo, cuando el hurto se efectúa por la utilización de la telemática general; y, tercero, cuando el hurto se produce violando claves secretas". SALINAS SICCHA, Ramiro. "Derecho Penal. Parte Especial". Tercera Edición. Lima: Grijley, 2008. p. 437.

[7] De acuerdo al Organismo Supervisor de la Inversión Privada en Telecomunicaciones (OSIPTEL) se pasó de 500 a 600 mil accesos a Internet entre 1994 y 1997. Sin embargo, según INEI, sólo el 3% de los hogares a nivel nacional tenían conexión a Internet. BUSINESS: Negocios en el Perú. Año 5. No. 42. Marzo de 1998. p. 18

web era ínfimo[8] y, de otro, no contábamos con legislación que castigara estos nuevas conductas ilícitas.

Los primeros debates registrados en el Perú en torno a los delitos informáticos se originaron en agosto de 1999 tras la presentación de los Proyectos de Ley No. 05071, 05132 y 05326 por los Congresistas Jorge Muñíz Ziches, Susana Díaz Díaz y Anastacio Vega Ascencio, respectivamente. Si bien las propuestas efectuadas hace más de una década fueron bastante incipientes pues, incluso, partían de comprender que "*los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella*", lo cierto es que respondieron a la revolución informática – económica de su época,[9] al contexto electoral en que se encontraban envueltos[10] y a los primeros escándalos de interceptación de correos electrónicos suscitados nuestro país.[11]

Estas propuestas se materializaron en la Ley No. 27309 promulgada el 17 de julio de 2000 que creó el **Delito informático**[12] (Art. 207-A CP), el **Delito de alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras**[13] (Art. 207-B CP) y el **Delito informático agravado** (Art. 207-C CP).[14] Contextualizar esta implementación nos permite precisar algunos problemas generados, tanto con su incorporación al ordenamiento como con las propuestas de modificación posteriores:

a) El legislador identificó la criminalidad informática con el fraude informático, razón por la cual su tipificación se enmarcó en el Título V del Código Penal, correspondiente a los Delitos contra el Patrimonio. Esto se debió a que inicialmente se pensaba que estos ilícitos eran sólo una extensión de lo que el Código Penal de 1991 preveía como agravantes en la comisión del hurto (utilización de sistemas de

---

8 La Revista Business realizó una encuesta en abril de 1998 entre 250 ejecutivos peruanos y detectó que al 79,2% de los encuestados les preocupada la privacidad de sus comunicaciones por *email*. El 52,6% utilizaban sólo un método de seguridad; mientras que un 36,8%, dos mecanismos; y un 10,6%, de tres a cinco métodos –entre ellos, contar con un *password* para la PC y otra para la cuenta de correo electrónico, utilizar su cuenta en una computadora de uso personal así como guardar sus mensajes en disquetes. BUSINESS: Negocios en el Perú. Año 5. No. 43. Abril de 1998. pp. 62 y s.

9 Hacia julio de 1998, se señalaba que el fenómeno de delitos informáticos no se ha presentado con fuerza en el Perú pues sólo se detectaron algunos casos de hackers locales, cuyas operaciones se limitaron al uso de claves para entrar a sistemas que requerían pagar por obtener una suscripción. BUSINESS: Negocios en el Perú. Año 5. No. 46. Julio de 1998. p. 36

10 En la Sesión Vespertina del 03 de mayo de 2000, al discutirse la creación de los delitos informáticos se trajo a colación las elecciones presidenciales a realizarse en julio de ese año pues se señaló que las penas resultaban demasiado benignas en caso de producirse la alteración en el sistema de cómputo que operaría en la segunda vuelta electoral.

11 En la misma Sesión, para justificar que la sanción de los delitos informáticos debía equipararse a las de interceptación telefónica (03 años), se citó la interceptación de los correos electrónicos del Congresista García – Sayán y su publicación en el Diario Expreso.

12 El delito informático ha recibido diferentes denominaciones en la doctrina penal peruana, tales como *hacking* lesivo, intrusismo informático y acceso informático indebido.

13 Identificado en nuestro medio como delito de sabotaje informático o de daño informático.

14 Este artículo no se encontraba regulado en los proyectos inicialmente discutidos por el Congreso sino que fue producto de la séptima observación formulada por el Poder Ejecutivo, la cual fue aceptada y respaldada por el Congresista Muñiz Ziches, Presidente de la Comisión de Reforma de Códigos. *Vid*. p. 920 del Diario de Debates del Congreso de la República del 21 de junio de 2000.

transferencia electrónicas de fondos, de la telemática en general o la violación del empleo de claves secretas). Por esta razón, muchos autores han considerado que estos delitos no forman parte del Derecho Penal Económico ni que protegen la seguridad informática o la intimidad[15] pues identifican al patrimonio como el principal –o, en algunos casos, como el único– bien jurídico tutelado por estas normas. El agrupar en un solo Capítulo conductas que en realidad protegían diversos bienes jurídicos generó un grave error: pensar que cualquier acto de intrusismo o *hacking* lesionaba el patrimonio de los agraviados.[16] De allí que, pese a las observaciones que el Poder Ejecutivo realizó, el Congreso reiteró que la finalidad de estos nuevos delitos era la protección del patrimonio de sus titulares.[17]

b) Al ser considerados como ilícitos contra el patrimonio, erróneamente fueron catalogados como delitos de peligro y no de resultado. En efecto, en el Debate previo a su aprobación, se señaló que

> El delito de peligro surge ya desde el ingreso a la utilización indebida de los elementos informáticos o a la información de las personas contenidas en los mismos o en las bases de datos, sea para sabotear, espiar, defraudar o dañar. Es decir, no se requiere que se produzca un resultado para estar frente a un delito informático, pues basta la intención.[18]

El Artículo IV CP prevé que la pena, necesariamente, precisa de la lesión o puesta en peligro de bienes jurídicos tutelados por la ley, de ahí que existan delitos de resultado y delitos de peligro concreto y abstracto. Cuando nuestro legislador identificó este nuevo tipo de delitos como ilícitos contra el patrimonio, creó una paradoja. Si esto fuese así, el ingreso a la base de datos no debió ser punible ya que no lesionaba o ponía en riesgo concreto el patrimonio de su titular. De ahí que hubiese sido necesario reconocer que el bien jurídico protegido no era el patrimonio sino una gama diferente de derechos informáticos, debiéndose crear un Título independiente en el Código Penal para su correcta tipificación.

c) El legislador acudió a las sanciones del Derecho Penal como *prima ratio* pues evitó acudir a un ente administrativo que pueda sancionar conductas que por su gravedad (cuantitativa o cualitativa) no merezcan el máximo reproche punitivo con el que cuenta el Estado. Además, promulgó las normas penales sin contar con personal técnico especializado que colaborase con las investigaciones preliminares o judiciales, lo que originó que muchos procesos queden impunes.[19] En efecto, como más adelante se precisará, la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú se creó cinco años después de la promulgación de la Ley No. 27309.

---

15 Entre ellos, Percy García Cavero y Ramiro Salinas Siccha.

16 SALINAS SICCHA, Ramiro. Op. Cit. pp. 1202 y 1210.

17 *Vid*. p. 921 del Diario de los Debates del Congreso de la República del 21 de junio de 2000.

18 Ibídem.

19 En el mismo sentido, MAZUELOS COELLO, Julio F. "Los delitos informáticos: Una aproximación a la regulación del Código Penal Peruano". En: "Revista Peruana de Doctrina y Jurisprudencia Penales". Lima: Grijley, 2001. p. 292.

d) Luego de la incorporación de estos delitos al Código Penal, en cada periodo legislativo se presentaron diversas propuestas que apuntaban a endurecer las penas, crear nuevas modalidades delictivas, mejorar la redacción de los tipos penales siguiendo los lineamientos internacionales que año a año se venían desarrollando o mejorar las unidades especiales a cargo de su investigación y juzgamiento:[20]

- En el Periodo 2000-2001, se presentó un proyecto de ley a través del cual se intentó adicionar la pena de inhabilitación a los delitos informáticos.[21]

- En el Periodo 2001-2006, se presentaron dos proyectos legislativos para aumentar las penas de los delitos informáticos,[22] tres proyectos para crear nuevas modalidades de delitos informáticos,[23] y uno para incorporar este tipo de ilícitos al Código de Justicia Militar Policial.[24]

- En el Periodo 2006-2011, se presentaron tres proyectos de ley para crear un cuerpo normativo especializado en delitos informáticos[25] y uno para regular los sistemas informáticos a fin de prevenir la comisión de este tipo de ilícitos.[26]

e) Durante la década posterior a la incorporación de los delitos informáticos al Código Penal, el número de estas conductas ilícitas se incrementaron. Así, entre enero de 2000 y diciembre de 2010, se registraron 975 denuncias por delitos informáticos en 27 distritos judiciales pero sólo se formalizaron el 32.3% de aquellas.[27] El Observatorio de Criminalidad del Ministerio Público registró la siguiente información que nos permite explicar las razones que justificaron la tipificación de nuevas modalidades de delitos cometidos a través de medios informáticos:

Ilícito	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Delitos Informáticos	24	26	29	44	57	81	81	109	112	189	223

Cuadro 2

---

20 En este análisis no se ha considerado el periodo 2011-2016 pues se analizará de manera conjunta con la Ley de Delitos Informáticos y su posterior modificación.

21 Proyecto de Ley No. 01744 del 03 de mayo de 2001.

22 Proyectos de Ley No. 02226 del 13 de marzo de 2002 y 11402/2004 del 10 de setiembre de 2004.

23 Proyectos de Ley No. 07197 del 13 de junio de 2003, 07807 del 12 de agosto de 2003 y 10079 del 17 de marzo de 2004.

24 Proyecto de Ley No. 11346/2004 del 06 de setiembre de 2004.

25 Proyectos de Ley No. 01318/2006 del 21 de mayo de 2007, 01828/2007 del 31 de octubre de 2007 y 03083/2008 del 12 de marzo de 2009.

26 Proyecto de Ley No. 04279/2010 del 02 de setiembre de 2010.

27 OBSERVATORIO DE CRIMINALIDAD DEL MINISTERIO PÚBLICO. "Delitos informáticos registrados por el Ministerio Público. Enero 2000 – Diciembre 2010". En: "Persecución estratégica del delito". Año 02. No. 02. Febrero 2011. p. 8.

Número de delitos registrados a nivel nacional por el Ministerio Público entre el 2000 y el 2010. Fuente: Observatorio de Criminalidad del Ministerio Público (2011). Elaboración propia.

El referido Observatorio disgregó la información expuesta en el Cuadro 2 según la incidencia delictiva acontecida en los distritos judiciales. Así, podemos encontrar que los distritos judiciales con mayor incidencia delictiva fueron: Lima (567), Amazonas (97), Huaura (69), Callao (25), Cusco (23), Arequipa (21) y La Libertad (21). Estos distritos registraron en una década, el 84.4% de los delitos informáticos cometidos a nivel nacional. En oposición, los distritos judiciales con menor incidencia fueron: Ancash (4), Pasco (3), Huancavelica (2), Cañete (1) y Ucayali (1). Estos cinco distritos registraron el 1.1% de los delitos informáticos cometidos a nivel nacional.

Trece años después, el Legislador creó el **Delito de Tráfico Ilegal de Datos** (Art. 207-D CP). Este artículo fue incorporado al Capítulo de Delitos Informáticos del Código Penal por la Ley No. 30076 del 19 de agosto de 2013. Como se recordará, esta Ley fue promulgada con el objeto de combatir la inseguridad ciudadana, razón por la cual se modificaron 28 artículos del Código Penal y se crearon 3 delitos, entre ellos, el delito de tráfico ilegal de datos pues el Legislador consideró que uno de los problemas relacionados a la inseguridad ciudadana se encontraba relacionado con la comercialización indebida de información.[28] Lamentablemente, la redacción de esta norma era tan amplia que podía castigarse incluso las actividades realizadas por las agencias de medios o publicidad a través de las *mailing list*.

2.2. Breve recuento sobre los cambios normativos relacionados a los delitos tradicionales cometidos a través de las Nuevas Tecnologías

Poco tiempo después de la incorporación de los primeros delitos informáticos al Código Penal, el Legislador consideró necesario modificar algunos ilícitos y agravar otros tantos para evitar que las Nuevas Tecnologías sean empleadas como medios para la comisión de otros delitos. De este modo, progresivamente se realizaron las siguientes modificaciones del Código Penal:

a) **Pornografía Infantil** (Artículo 183-A CP) y **Turismo Sexual Infantil** (Artículo 181-A CP).- El 26 de mayo de 2001, se creó el delito de pornografía infantil; sin embargo, mediante la Ley No. 28251 del 08 de junio de 2004, este ilícito fue modificado para precisar que la difusión a través del internet también es punible y así evitar lagunas legislativas que pudiesen generar cualquier tipo de impunidad. Esta misma norma creó el delito de turismo sexual infantil y precisó que una de las modalidades a sancionar sería aquella en el que se emplee Internet para su promoción. He de precisar

[28] En el Proyecto de Ley No. 2129/2012 del 16 de abril de 2013, presentado por el Congresista Jaime Delgado Zegarra, se señala que "Actualmente uno de los problemas existentes es el de la comercialización indebida de información. En estos lugares, identificados como las zonas comerciales de la Av. Wilson, Polvos Azules, Av. Argentina entre otros no tan recurridos, cualquier persona puede adquirir a precios asequibles bases de datos completas empleadas para la sistematización de datos por sectores de la industria o el comercio. Lo preocupante es que más allá de la aparente impunidad con que los traficantes pueden realizar las transacciones comerciales ilegales de venta de bases de datos, la vulnerabilidad de nuestra información queda reflejada en lo fácil que es obtener esta base de datos de primera fuente para su posterior venta ilegal".

que la Ley No. 30096 individualizó el empleo de las tecnologías de la información o de la comunicación como un agravante.

b) **Penalización de la clonación o adulteración de terminales de telefonía celular** (Art. 222-A CP).- Este artículo fue incorporado al Código Penal por la Ley No. 28774 del 07 de julio de 2006 en respuesta al alto índice porcentual de hurtos de celulares registrado un año antes. Según el legislador, de 28,814 hurtos de menor cuantía, la Policía constató que 14,804 eran celulares (64.88%) los cuales –y en esto se fundamenta la creación de este tipo penal– serían utilizadas por los delincuentes para cometer otros actos delictivos como extorsión, secuestro y robo.[29]

c) **Apología al delito de terrorismo** (Artículo 316 CP).- Este artículo fue modificado por el Decreto Legislativo No. 982 del 22 de julio de 2007, el cual incorporó como circunstancia agravante la apología al terrorismo a través de los medios de comunicación, incrementándose de 12 a 15 años la pena máxima para este tipo de actividades. Según la Exposición de Motivos del referido Decreto Legislativo, la agravación de la pena se debería a la apología al terrorismo se viene difundiendo peligrosamente a través de Internet ya que "tienen un alcance ilimitado a nivel nacional e internacional."

d) **Elusión de medidas tecnológicas, productos destinados a la elusión de medidas tecnológicas y servicios destinados a la elusión de medidas tecnológicas** (Art. 220-A, 220-B y 220-C CP).- La Ley No. 29263 del 02 de octubre de 2008 –modificada por la Ley No. 292316 del 14 de enero de 2009- incorporó estas tres modalidades delictivas propuestas por el Ejecutivo a través del Proyecto de Ley No. 2547/2007 del 30 de junio de 2008 a fin de cumplir con las obligaciones asumidas por el Estado peruano en el artículo 16 del Acuerdo de Promoción Comercial Perú – Estados Unidos (APC).[30]

e) **Ingreso Indebido de equipos o sistemas de comunicación, fotografía y/o filmación en centros de detención o reclusión** (Art. 368-A CP y 368-B CP). Estos artículos fueron incorporados por la Ley No. 29867 del 22 de mayo de 2012 con la finalidad de combatir los crímenes cometidos o direccionados desde el interior de los centros penitenciarios. En este sentido, el legislador consideró que diversas herramientas electrónicas podrían ser empleadas para la comisión de nuevos delitos pues el espacio físico no era un impedimento para ello, por lo que no sólo prohibió su uso sino que creó tipos penales que castigan el ingreso indebido de estos.

Como se explicará a continuación, frente a la complejidad en la investigación de estos nuevos delitos, la respuesta del Legislador estuvo acompañada de un cambio organizacional al interior de la Policía Nacional del Perú pero no del Ministerio Público.

---

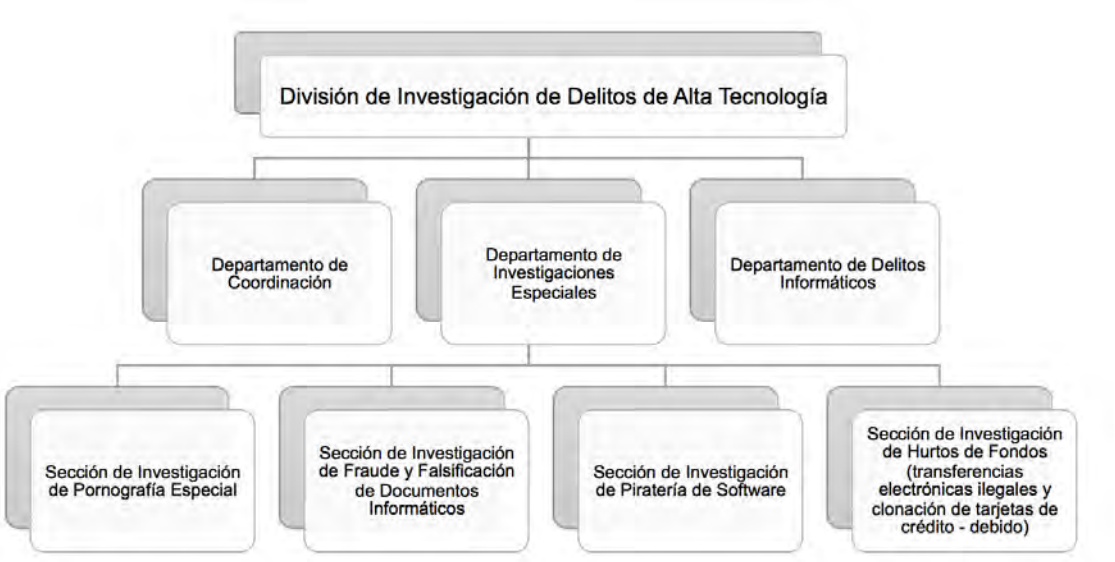
[29] Esta cifra corresponde al periodo enero – agosto de 2005 según la VII Dirección Territorial de la Policía Nacional del Perú. *Vid.* Proyecto de Ley No. 13855/2005-CR presentado el 10 de octubre de 2005 por el Célula Parlamentaria Aprista.

[30] Lamentablemente, la discusión generada a partir de la propuesta de incorporación de estos nuevos delitos al Código Penal fue ínfima. Así, en el Debate del 04 de setiembre de 2008, encontramos que al referirse al Art. 220-A CP únicamente se señala que: "Hay programas que están encriptados, que incluso se pueden bajar del satélite o de Internet por aquel que desarrolla programas para romper esa seguridad puesta por el titular de la propiedad intelectual".

2.3. La creación de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú

Durante los cinco años siguientes a la incorporación de los delitos informáticos al Código Penal, la investigación a nivel policial no se realizó por un ente especializado en materia informática sino que las pesquisas eran conducidas por el Ministerio Público en coordinación con Comisarías o Divisiones especializadas en otras materias: Estafas y otras Defraudaciones contra el Patrimonio, Robos, etcétera. Sin embargo, la Policía rápidamente cayó en cuenta que necesitaba crear una División capacitada en la investigación de estos nuevos ilícitos.

Es así que mediante Resolución Directoral No. 1695-2005-DIRGFN/EMG del 08 de agosto de 2005, la Dirección General de la Policía Nacional del Perú creó la División de Investigación de Delitos de Alta Tecnología – DIVINDAT para que esta Unidad especializada investigue la comisión de delitos informáticos y aquellos casos en los que se empleen medios informáticos para la comisión de otros delitos (difusión de pornografía infantil, fraudes electrónicos, hurtos de fondos, etcétera). De acuerdo al artículo 2 de la citada Resolución, la DIVINDAT está conformada por tres departamentos y una de ellas, a su vez, por cuatro secciones.



CUADRO 3
ORGANIGRAMA DE LA DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA DE LA POLICÍA NACIONAL DEL PERÚ. ELABORACIÓN PROPIA.

La creación de esta Unidad Policial ha permitido que se realicen un número significativo de investigaciones especializadas a nivel nacional.

Delito	2006	2007	2008	2009	2010	2011	2012	2013	TOTAL
Delitos Informáticos	77	73	128	125	161	184	147	85	980
Pornografía Infantil	53	72	43	65	90	151	136	49	659
Hurtos de Fondo	93	200	239	523	384	705	401	126	2671
Otros	53	58	53	223	299	468	184	242	1580
Total	276	403	463	936	934	1508	868	502	5890

Cuadro 4
Número de delitos registrados por la DIVINDAT entre el 2006 y el 2013.
Fuente: División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú. Elaboración propia.

Lamentablemente, existen problemas que impiden la obtención de mejores resultados: personal y logística insuficiente, infraestructura en malas condiciones[31] así como falta de capacitación y actualización permanente para el personal. En este sentido, una reforma íntegra para la persecución de delitos cometidos a través de las Nuevas Tecnologías debe traer consigo mejoras sustanciales para la Unidad Especializada que tiene como labor la investigación de estos ilícitos.[32]

III. ANÁLISIS DE LA LEY DE DELITOS INFORMÁTICOS (LEYES NO. 30096 Y 30171)

Entre agosto del 2011 y mediados del 2013, se presentaron ocho proyectos de ley que trajeron consigo la promulgación de la Ley No. 30096 del 22 de octubre de 2013 conocida como Ley de Delitos Informáticos (LDI).[33] Es importante destacar que la última propuesta recibida por el Congreso, remitida por el Poder Ejecutivo el 26 de julio de 2013 y rotulada como "Ley de represión de la Cibercriminalidad," es la que más similitud guarda con la referida Ley pese a que no alcanzó a ser debatida ni dictaminada por ninguna Comisión del

[31] En la pequeña oficina donde funciona la DIVINDAT antes operaba la OFICRI DIRINCRI.

[32] En este sentido, no basta con exigir la creación de protocolos de cooperación operativa para que la Policía Nacional coordine con el Ministerio Público, el Poder Judicial, el Pe-CERT, la ONGEI, los Organismos Especializados de las Fuerzas Armadas y los operadores del sector privado pues se necesita que el principal órgano a cargo de la investigación se encuentre constantemente capacitado y cuente con recursos humanos y logísticos que le permitan actuar eficaz y eficientemente.

[33] Proyectos de Ley No. 00034/2011 del 11 de agosto de 2011, 00307 del 05 de octubre de 2011, 01136 del 17 de mayo de 2012, 01257 del 14 de junio de 2012, 02112 del 12 de abril de 2012, 02112 del 12 de abril de 2013, 02398 del 21 de junio de 2013, 02482 del 17 de julio de 2013 y 02520 del 26 de julio de 2013.

Legislativo antes de ser discutido en el Pleno.[34] Es más, este Proyecto fue modificado en menos de seis horas y aprobado con un texto sustitorio que no fue puesto a debate a la sociedad civil, lo que generó gran malestar y preocupación a nivel nacional[35] debido a que la ambigüedad de su redacción ponía en riesgo la libertad de expresión y de prensa.

Pocas semanas después de la promulgación de la LDI, se propusieron cinco nuevos proyectos de ley que buscaban precisar la tipificación de los nuevos delitos al amparo del Convenio de Budapest o Convenio sobre la Ciberdelincuencia: Proyecto de Ley No. 02991/2013 del 25 de noviembre de 2013 presentado por Juan Carlos Eguren Neuenschwander, 02999/2013 del 27 de noviembre de 2013 presentado por Mauricio Mulder Bedoya, 03017/2013 del 29 de noviembre de 2013 presentado por Alberto Beingolea Delgado, 03048/2013 del 05 de diciembre de 2013 presentado por José Luna Gálvez y 03105/2013 del 18 de diciembre de 2013 presentado por Carmen Omonte Durand. Estos proyectos trajeron consigo el Debate en la Comisión Permanente del 12 de febrero de 2014, su exoneración de la doble votación y la promulgación de la Ley No. 30171 del 10 de marzo de 2014.

Antes de comenzar a analizar la LDI es necesario tener presente la diferencia entre sistemas y datos informáticos pues son términos empleados a lo largo de dicha norma. Así, la definición planteada por el Legislador peruano (Novena Disposición Final y Complementaria de la Ley) es idéntica a la propuesta por el Convenio de Budapest (Art. 1):

a) Sistemas informáticos.— Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

b) Datos informáticos.— Toda representación de hechos, 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.

En las líneas siguientes se comparará la tipificación prevista en cada uno de los capítulos de las dos Leyes con la regulación prevista en el Convenio de Budapest. Asimismo, se analizarán las diferentes normas con la finalidad de realizar algunos comentarios y propuestas de modificación.

---

[34] MORACHIMO RODRÍGUEZ, Miguel. "Deconstruyendo la Ley de Delitos Informáticos". En: Gaceta Constitucional. No. 71. Noviembre de 2013. p. 346. De acuerdo a este autor, también debe tenerse en cuenta que habrían existido presiones externas para su aprobación ya que "el otro antecedente directo de la Ley de Delitos Informáticos es la reunión de técnicos de la Conferencia de Ministros de Justicia de Iberoamérica (COMJIB), que se llevó a cabo en Lima a fines de junio (…) Se sabe que en la última reunión de Lima se avanzó sobre la redacción de un convenio sobre la ciberdelincuencia para la región, que ha pasado a evaluación y espera ser firmado por todos los países antes de que termine el 2013". Ibíd. p. 347.

[35] CISNEROS, Claudia. "Presidente: No firme la Ley Beingolea". Publicado en La República el 04 de octubre de 2013. Ver: http://www.larepublica.pe/columnistas/de-centro-radical/presidente-no-firme-la-ley-beingolea-04-10-2013. Última consulta realizada el 02 de junio de 2014.

3.1. Delitos contra datos y sistemas informáticos

La LDI derogó los Arts. 207-A, 207-B y 207-C CP, reemplazando a los dos primeros por los **Delitos de Acceso Ilícito** (Art. 2 LDI), **Atentado a la integridad de datos informáticos** (Art. 3 LDI) y **Atentado a la integridad de sistemas informáticos** (Art. 4 LDI). Siguiendo los parámetros establecidos por el Convenio de Budapest, se puede afirmar que el bien jurídico protegido por estos tipos penales es *la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.*[36]

Ley No. 30096	Ley No. 30171	Convenio de Budapest
Art. 2 LDI.- El que accede sin autorización a todo o en parte a un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.	**Art. 2 LDI.-** El que **deliberada e ilegítimamente** accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecida para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.	**Art. 2.-** 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 todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.
Art. 3 LDI.- Atentado a la integridad de los datos informáticos. El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.	**Art. 3 LDI.-** El que **deliberada e ilegítimamente daña,** introduce, borra, deteriora, altera, suprime o hace inaccesible datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.	**Art. 4.-** 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos. 2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

[36] En el mismo sentido, RUEDA MARTÍN, María Ángeles. "Cuestiones político – criminales sobre las conductas de hacking". En: Derecho Penal Contemporáneo - Revista Internacional No. 28. Setiembre de 2009. p. 174.

Art. 4 LDI.- El que, a través de la tecnología de la información o de la comunicación, inutiliza total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.	**Art. 4 LDI.-** El que **deliberada e ilegítimamente** inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.	**Art. 5.-** 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, daño, borrado, deterioro, alteración o supresión de daños informáticos.

Cuadro 5

Cuadro comparativo de los Delitos de Acceso Ilícito, Atentado a la integridad de datos informáticos y Atentado a la integridad de sistemas informáticos. Elaboración propia.

En los términos en que el **Delito de Acceso Ilícito** ha sido tipificado, podemos afirmar que se sanciona el *hacking blanco* o *mero intrusismo* pues sólo se requiere el acceso ilícito a través de la vulneración de las medidas de seguridad para su configuración. De este modo, por ejemplo, si estudiantes de Ingeniería Informática quieren poner en práctica sus conocimientos y demostrar que pueden sobrepasar las medidas de seguridad de determinadas empresas para estudiar sus puntos vulnerables, no lo podrán hacer (sin autorización previa) pues estarían cometiendo un acto delictivo pese a que no persigan una finalidad ilícita adicional (lucrar con su actividad o causar algún tipo de perjuicio). Esta modalidad delictiva es utilizada por otros ordenamientos como el de Portugal, Italia y Suiza.[37]

En primer lugar, tomando en consideración los *principios de fragmentariedad* y de *ultima ratio* del Derecho Penal, el Estado sólo debe intervenir frente a actuaciones que comporten una grave lesión de los bienes jurídicos protegidos y cuando las vías extra penales no sean lo suficientemente útiles para resarcir el daño ocasionado. Siguiendo estos parámetros, el *hacking blanco* no debería ser castigado penalmente pues se podría acudir a la vía civil para solicitar el resarcimiento por el derecho vulnerado. Pese a ello, si nuestro Legislador persiste en considerar que sí es necesaria su tipificación penal debería de diferenciarla de aquel tipo de *hacking* que persiguen otras finalidades delictivas (como la obtención de datos informáticos) y que reviste un grado de mayor lesividad pues sancionar con hasta 04 años de pena privativa de libertad todo tipo de *hacking* deviene en desproporcionado.

En segundo lugar, la Ley No. 30096 sancionaba el acceso ilegal (Art. 1 LDI) pero preveía que el agente realizaba esta conducta, vulnerando las medidas de seguridad establecidas, "sin autorización" o "excediendo lo autorizado". De igual forma, se castigaba el atentado contra los datos (Art. 2 LDI) y sistemas informáticos (Art. 3 LDI) ocasionados "a través de las tecnologías de la información o de la comunicación". La Ley No. 30171 corrigió este error pues los elementos del delito eran vagos e imprecisos, reemplazándolos por la expresión "deliberada e ilegítimamente" (sugerida por el Convenio de Budapest). Sin embargo, he de

[37] *Vid.* RUEDA MARTÍN, María Ángela. Op. Cit. p. 162.

precisar que es innecesario emplear el término "deliberadamente" en la tipificación de estos delitos pues el Art. 12 CP prevé que las penas establecidas por la ley se aplican siempre al agente de infracción dolosa –entiéndase, deliberada– ya que los ilícitos culposos son únicamente punibles en los casos expresamente previstos en la ley. Conviene anotar que el término "deliberadamente" es empleado en el CP en otros casos como secuestro (Art. 152 CP), extorsión (Art. 200 CP), rehusamiento a prestar información económica, industrial o comercial (Art. 242 CP) y falsedad de información presentada por un emisor en el mercado de valores (Art. 245 CP) pese a que dicho término no llega a exigir un elemento subjetivo de relevancia trascendente.

En tercer lugar, al equiparar la pena prevista para las dos modalidades de acceso ilícito –regulación que no fue recomendada por el Convenio de Budapest– se trasgrede el *principio de proporcionalidad de las penas*. En efecto, el Tribunal Constitucional ha reconocido que toda pena debe guardar proporción y correspondencia con el nivel de reprobabilidad jurídica y social del acto sancionado, es decir debe sancionar el acto en tanta dimensión como tan reprobable resulte el acto respecto a la persona responsable. Así, el reproche es distinto en estos dos escenarios pues en uno además de no tenerse autorización, se vulnera las medidas de seguridad del usuario mientras que en el segundo únicamente se excede la autorización conseguida. Este punto se ve reforzado con el hecho que el acceso ilegal no es penalmente relevante si el agente no ha vulnerado las medidas de seguridad establecidas para impedirlo. No obstante, en este último escenario, el agraviado podría acudir a vías extra penales como la civil para solicitar el resarcimiento del derecho vulnerado.

Finalmente, podemos apreciar que la pena también es desproporcional respecto a otros ilícitos similares previstos en nuestro ordenamiento. Por ejemplo, si comparamos el delito bajo análisis con el de violación de domicilio o el de violación de correspondencia podemos apreciar que el primero puede recibir hasta 4 años de pena privativa de libertad mientras que los otros dos delitos sólo hasta 2 años.

De otro lado, el Art. 3 de la LDI tipifica el **Delito de atentado a la integridad de datos informáticos** en las modalidades sugeridas en el Convenio de Budapest. Sin embargo, se aparta de este instrumento al incorporar los términos "introduce" y "hace inaccesible" a la redacción del tipo penal. En efecto, al sancionarse otro tipo de conductas como "daña", "borra", "deteriora", "altera" o "suprime" –que sí fueron recomendadas por el Convenio– la incorporación de las dos modalidades en comentario se convierten en inútiles. En efecto, ¿cuándo debería castigarse penalmente la "introducción" de datos informáticos? La respuesta está vinculada a una carencia de la norma: cuando se produzcan daños graves. Nuestra norma actual no lo prevé por lo que no tiene sentido y, de hecho, atenta contra el principio de lesividad del Derecho Penal, pues dicha modalidad *per se* no ocasiona daño alguno. Asimismo, sostengo que el término "hace inaccesible" es inútil por cuanto es una consecuencia de la modalidad "daña".

Por razones de política criminal, se puede diferenciar una conducta ilícita de otra. Así, por ejemplo, nuestro Código Penal diferencia entre el delito de daños (Art. 205 CP) y el daño como falta contra el patrimonio (Art. 444 CP). Esta diferencia es importante pues, entre otras razones, en el primer caso el autor puede recibir hasta 3 años de pena privativa de libertad y en el segundo, sólo 40 a 120 jornadas de prestación de servicio comunitario. Esta diferencia radica en el monto del daño ocasionado pues si supera una remuneración mínima vital (S/. 750.00 nuevos soles, al año 2014) será delito; de lo contrario, únicamente

será una falta. Establezco esta diferencia pues la redacción actual del Delito de atentado a la integridad de datos informáticos no diferencia la gravedad del daño causado pese a que fue recomendado en el segundo párrafo del Art. 4 del Convenio de Budapest. De este modo, una correcta tipificación debería precisar que será un acto ilícito siempre y cuando ocasione un *daño grave.*[38]

Lo expuesto en el párrafo anterior, también nos permite comparar la sanción máxima prevista para el delito de atentado contra la integridad de datos informáticos (06 años) con la del delito de daños (03 años). Así, al no sancionarse únicamente los daños informáticos graves, de manera absurda, casos insignificantes podrían recibir una pena mayor que un acto grave de daños.

Finalmente, la LDI también sanciona el **Delito de atentado a la integridad de sistemas informáticos** conocido también como sabotaje informático.[39] En este caso, debemos partir comparando los Arts. 3 y 4 del Convenio de Budapest pues el primero sanciona el dañar, borrar, deteriorar, alterar o suprimir los datos informáticos. En cambio, el segundo castiga la obstaculización grave del funcionamiento de un sistema informático cuando se produzca a través de las conductas descritas en el artículo anterior –dañar, borrar, deteriorar, alterar o suprimir datos informáticos- o a través de la introducción o transmisión de datos informáticos. La redacción del Convenio es coherente; nuestra Legislación, no. Sostengo que es coherente porque en esta regulación sí tiene sentido las modalidades de introducción y transmisión pues son el medio para la obstaculización grave del sistema información. Si bien una conducta podría originar la configuración de ambos tipos delictivos, lo cierto es que nos encontraríamos frente a un concurso aparente de delitos pues el especial absorbe al general.

Nuestra Legislación es incoherente pues al no incorporar la segunda parte del Art. 4 del Convenio –referido al daño, borrado, deterioro, alteración, supresión, introducción o transmisión de datos informáticos–, posibilita que cualquier acto material configure el delito de atentado a la integridad de sistemas informáticos. En efecto, no se precisa que este atentado debe ser producto de un acto ilícito informático previo. Así, si una persona impide físicamente que otra acceda a su sistema informático, de acuerdo a nuestra Legislación vigente, se configuraría el delito de atentado a la integridad de sistemas informáticos. De igual forma, si entendemos que un sistema informático requiere, cuando menos, de un equipo físico (*hardware*), el delito de atentado a la integridad de sistemas informáticos se configuraría si una persona destruye a golpes dicho equipo físico pues inutilizaría parcialmente los datos informáticos que el agraviado pudo subir él. Este tipo de interpretación, aun cuando parece absurda, es posible por la mala técnica legislativa empleada y por los incipientes conocimientos en materia informática que muchos operadores jurídicos adolecen.

Para finalizar esta sección, debo recomendar que una eventual reforma tome en consideración las propuestas aquí plasmadas. De lo contrario, se podrían criminalizar actos de escasa relevancia y dejar impunes delitos graves por los defectos normativos expuestos.

---

[38] En igual sentido: MORACHIMO RODRÍGUEZ, Miguel. Op. Cit. p. 348.

[39] PALOMINO RAMÍREZ, Walter. "El intrusismo y los otros delitos informáticos regulados en la Ley No. 30096". En: Gaceta Penal y Procesal Penal. Tomo No. 56. p. 150.

3.2. Delitos informáticos contra la indemnidad y libertad sexuales

La LDI tipificó el *Child Grooming* a través de la creación del **Delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos** (Art. 5 LDI). Como se desarrollará a continuación, esta propuesta no es parte del Convenio de Budapest ni existe consenso sobre la necesidad de contar con este tipo penal.

Ley No. 30096	Ley No. 30171	Ley No. 30171
Art. 5 LDI.- El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.	Art. 5 LDI.- El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.	Art. 183-B CP.- El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación de conforme a los numerales 1, 2 y 4 del artículo 36. Cuando la víctima tiene entre catorce y menos de dieciocho de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36.

CUADRO 6

CUADRO COMPARATIVO DEL DELITO DE PROPOSICIONES A NIÑOS, NIÑAS Y ADOLESCENTES CON FINES SEXUALES POR MEDIOS TECNOLÓGICOS Y SIN ELLOS. ELABORACIÓN PROPIA

La Ley No. 30096 creó el **Delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos**, el cual no forma de las recomendaciones del Convenio de Budapest pero sí del Convenio del Consejo de Europa sobre la Protección de Niños contra la Explotación Sexual y el Abuso Sexual del 25 de octubre del 2007. Según esta norma, es un acto delictivo contactar a un menor de 14 años para solicitar u obtener material pornográfico o para llevar a cabo actividades sexuales con él. La redacción nos permite afirmar que se sanciona el mero contacto, sin importar que se llegue a solicitar, obtener el material pornográfico o se lleven a cabo las actividades sexuales. De este modo, nuestro Legislador ha adelantado la barrera de punibilidad de manera peligrosa pues ha convertido el *child grooming* en un delito de peligro abstracto al no requerir un riesgo inminente. En este sentido, recomiendo seguir los parámetros establecidos en el Art. 23 del Convenio del Consejo de Europa pues sugiere:

> Cada parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito el hecho de que un adulto, mediante las tecnologías de la información y la comunicación, proponga un encuentro a un niño (…) con el propósito de obtener cualquier de los delitos tipificados con arreglo al apartado 1.a del artículo 18 o al apartado 1.a del artículo 20, cuando a dicha proposición le hayan seguido actos materiales conducentes a dicho encuentro.[40]

Es decir, tipifica un delito de peligro concreto ya que dichos actos materiales sí ponen en riesgo bienes jurídicos de relevancia penal.

Una crítica que recibió este Delito es que si bien se sancionaba las proposiciones efectuadas a través de medios informáticos, lo cierto es que si el agente no utilizaba estos medios y sí un conversación física directa, por ejemplo, el hecho no era delictivo. La promulgación de la Ley No. 30171 superó este *impasse* al crear el Delito de proposiciones a niños, niñas y adolescentes e incorporarlo al Código Penal a través del Art. 183-B. Sin embargo, la sanción punitiva regulada es idéntica al de proposiciones por medios tecnológicos por lo que, hoy en día, coexisten dos normas penales que regulan la misma conducta delictiva.

Un punto adicional que debo cuestionar está relacionado al elemento "engaño" previsto en el segundo párrafo del delito de proposiciones (ordinarias o a través de medios tecnológicos). Después de muchos años de discusión, el Tribunal Constitucional declaró que los mayores de 14 y menores de 18 años pueden mantener relaciones sexuales ya que les asiste el derecho a la libertad sexual –contrario a la indemnidad sexual que protege a los menores de 14 años–.[41] Siendo esto así, no cualquier engaño debe ser castigado sino únicamente aquel idóneo para lograr el consentimiento de la víctima. De este modo, información falsa relacionada a la edad, la condición económica, la orientación sexual, el aspecto físico o promesas que no se cumplirán serán irrelevantes penalmente. En cambio, si el autor suplanta virtualmente la identidad de la pareja de la víctima para obtener el acceso ilícito, sí será susceptible del reproche punitivo.[42]

Finalmente, al igual que en los delitos previamente analizados, encuentro que la pena prevista es desproporcional en comparación con otros ilícitos en los que se protege a menores de edad.[43] Así, el delito de proposiciones con fines sexuales –que, como se ha analizado, es de peligro abstracto pues, en principio, no afecta concretamente el bien jurídico protegido– prevé una pena máxima mayor (08 años) al delito de exposición a peligro o abandono de un menor de edad (04 años) –ilícito que es de peligro concreto pues

---

[40] *Vid.* DÍAZ CORTEZ, Lina Mariola. "El nuevo delito de contacto TIC preordenado a la actividad sexual con menores en España". En: Derecho Penal Contemporáneo. Revista Internacional No. 38. Enero-Marzo de 2012. pp. 5-43.

[41] Sentencia del Tribunal Constitucional recaída en el Expediente No. 00008-2012-PI/TC del 24 de enero de 2013.

[42] En similar opinión se pronuncia la Corte Suprema de la República en el Recurso de Nulidad No. 1628-2004-Ica. En dicho pronunciamiento ejemplifica el Precedente Vinculante establecido en los siguientes términos: "El agente engaña al sujeto pasivo sobre su identidad aprovechando su parecido físico con la pareja sentimental de la víctima. Si esta es afectada por el error y se relaciona sexualmente con el agente, a quien cree su pareja sentimental, el tipo penal del artículo 175 del Código Penal se habrá configurado. Por el contrario, si el agente hace promesas al sujeto pasivo para que este acepte el acceso carnal, y luego dichas promesas no se cumplen, no se dará el delito".

[43] En el mismo sentido, MORACHIMO RODRÍGUEZ, Miguel. Op Cit. p. 350.

sí se necesita una grave amenaza al bien jurídico– y al delito de seducción (05 años) –delito de resultado pues se configura cuando el agente mantiene relaciones sexuales con un menor de edad mediante engaño–.

3.3. Delitos informáticos contra la intimidad y el secreto de las comunicaciones

Si bien la Ley No. 30096 derogó el Art. 204-D CP creado pocos meses antes e incorporó el mismo ilícito bajo el nombre de **Delito de Tráfico ilegal de datos** (Art. 6 LDI), lo cierto es que la Ley No. 30171 lo volvió a derogar poco tiempo después para incorporarlo nuevamente al Código Penal bajo el Art. 154-A. Bajo el mismo capítulo, la actual LDI sanciona también el **Delito de Interceptación de datos informáticos** (Art. 7 LDI)

Ley No. 30096	Ley No. 30171	Convenio de Budapest
Art. 6 LDI.- El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar o patrimonial, laboral o financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.	Derogó el Art. 6 LDI. Art. 154-A CP.- El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años. Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior.	No previsto

Art. 7 LDI.- El que a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años. La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia. La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.	Art. 7 LDI.- El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años. La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública. La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, seguridad o soberanía nacionales. Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.	Art. 3.- 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 en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos actos informativos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otros sistemas.

Cuadro 7

Cuadro comparativo de los Delitos de Tráfico ilegal de datos y de Interceptación de Datos Informáticos. Elaboración propia.

De la manera en la que el **Delito de Tráfico ilegal de datos** (Art. 154-A CP) se encuentra actualmente redactado, se puede afirmar que el bien jurídico protegido es la intimidad, razón por la cual la Ley No. 30171 derogó el Art. 6 de la LDI e incorporó este ilícito en el Capítulo referido a los delitos de violación a la intimidad. Esta técnica legislativa es correcta pues sí encuentra sustento sistemático y es proporcional con relación a la pena prevista para el delito de violación a la intimidad. Así, quien comete esta conducta será sancionado con hasta 2 años de pena privativa de libertad pero quien trafica o comercializa datos personales puede recibir hasta 4 años. Hay que agregar que, además, el Delito de Tráfico Ilegal de datos se persigue de oficio mientras que el resto de delitos previsto en dicho Capítulo (violación

de la intimidad, revelación de la intimidad personal y familiar y uso indebido de archivos computarizados) se impulsan por acción privada (querella). Esta diferencia trae consigo el siguiente problema: ¿Qué sucedería si el agraviado de quien el agente está comercializando la información privada considera que su intimidad no ha sido vulnerada o no le interesa su persecución? Aquí, procesalmente, existe un problema pues si consideramos que se ha violado su intimidad al amparo del Art. 154 CP, el agraviado tiene el derecho de querellar o no al agresor. Si esto es así, y decide no hacerlo, ¿por qué el Estado se irroga la facultad de perseguir públicamente el delito posterior, es decir, la comercialización de su información?

De otro lado, respecto al **Delito de Interceptación de datos informáticos**, se aprecia que al precisarse que se castigan las interceptaciones deliberadas e ilegitimas –no previsto inicialmente en la LDI-, la tipificación del primer párrafo es acorde al Convenio de Budapest. Asimismo, las penas previstas por este delito son similares a las del Delito de interferencia telefónica (Art. 162 CP) por lo que supera las críticas al principio de proporcionalidad de las penas que hemos venido realizando.

El problema que percibo se encuentra relacionada a las agravantes previstas en los párrafos subsiguientes. En el primero, como resalta Morachimo[44], serán fueros extrapenales los que deberán decidir si la información clasificada a la que se accedió tiene o no interés público que la haga merecedora de publicidad. En estos casos, de no derogarse este extremo de la norma, los imputados deberían deducir una cuestión prejudicial[45] a fin que un juez constitucional dictamine sobre la naturaleza de la información a la que accedió. Esto garantizará que el sistema penal no castigue actos que otras vías podrían declarar lícitos.

Finalmente, el tercer párrafo prevé que cuando el delito "comprometa" la defensa, seguridad o soberanía nacionales[46] nos encontraremos frente a un ilícito agravado que podrá ser castigado con hasta 10 años de pena privativa de libertad. Al igual que en el caso anterior, esta agravante tampoco fue recomendada por el Convenio de Budapest. Ahora bien, al analizar la expresión "compromete" podemos afirmar que nuestro Código Penal la emplea únicamente al desarrollar una de las modalidades del proxenetismo: el que compromete a una persona para entregarla a otro con el objeto de tener acceso carnal. Así, no existe un ilícito de naturaleza análoga con el cual podamos comparar los artículos incorporados por la LDI. Por ello, deberemos de entender el verbo "comprometer" como "exponer o poner en riesgo a alguien o algo en una acción o caso aventurado". Si esto es así, para que se sancione esta modalidad se requerirá la acreditación de un peligro concreto –no abstracto– contra la defensa, seguridad o soberanía estatal; lo que es innecesario al ya existir un delito que sanciona este tipo de actuaciones: el delito de espionaje (Art. 331 CP). En consecuencia, considero que estas dos agravantes deberían ser suprimidas pues desnaturalizan los alcances del delito bajo análisis.

---

44 MORACHIMO, Miguel. Op. Cit. p. 350.

45 Art. 5 CPP.- 1. La cuestión prejudicial procede cuando el Fiscal decide continuar con la Investigación Preparatoria, pese a que fuere necesaria en vía extra - penal una declaración vinculada al carácter delictuoso del hecho incriminado.

2. Si se declara fundada, la Investigación Preparatoria se suspende hasta que en la otra vía recaiga resolución firme. Esta decisión beneficia a todos los imputados que se encuentren en igual situación jurídica y que no la hubieren deducido.

4. De lo resuelto en la vía extra - penal depende la prosecución o el sobreseimiento definitivo de la causa.

46 La LDI también incorpora esta agravante en el delito de interferencia telefónica.

3.4. Delitos informáticos contra el patrimonio

El delito de **Fraude informático** fue incorporado por el Art. 8 LDI y modificado poco tiempo después para que guarde relación con los términos empleados por el Convenio de Budapest. En esta ocasión la crítica también viene dada por reconocer que los términos en que el delito está planteado posibilitan el inicio de una investigación y sanción frente a hechos que si bien pueden producir un daño en su contra, este no es significativo.

Ley No. 30096	Ley No. 30171	Convenio de Budapest
Art. 8 LDI.- El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.	Art. 8 LDI.- El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.	Art. 8.- Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. la introducción, alteración, borrado o supresión de datos informáticos; b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Cuadro 8
Cuadro comparativo del Delito de fraude informático. Elaboración propia.

3.5. Delitos informáticos contra la fe pública

Frente a cualquier tipo de falsedad que no encuentra tipificación específica en nuestro ordenamiento, se acude al delito de falsedad genérica (Art. 438 CP)[47] para evitar que un acto de esta naturaleza quede impune. De hecho, los **delitos informáticos cometidos**

[47] Art. 438 CP.- El que de cualquier otro modo que no esté especificado en los Capítulos precedentes, comete falsedad simulando, suponiendo, alterando la verdad intencionalmente y con perjuicio de terceros, por palabras, hechos o usurpando nombre, calidad o empleo que no le corresponde, suponiendo viva a una persona fallecida o que no ha existido o viceversa, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años.

contra la fe pública han venido siendo tratados como delitos de falsedad genérica. Sin embargo, para evitar la sobre criminalización, recomiendo que la lectura que se realice de este tipo penal se efectúe al amparo de los derechos y garantías que como ciudadanos nos asiste. De otro lado, esta norma innecesariamente prevé que el daño originado con esta actuación también puede ser moral –además de la patrimonial–, razón por la cual este extremo debería derogarse ya que el Derecho Penal no puede salvaguardar la moralidad como uno de los bienes jurídicos concretos que protege al ser un concepto ambiguo. En tal sentido, se hubiese preferido que el Art. 9 LDI sancione este tipo de ilícitos siempre y cuando ocasionen "algún perjuicio" y no que lo reduzca al patrimonial y al moral.

Ley No. 30096	Ley No. 30171	Convenio de Budapest
Art. 9 LDI.- El que, mediante las tecnologías de la información o de la comunicación, suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.	No hubo modificación	Art. 7.- Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e intelegibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Cuadro 9
Cuadro comparativo del Delito de Suplantación de Identidad. Elaboración propia.

A modo de síntesis, en primer lugar, debo indicar que en este artículo he expuesto brevemente el desarrollo normativo que trajo consigo la creación de los delitos informáticos hacia el año 2000 y, durante la década siguiente, la incorporación o modificación de delitos en los que se empleaban Nuevas Tecnologías para su comisión. Si bien nuestro Legislador se preocupó por penalizar este tipo de conductas y ciertas instituciones como la Policía Nacional han intentado luchar contra el cibercrimen a través de la especialización de sus divisiones, lo cierto es que muchas instituciones como el Ministerio Público y el Poder Judicial han quedado rezagadas por lo que también deberían modernizarse y especializar a sus operadores jurídicos pues las técnicas que se requieren para la investigación y persecución de este tipo de ilícitos no es igual a la de los delitos tradicionales. Algunos países como Paraguay y Argentina ya lo han entendido y han creado Fiscalías Especializadas en Delitos Informáticos.

En segundo lugar, el incremento desmesurado de los delitos informáticos y los cometidos con las Nuevas Tecnologías en esta época obliga al Estado a adoptar un marco punitivo severo pero que respete los lineamientos constitucionales que nutren el Derecho Penal. Así, se debe mejorar la redacción de los actuales tipos penales previstos en la Ley de Delitos Informáticos para no seguir usando expresiones ambiguas que permitan castigar el ejercicio regular de nuestros derechos civiles. Se debe respetar el principio de lesividad y de *ultima*

ratio del Derecho Penal pues sólo merecen reproche penal aquellas conductas que gravemente afecten o pongan en riesgo concreto un bien jurídico protegido. También se debe evitar el populismo punitivo pues no se trata de incrementar las penas de manera draconiana sino que se debe analizar nuestro ordenamiento de manera sistemática para que estas sanciones guarden relación con las previstas por otros delitos de naturaleza jurídica similar.

Finalmente, considero que se deben impulsar los canales de comunicación y diálogo con nuestras autoridades políticas pues esto permitirá enriquecer la lucha contra este nuevo fenómeno delictivo mundial y evitar que los cambios normativos se realicen a puerta cerrada y sin la participación u opinión ciudadana. De la misma forma, es necesario compartir este diálogo con la sociedad civil pues son ellos quienes están expuestos a estos delitos y serán ellos quienes los denuncien y colaboren con las autoridades para esclarecer los hechos delictivos. Esta tara es ardua pero es necesario emprenderla para ejercer libremente nuestros derechos y exhortar que se respeten nuestras garantías. ■