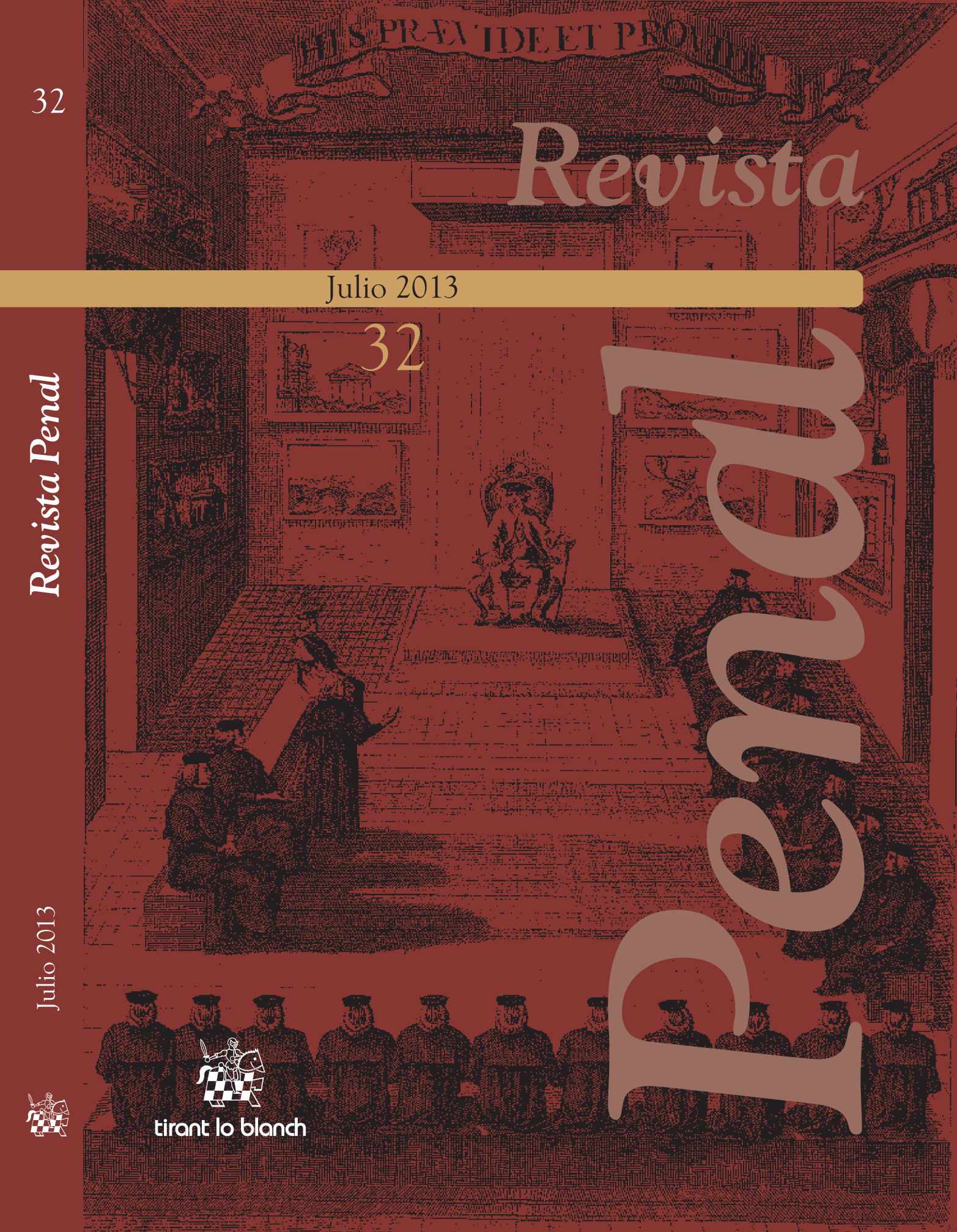
32
Revista
Julio 2013
32
Penal
Revista Penal
Julio 2013
tirant lo blanch

Revista Penal

Número 32

Sumario

Doctrina:

– Aspectos problemáticos del delito de tráfico de órganos, por *Carmen Alastuey Dobón* 3
– Derecho Penal mínimo de los bienes jurídicos colectivos (Derecho Penal mínimo máximo) por *Mercedes Alonso Álamo* 23
– Investigando crímenes internacionales ante la Corte Penal Internacional: ¿existe una estrategia de enjuiciamiento coherente y comprehensiva?, por *Kai Ambos e Ignaz Stegmiller*..... 41
– La protección de sistemas de información crítica y la Ley 53/07 de la República Dominicana sobre crímenes y delitos de alta tecnología, por *Désirée Barinas Ubiñas* 60
– Securitización, por *María Laura Böhm*..... 72
– Peligrosa irretroactividad y retroactividad para los peligrosos o socialmente indeseables por *Emiliano Borja Jiménez* 91
– La conducción tras el consumo de alcohol y drogas tóxicas: el inciso segundo del artículo 379.2 CP como infracción formal por *Luis Cáceres Ruiz*..... 113
– Reflexiones sobre los actos neutrales y la cooperación delictiva desde los criterios de la imputación objetiva, por *María José Cuenca García* 141
– La protección penal del medio ambiente a través de los delitos de incendio, por *Pastora García Álvarez y Carmen López Peregrín* 153
– El terrorismo al amparo de la reforma efectuada por la Ley Orgánica 5/2010: concepto y elementos por *Elena Núñez Castaño*..... 179
– La imprescriptibilidad de las violaciones contra los derechos humanos cometidas en Uruguay (1973-1985) por *Jan-Michael Simon y Pablo Galain Palermo* 222
– CATORCE (14) AÑOS. Una propuesta de criterio "vinculante", intocable desde los actuales postulados del Derecho penal de la seguridad, para la fijación del límite mínimo de la Ley reguladora de la responsabilidad penal del menor, por *María A. Trapero Barreales* 250

Sistemas penales comparados: Corrupción en el sector público y privado (Corruption in public and private sector) 283

Crónicas:

– "Cruce de caminos". Laudatio en honor de Hernán Hormazábal y José Ramón Serrano-Piedecasas Fernández, por *Eduardo Demetrio Crespo* 331
– La pena de muerte en el International Forum on Crime and Criminal Law in the Global Era (IFCCLGE) por *Miguel Ángel Núñez Paz* 335
– Notas sobre genoma humano y Derecho penal y comentarios a las XX Jornadas de Derecho y Genoma Humano, organizadas por la Cátedra Interuniversitaria de Derecho y Genoma Humano, Director Carlos M. Romeo Casabona, Bilbao 21 y 22 mayo 2013 por *Francisco Muñoz Conde*..... 337

Universidad de Huelva · Universidad de Salamanca · UCLM Universidad de Castilla-La Mancha · Universidad Pablo de Olavide Sevilla Año 1997 · Cátedra de Derechos Humanos Manuel de Lardizábal · Santander

tirant lo blanch

Publicación semestral editada en colaboración con las Universidades de Huelva, Salamanca, Castilla-La Mancha, Pablo Olavide de Sevilla y la Cátedra de Derechos Humanos Manuel de Lardizábal.

www.revistapenal.com

EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELFS.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email:tlb@tirant.com
http://www.tirant.com
Librería virtual: http://www.tirant.es
DEPÓSITO LEGAL: B-28940-1997
ISSN.: 1138-9168
IMPRIME: Guada Impresores, S.L.
MAQUETA: PMc Media

La protección de sistemas de información crítica y la Ley 53/07 de la República Dominicana sobre crímenes y delitos de alta tecnología

Désirée Barinas Ubiñas

Revista Penal, n.º 32. - Julio 2013

Ficha técnica

Autor: Désirée Barinas Ubiñas
Adscripción institucional: Máster en Derecho multimedia e informático (Université Panthéon-Assas Paris II) Doctora en Derecho (Universidad del País Vasco-UPV/EHU)

Abstract It is undeniable the impact of information and communication technology in the development of modern society, becoming a common international concern the protection against cybercrime. All over the world legislations have been adapted in order to restructure the defense of legal interests traditionally recognized, raising the question of whether we are witnessing the birth of new interests that deserve the attention of criminal law. In most European countries, as it is the case of Germany, Spain and Italy, the legal framework has been adapted to strengthen the protection of legal interests already established as traditionally important; while the United States reform has been more specific and focalized in protecting patrimonial rights and interests. In the European context, the 2012 reform of the French legislation reinforces a different model, in which not only the existing criminal law is amended but new offenses are created to protect automated data processing systems. This reform followed the model that had already been incorporated into the legislation of Dominican Republic in 2007, a pioneer in the field, which, besides from the protection given by the general criminal law, counts with a law of high-tech crimes that establishes the protection not only of traditional legal interests, but also information systems and data. This legislation deserves special attention, although it follows the guidelines of the Convention on Cybercrime 2001 and the Resolution AG/RES 2004 (XXXIV/O/04) of the Organization of American States on the adoption of a comprehensive Inter-American strategy to combat threats to cybersecurity, it introduces certain criminal offenses that outrun the previous ones towards the construction of a comprehensive and complete legal protection layers against crimes, committed through the use of a computer and against the computer, that might inspire other legislations. It recognizes the need to protect the tools that drive the interactions and the functioning of this Information Society in the Digital age.
Key Words: Cybercrime - Cybersecurity - Computer - Criminal Law - Data - Information system - Information and communication technology (ICT) - Legal interests

Resumen: El impacto de las tecnologías de la información y de la comunicación en el desarrollo de la sociedad actual es innegable, transformándose en una preocupación común a nivel internacional la lucha contra la criminalidad informática. Se busca así proteger dentro de este entorno digital bienes jurídicos tradicionalmente tutelados, planteándose a su vez la cuestión de dilucidar si estamos frente al nacimiento de bienes jurídicos de nuevo cuño que merecen la atención del Derecho penal. En Europa la mayoría de los países han modificado su marco legal a fin de reforzar la protección de bienes jurídicos tradicionalmente tutelados, siendo el caso de Alemania, España e Italia, mientras en Estados Unidos de Norteamérica la respuesta ha sido más sectorial y focalizada en la protección de bienes jurídicos de corte patrimonial. En el contexto europeo, Francia afianza con la reforma legislativa de 2012 un modelo diferente, en el que no tan solo se modifican preceptos penales existentes sino que se crean nuevos tipos penales que viene a proteger los sistemas de tratamiento automatizado de datos. Este modelo había ya sido incorporado en la legislación de República Dominicana en 2007, pionera en la materia, donde, independientemente de la protección penal general, se introduce una ley de delitos

y crímenes de alta tecnología en la que se busca tutelar, además de bienes jurídicos tradicionales, los sistemas de información y datos. Merece especial atención esta legislación, que si bien sigue los lineamientos del Convenio de cibercriminalidad de 2001, así como la Resolución AG/RES 2004 (XXXIV/O/04) de la Organización de Estados Americanos sobre la adopción de una estrategia interamericana integral de seguridad cibernética, introduce ciertos tipos penales que los desbordan buscando estructurar una capa de protección integral contra delitos realizados a través de la informática y contra la informática que podrían servir de ejemplo a otras legislaciones. En ella se reconoce la necesidad de proteger las herramientas que motorizan las interrelaciones y el funcionamiento de la Sociedad de la información en la Era digital.
Palabras clave: Acceso Ilícito - Bienes jurídicos - Cibercriminalidad - Sistemas de información - Datos - Delitos de contenido - Delitos informáticos - Tutela penal-Tecnologías de la información y de la comunicación (TIC)

Recepción del artículo: 20-01-2013
Evaluación favorable: 17-02-2013

(I)

Los países europeos se han visto en la necesidad de replantear y desarrollar un nuevo arsenal normativo a fin de hacer frente a la creciente criminalidad informática, realidad que es una preocupación que trasciende las fronteras nacionales. A nivel internacional se ha intentado encontrar una respuesta común a la problemática, siendo los más representativos ejemplos de ello el Convenio sobre cibercriminalidad aprobado en Budapest el día 23 de noviembre de 2001 y, en el viejo continente, la Decisión marco 2005/222/JAI del Consejo de Europa, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

Precursora en la materia, vemos cómo para 1986 la legislación alemana comienza la lucha contra la delincuencia relacionada con la informática con la promulgación de la Segunda Ley contra la Criminalidad Económica, que introduce los tan comentados artículos, en su momento (modelo para muchas otras legislaciones), de espionaje de datos (parágrafo 202 a), estafa informática (parágrafo 263 a), alteración de datos (parágrafo 303 b) o sabotaje informático (parágrafo 303 b). Este modelo legislativo opta por modificar preceptos penales existentes para la tutela de bienes jurídicos tradicionales (o por la creación de otros que complementan los anteriores), dejando a un lado la discusión sobre el posible nacimiento de nuevos bienes jurídicos necesitados de protección penal.

Es el modelo seguido también en Italia con sus artículos, dispersos entre los delitos contra la libertad individual o contra el patrimonio, 600 *quater*, 615 *ter* a *quinquies*, 617 *quater* a *sixies*, 623 *bis*, 635 *bis* y *ter*, 635 *quater* y *quinquies*, 640 *ter* y 640 *quinquies*, varios de ellos introducidos en las importantes reformas de 2006 y 2008. Y en España. Aquí, las diferentes reformas que se han ido operando en esta materia, culminadas en lo que aquí interesa con la entrada en vigor de la Ley Orgánica 5/2010, de 23 de junio, han ido incorporando diversos preceptos de nuevo cuño, de entre los que pueden destacarse los artículos 183 *bis*, 197.3, 256, 264, 248.2 a), b) y c), 282 bis, 286, 392.2 o 400 bis, por ejemplo, para tutelar bienes jurídicos de naturalezas muy diversas, pero en relación a ataques que de alguna u otra manera tienen que ver con las tecnologías de la información y de la comunicación (TICs) o con la utilización de la informática, en su sentido más amplio.

Desde otra perspectiva diferente, Estados Unidos ha optado, dentro de lo que podría considerarse un segundo modelo, por una penalización promovida desde la regulación legal de concretos ámbitos de actuación, respondiendo a las realidades sociales y económicas de mayor impacto en su entorno, apuesta que no dista mucho de la de otros países, pero que se focaliza más en la protección de bienes jurídicos de corte patrimonial y en la protección de información federal y financiera. Surgen así, entre otras muchas, la primera Ley Federal de Protección contra el Abuso y Fraude Informático en 1984[1], que sufrirá subsecuentes e importantes modificaciones de entre las que destacan las de 1994 y 1996, que introduce la penalización de todo acceso ilícito a sistemas de información sea con fines

1 Computer Fraud and Abuse Act of 1984, U.S. Public Law 98-473. 18 U.S.C. 1030.

lucrativos o no, así como el uso de códigos maliciosos diseñados para alterar, dañar o destruir los datos en una computadora. Y, posteriormente, la Ley sobre la Privacidad de las Comunicaciones Electrónicas de 1986[2] o la Ley de Mejora de la Seguridad Cibernética de 2002[3], entre otras.

Frente a ambos sistemas, Francia, que si bien ya había ido modificando su Código Penal con las leyes 2004-575, 2004-801 y 2009-526, e incorporando diversos preceptos entre los atentados contra la personalidad (atentados contra los derechos de la persona derivados de ficheros o tratamiento informáticos), crea con la Ley 2012-410[4] un específico Capítulo III, dentro del Título II del Libro III del texto penal, dedicado a los atentados contra los sistemas de tratamiento automático de datos, en un tránsito que va de la tutela de los intereses estrictamente personales a la tutela de lo que en Francia se define como "otros bienes", incorporando así los sistemas informáticos de datos como un bien jurídico digno de protección. Ello, por supuesto, al margen de los denominados delitos de contenido, también presentes en su regulación. De algún modo lo que se va pretendiendo con ello es, al margen de la tradicional consideración del tratamiento de todos estos delitos como "*computer related crimes*" (delitos vinculados con la informática), la estructuración de una doble protección: por una parte, la reformulación de la tutela de clásicos intereses de corte individual frente al uso de las TICs (como, por ejemplo, la privacidad) y, por otra parte, la incorporación de tipo penales protectores de los sistemas informáticos y los datos, como nuevos bienes dignos de tutela.

Esta nueva regulación francesa, sobre la que ya se está empezando a debatir de modo intenso en Bruselas y en Luxemburgo, ha abierto el debate sobre si es posible estructurar o no un grupo de delitos, al modo de los delitos contra la intimidad, contra el honor, contra el patrimonio o contra determinadas instituciones estatales, vinculados a los ataques —informáticos— a sistemas de información y comunicación, independientemente del perjuicio a intereses particulares que los mismos puedan conllevar.

Vemos así un posible tercer modelo en el que fue pionera, en su momento, sin que se le prestara quizás la debida atención, la legislación de la República Dominicana, que, con los objetivos de procurar una protección integral de los sistemas de información y de regular los delitos cometidos contra éstos o contra sus componentes, junto a los delitos cometidos mediante las TICs en perjuicio de personas físicas o jurídicas, insiste en la necesidad de distinguir lo que estrictamente considera delitos de Alta Tecnología de los clásicos delitos de contenido (que son, de alguna manera, los únicos que se están tomando en consideración en legislaciones como la española).

Ello, para tutelar la integridad de los sistemas y sus componentes, la información y los datos, las transacciones y los acuerdos y la confidencialidad de éstos. Fue con esta idea cómo surgió la Ley 53/07, cuya breve consideración motiva estas líneas, para llamar la atención sobre el hecho de que el enfoque que se intuye en la legislación francesa y que posiblemente irán siguiendo otras normativas penales tiene un antecedente poco conocido que también puede servir de referente.

(II)

El legislador dominicano, con la Ley 53-07 contra Crímenes y Delitos de Alta Tecnología de 23 de abril de 2007, optó por incluir en una legislación especial independiente del Código Penal general todo lo relativo a los delitos informáticos, sin que esto implique una desvinculación absoluta de otras figuras clásicas ya existentes que pudieran asociarse al hecho informático.

Esta ley establece en sus Considerandos que las tecnologías de la información y de la comunicación se erigen como un soporte a la comisión de delitos tradicionales y crean "nuevas" modalidades de infracción y de hechos que deben ser sancionados penalmente. Introduce, por así decir, nuevas conductas anti-sociales a sancionar, así como la agravación de otras ya tradicionalmente reconocidas, por la magnificación del daño que implica la utilización de las tecnologías, como sucede por ejemplo con el caso de la difamación o la injuria, para las que la Ley 53-07 prevé penas agravadas[5]. Como expresamente

2 Electronic Communications Privacy Act of 1986. U.S. Public Law 99-508, 100 Stat. 1848, 18 U.S.C. 2510-2522.

3 Cyber Security Enhancement Act of 2002. Public Law 107-296. Included as section 225 of the Homeland Security Act of 2002.

4 Loi No. 2012-410 du 27 mars 2012 relative à la protection de l'identité.

5 Los artículos 21 y 22 de la Ley N.º 53-07 contra Crímenes y Delitos de Alta Tecnología establecen para estas conductas una pena de 3 meses a 1 año y de cinco a quinientos salarios mínimos, frente a las penas de la Ley 6132 de Expresión y Difusión del Pensamiento de 15 de diciembre de 1962, de 15 días a 6 meses de prisión y multa de RD$25 a RD$200 para la difamación (Art. 33) y de 5 días a 2 meses de prisión y multa de RD$6 a RD$50 para la injuria (Art. 35). Esto al margen de las penas previstas directamente por el Código Penal general, aún más leves (Art. 372 para la injuria y Art. 371 para la difamación).

señala la ley, las TICs han experimentado un desarrollo impresionante, que brinda "un nuevo soporte para la comisión de delitos tradicionales" y crea "nuevas modalidades de infracciones y hechos no incriminados".

La novedosa normativa dominicana tomó en cuenta la Resolución AG/RES 2004 (XXXIV-O/04) de la Organización de Estados Americanos sobre la adopción de una estrategia interamericana integral de seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética (aprobada en la cuarta sesión plenaria, celebrada el día 8 de junio de 2004), cuyo contenido no dista mucho de los parámetros establecidos en el Convenio europeo sobre la Ciberdelincuencia (Budapest, 23 de noviembre de 2001). En éste se conciben cuatro grupos de infracciones: contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; las que denomina netamente informáticas (estafa y falsedad); las relativas al contenido (limitadas prácticamente a lo que tiene que ver con pornografía infantil); y las vinculadas a los atentados a la propiedad intelectual y a los derechos afines. Convenio en cuya aprobación estuvo presente —y hay que subrayarlo—, como país no miembro del Consejo de Europa, República Dominicana (junto a Argentina, Australia, Canadá, Chile, Costa Rica, Japón, México, Filipinas, Senegal, República de Sudáfrica y Estados Unidos de América) y que actualmente está en vías de ratificación en este país.

Los objetivos que definen la aprobación de la Ley se vinculan en su Artículo 1 a la protección de los sistemas que utilicen tecnologías de información y comunicación y de su contenido, considerando que son bienes jurídicos protegidos en ella "la integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos".

Con tales objetivos, y con un Título I de carácter general, el legislador dominicano dedica el Título II de la Ley a cuestiones de Derecho penal sustantivo (Sección I) y de Derecho Procesal (Sección II). Y en lo que aquí interesa destacar, distingue claramente lo que son los crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información (por así decirlo, los delitos de más marcado carácter informático en los que este hecho es lo que realmente da carta de naturaleza a las conductas consideradas), que encuadra en el Capítulo I de dicha Sección I, y los delitos de contenido (contra bienes jurídicos tradicionales, pero cometidos a través de tecnología informática), a los que dedica el Capítulo II. Reserva otros tres capítulos para delitos contra la propiedad intelectual, delitos contra las telecomunicaciones y delitos de terrorismo y contra la nación.

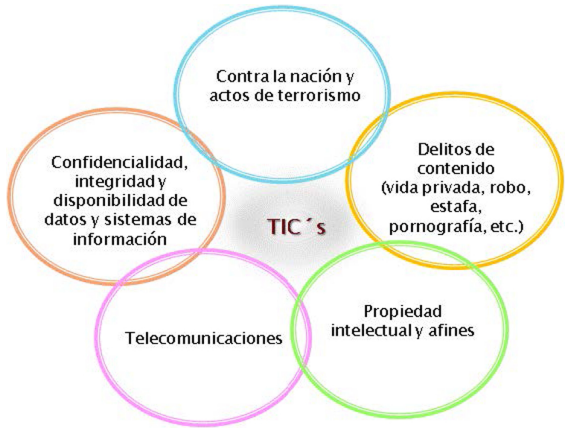

Imagen 1: Clasificación de los delitos de la Ley 53-07 de Delitos y Crímenes de Alta Tecnología, 23 abril 2007.

(III)

El Capítulo I de la Sección I del Título II de la Ley, como se acaba de indicar, se dedica a los delitos (crímenes y delitos) contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información.

Vemos así cómo el legislador dominicano ha claramente optado por incorporar al Derecho penal sustantivo nuevos bienes jurídicos que podrían considerarse intermedios, a fin de salvaguardar en última instancia el derecho a la vida privada y otros valores e intereses. Así, la confidencialidad, la integridad y la disponibilidad de los datos se transforman con esta regulación en valores a ser protegidos de modo expreso, configurándose una protección penal alrededor de nuevos conceptos, surgidos con el desarrollo de las TICs, al margen de que con ello, al mismo tiempo, se garanticen directa o indirectamente otros bienes jurídicos tradicionalmente reconocidos como merecedores de tutela penal.

Y no parece ser que estemos ante clásicos delitos de peligro condicionados a la existencia de un "riesgo" de vulneración de un bien jurídico individual clásico, sino ante verdaderos delitos de lesión frente a los nuevos bienes jurídicos protegidos por esta legislación.

Interesante es plantearse a este respecto que, incluyendo la Constitución de la República Dominicana de 2010 dentro de su Art. 44 la autodeterminación infor-

mativa sobre los datos relativos a una persona o sus bienes y las prácticas de transparencia informativa como elementos esenciales de ese derecho más amplio que es la intimidad, perfectamente se podría interpretar que esta Ley 53-07, aún siendo anterior la nueva Carta Magna dominicana, refuerza la protección de esos aspectos de la vida privada descritos en ésta. Sin embargo, no por ello tiene que entenderse que los mismos dejen de erigirse como bienes jurídicos intermedios, protectores también de otros intereses y valores a ser resguardados, ni que se haya condicionado o limitado la tutela a aquellos casos en los que estos "datos" o "sistemas" afecten la vida privada; lo que va a generar numerosas controversias, de entre las que cabe destacar, por ejemplo, la problemática concursal que puede plantearse cuando realmente se afecten también esos bienes jurídicos tradicionalmente tutelados penalmente.

Los delitos que sanciona la Ley en este Capítulo son los siguientes:

- La utilización de códigos de acceso (Art. 5).
- La clonación de dispositivos de acceso (Art. 5, párrafo).
- El acceso ilícito (Art. 6).
- El uso de datos por acceso ilícito (Art 6, párrafo I).
- La explotación ilegítima del acceso inintencional (Art. 6, párrafo II).
- El acceso ilícito para servicios a terceros (Art. 7).
- El beneficio de actividades de un tercero (Art. 7, párrafo).
- El uso de dispositivos fraudulentos (Art. 8).
- La interceptación e intervención de datos o señales (Art. 9).
- El daño o alteración de datos (Art. 10).
- El sabotaje (Art. 11).

El Capítulo II de dicha Sección I se dedica a los delitos de contenido, vinculados a la tutela de bienes jurídicos clásicos y nucleados en torno al hecho informático. Comprende:

- El atentado contra la vida de la persona (Art. 12).
- El robo mediante la utilización de alta tecnología (Art. 13).
- La obtención ilícita de fondos (Art. 14).
- Las transferencias electrónicas de fondos (Art. 14, párrafo).
- La estafa (Art. 15).
- El chantaje (Art. 16).
- El robo de identidad (Art. 17).
- La falsedad de documentos y firmas (Art. 18).
- El uso de equipos para la invasión de la privacidad (Art. 19).
- El comercio ilícito de bienes y servicios (Art. 20).
- La difamación (Art. 21).
- La injuria pública (Art. 22).
- El atentado sexual (Art. 23).
- La pornografía infantil (Art. 24).

Como puede verse, en este caso se trata de delitos tradicionales en los que la Ley se fija en el hecho de que pueden ser cometidos a través de lo que denomina Alta Tecnología, pero que en el fondo no dejan de ser delitos contra bienes individuales clásicos. De cualquier modo, la concepción de delitos relacionados con el contenido excede y difiere de la del Convenio de Cibercriminalidad, que sólo tipifica dentro de éstos la pornografía infantil.

A ambos capítulos, I y II, nos referiremos en estas páginas.

El Capítulo III lo compone un único Art. 25 dedicado a los delitos relacionados con la propiedad intelectual y afines, que remite a las Leyes 20-00 sobre propiedad industrial y 65-00 sobre derecho de autor.

El Capítulo IV, rubricado "Delitos contra las telecomunicaciones" tiene también un único Art. 26, que, integrado por siete modalidades delictivas, abarca:

- La llamada de retorno de tipo fraudulento (letra a).
- El fraude de proveedores de servicio de información (letra b).
- El redireccionamiento de llamadas de larga distancia (letra c).
- El robo de línea (letra d).
- El desvío de tráfico (letra e).
- La manipulación ilícita de equipos de telecomunicaciones (letra f).
- La intervención de centrales privadas (letra g).

Y, finalmente, el Capítulo V comprende los crímenes y delitos contra la nación (Art. 27) y los actos de terrorismo (Art. 28).

(IV)

Merece especial atención el Capítulo I sobre crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información, donde se persigue, como se ha dicho, tutelar nuevos bienes jurídicos intermedios, intentando al mismo tiempo incorporar una visión de neutralidad tecnológica en la redacción de las conductas punibles en aras a buscar que no se limite la tipificación de una infracción al uso de un determinado dispositivo o tecnología que quede en poco tiempo obsoleta.

El Art. 5 de la Ley 53-07, reproducido a pie de página[6], es ejemplificativo de lo que pretende el legislador en cuanto sanciona el mero hecho de manipular códigos o mecanismos de acceso a un sistema de datos o el falsificar cualquier tipo de dispositivo que tenga estos fines, sin que necesariamente se produzca el acceso ilícito al mismo, siendo suficiente que sea "posible". De esta forma, este primer artículo se diferencia de lo que se propone en el artículo 6, sirviendo para punir lo que no es sino una fase previa a la materialización del acceso ilícito.

Se coloca una primera barrera de protección frente a aquellos que se dedican a procurar y utilizar códigos de acceso, información o mecanismos similares y a falsificar dispositivos que permitan acceder ilícitamente a un sistema informático, permitiendo sancionar la mera intención de ingresar sin autorización en sistemas ajenos, al margen de la tipificación expresa de esta conductas y aunque normalmente el hecho de divulgar, generar, copiar, grabar, capturar, utilizar, alterar, traficar, desencriptar, decodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares o falsificar cualquier tipo de dispositivo para acceder al mismo, precederán al acceso ilícito en sí mismo.

Cabe destacar que el párrafo de este artículo introduce como agravante los supuestos de clonación[7]. El mismo se focaliza en el acceso a un servicio. Enfrenta el problema de la clonación vinculada a robos financieros, que se ha vuelto común con la utilización de dispositivos electrónicos (tarjetas de crédito y debito) para tener acceso al dinero, así como a la banca electrónica. El mayor problema que enfrentan estos delitos es la no denuncia de las entidades bancarias, por miedo a perder la confianza de sus clientes, que han preferido desarrollar complejos departamentos de detección de fraudes y estafas, en los que se da seguimiento al comportamiento de sus clientes en la utilización de los productos y servicios bancarios a fin de crear patrones y contrarrestar tales fraudes

De nuevo nos encontramos con un hecho más bien de carácter preparatorio, en el cual, sin embargo, se establecen penas agravadas muy considerables (de las más severas de esta ley). Esto responde a una realidad social, buscando establecerse sanciones persuasivas ante una clonación de tarjetas que se ha convertido en forma habitual de fraude en relación con el que se han detectado bandas organizadas dedicadas precisamente a esta clonación de tarjetas para la venta, frente a las que no se podía actuar antes de la existencia de esta legislación.

El Art. 6[8] de la Ley 53-07 penaliza el acceso ilícito. Resulta curioso que la sanción frente a un real y efectivo acceso ilícito reciba una penalización inferior a la manipulación de códigos o mecanismos o a la falsificación de dispositivos que permitan ese acceso. Las sanciones contempladas en el Art. 5 son sustancialmente más considerables que las del Art. 6 en lo que se refiere a la pena privativa de libertad, pudiendo llegar, como se ha señalado, hasta 3 años de prisión frente al año previsto para el acceso ilícito. Es cierto, no obstante, que la cuantificación máxima de la multa sí es superior en el caso del Art. 6.

En la sanción del acceso ilícito a un sistema se especifica que es irrelevante le hecho de que se utilice o no una identidad ajena o el que se cuente con autorización para ello (siempre que se exceda ésta): es decir, se sanciona prácticamente cualquier medio de acceso imaginable. Encontramos en este artículo un reflejo de esa búsqueda de neutralidad tecnológica, en la que se persigue sancionar el hecho cometido sin importar el medio de comisión.

El precepto podría abarcar el acceso indebido a los ordenadores personales y a las cuentas de usuarios, páginas y perfiles restringidos de los internautas y la posible explotación de los datos personales así obtenidos.

6 Artículo 5. Ley No. 53-07 contra Crímenes y Delitos de Alta Tecnología de 23 de abril de 2007. "*Códigos de Acceso. El hecho de divulgar, generar, copiar, grabar, capturar, utilizar, alterar, traficar, desencriptar, decodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares, a través de los cuales se logra acceso ilícito a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, o falsificar cualquier tipo de dispositivo de acceso al mismo, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo.*"

7 Artículo 5. Párrafo. Ley No. 53-07 contra Crímenes y Delitos de Alta Tecnología de 23 de abril de 2007. "*Clonación de Dispositivos de Acceso. La clonación, para la venta, distribución o cualquier otra utilización de un dispositivo de acceso a un servicio o sistema informático, electrónico o de telecomunicaciones, mediante el copiado o transferencia, de un dispositivo a otro similar, de los códigos de identificación, serie electrónica u otro elemento de identificación y/o acceso al servicio, que permita la operación paralela de un servicio legítimamente contratado o la realización de transacciones financieras fraudulentas en detrimento del usuario autorizado del servicio, se castigará con la pena de uno a diez años de prisión y multa de dos a quinientas veces el salario mínimo.*"

8 Artículo 6. Ley No. 53-07 contra Crímenes y Delitos de Alta Tecnología de 23 de abril de 2007. "*Acceso Ilícito. El hecho de acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de tres meses a un año de prisión y multa desde una vez a doscientas veces el salario mínimo.(…)*"

Asimismo, podría llegar a abarcar la captura de datos disponibles en distintos puntos de la red.

Este artículo resulta especialmente interesante por destacarse de modo claro en él que es indiferente si se ha lesionado o no un bien jurídico particular concreto; por eso permite sancionar a los llamados "hackers blancos"; lo importante es el acceso en sí no la lesión de un bien de naturaleza individual o colectivo derivada del mismo. Con independencia de que, al mismo tiempo, se salvaguarde la vida privada.

El Art. 6 de la Ley 53-07, en su Párrafo I[9], sanciona lo que denomina "uso de datos por acceso ilícito" y aquí ya incluye textualmente la noción de datos "confidenciales".

Al margen de la previsión de las conductas de supresión o modificación, referidas a cualesquiera datos, la limitación de la punición de la conducta de difusión sólo respecto a datos que sean confidenciales, abre la ambigüedad y obliga a plantearse lo que ha de entenderse por "confidencial".

¿Presupondrá esto la necesidad de establecer medidas de seguridad previas? ¿Se debe entender que se habla de un acceso ilícito necesariamente cuando se violentan medias de seguridad preestablecidas? ¿O la simple declaración del titular de los mismos basta para dar a los datos esta categoría? En todo caso estamos frente a un acceso no autorizado a un espacio privado de una persona (aunque virtual), donde nadie más que él, y quien él autorice, tiene derecho a estar y a conocer su contenido, independientemente de las medidas colocadas para proteger el mismo. Lo que ello sí implica, de una forma u otra, es la existencia de una configuración que permita nivelar o gestionar los niveles de posible acceso, pero el texto del artículo, en sí, en ninguna parte presupone la necesidad de que se violenten medidas de seguridad.

El Art. 6 de la Ley 53-07 en su Párrafo II[10] sanciona la explotación ilegítima de un acceso "coincidencial" a un sistema informático, electrónico, telemático o de telecomunicaciones.

Esta formulación resulta particularmente interesante, ya que se sale de la conceptualización de "acceso ilícito" como tal, previendo la posibilidad de un acceso casual. Este hecho podría entenderse que en sí no sería sancionable; pero que sí lo es la explotación o mal uso del acceso así conseguido.

Sin embargo, el artículo 6 penaliza todo acceso ilícito y el artículo 6 párrafo I el uso de los datos obtenidos por acceso ilícito. Cabe preguntarse si hay algo que diferencie el acceso ilícito del "no intencionado", no estando autorizados ni uno ni otro. En otros términos, si el párrafo II es redundante en relación con lo que expresa el párrafo I (máxime cuando las penas coinciden) o si lo único que se quiere explicar es que sancionándose en ambos casos el uso, el acceso sólo se sanciona cuando no es coincidencial. Podría concluirse, para explicar esto, que el acceso ilícito implica la violación de particulares barreras o medidas de seguridad, mientras que el ilícito coincidencial no. Pero, como antes se decía, no es esto algo expresamente estipulado en la ley, que define como acceso ilícito "*el hecho de ingresar o la intención de ingresar sin autorización, o a través del acceso de un tercero, a un sistema de información, permaneciendo o no en él*"[11]. Con lo que la interpretación de si el acceso ilícito coincidencial se sanciona en el artículo 6 es más compleja. La redacción de los preceptos no es acertada y deja abierta muchas lagunas.

También las referentes al alcance que a futuro los jueces puedan dar al concepto de "explotación ilegitima" del acceso logrado. Se deja al juez ponderar en qué consistirá esta explotación. ¿Podría sancionarse aquí la recolección y tratamiento de datos sin conocimiento de los interesados a fin de formar perfiles de usuarios con fines comerciales o incluso de vigilancia y seguridad? ¿Podrían considerarse aquí el tratamiento de datos de conexión y aquéllos que se ven duplicados a lo largo de la transmisión o "ruteo" de la información a través de diversos servidores?

El Art. 7[12] de la Ley 53-07 sanciona el acceso ilícito a sistemas para ofrecer servicios a terceros para salva-

9 Art. 6. Párrafo I. Ley No. 53-07 contra Crímenes y Delitos de Alta Tecnología de 23 de abril de 2007. "(…) *Uso de Datos por Acceso Ilícito. Cuando de dicho acceso ilícito resulte la supresión o la modificación de datos contenidos en el sistema, o indebidamente se revelen o difundan* ***datos confidenciales*** *contenidos en el sistema accesado, las penas se elevarán desde un año a tres años de prisión y multa desde dos hasta cuatrocientas veces el salario mínimo. (…)"* La negrita es nuestra.

10 Art. 6. Párrafo II. Ley No. 53-07 contra Crímenes y Delitos de Alta Tecnología de 23 de abril de 2007. *"(…) Explotación Ilegítima de Acceso Inintencional. El hecho de explotar ilegítimamente el acceso logrado* ***coincidencialmente*** *a un sistema electrónico, informático, telemático o de telecomunicaciones, se sancionará con la pena de un año a tres años de prisión y multa desde dos a cuatrocientas veces el salario mínimo."* La negrita es nuestra.

11 Art. 4 de la Ley No. 53-07 contra Crímenes y Delitos de Alta Tecnología.

12 Art. 7. Ley No. 53-07 contra Crímenes y Delitos de Alta Tecnología de 23 de abril de 2007. *"Acceso ilícito para Servicios a Terceros. El hecho de utilizar un programa, equipo, material o dispositivo para obtener acceso a un sistema electrónico, informático, telemático o de*

guardar a los que ofrecen legítimamente estos servicios de una competencia desleal e ilegal que va en detrimento del desarrollo de los mismos, de un modo amplio que abarca no sólo al autor del acceso sino también a su beneficiario, en un intento por cubrir ambos lados de la cadena del mercado.

El Art. 8[13] de la Ley 53-07 sanciona conductas vinculadas a la tenencia de dispositivos cuyo único uso o uso fundamental sea el de emplearse como herramienta para cometer crímenes y delitos de alta tecnología. Típica sanción de un acto preparatorio, herramienta interesante para prevenir la distribución de programas y equipos utilizados con fines fraudulentos, será sin embargo difícil probar el hecho de que su único uso o uso fundamental sea éste. La mayoría de las tecnologías en sí mismas no son de naturaleza "fraudulenta", sino neutrales.

El Art. 9[14] de la Ley 53-07, que penaliza la interceptación de datos está directamente vinculado a la protección del secreto, la intimidad y la privacidad, a la inviolabilidad de las comunicaciones electrónicas extendiendo la clásica protección del secreto de los documentos a la de los "sistemas" y "datos". Tanto de las personas físicas como de las personas jurídicas, pareciéndose hacer eco el legislador dominicano de la decisión de la Corte Europea de Derechos Humanos de 16 de abril de 2002 contra Francia, en la cual se consideró que las personas morales tienen derecho a la protección de su sede social bajo el fundamento de la tutela de la vida privada[15].

Por su parte, el Art. 10 de la ley 53-07[16] penaliza el daño o alteración de datos con fines fraudulentos, con la previsión de agravación para hechos cometidos por personas que prestan servicios a la afectada. Artículo vinculado con el posterior Art. 11, pero más focalizado en la sanción de hechos que persiguen llevar al error del sistema, no su completa inutilización o destrucción. No por ello, en todo caso, deja de atentarse contra la integridad de los sistemas y contra la llamada seguridad informática.

Y, finalmente, el Art. 11 la Ley 53-07[17] el denominado sabotaje, con independencia de la finalidad a que el mismo obedezca y del sistema que se ataque. Sin embargo, no es lo mismo alterar un sistema de seguridad nacional o de salud o un sistema bancario que el sistema de una pizzería o de un servicio de entrega a

---

telecomunicaciones, o a cualquiera de sus componentes, para ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, se sancionará con la pena de tres meses a un año de prisión y multa desde tres a quinientas veces el salario mínimo.

Párrafo. Beneficio de actividades de un Tercero. El hecho de aprovechar las actividades fraudulentas de un tercero descritas en este artículo, para recibir ilícitamente beneficio pecuniario o de cualquier índole, ya sea propio o para terceros, o para gozar de los servicios ofrecidos a través de cualquiera de estos sistemas, se sancionará con la pena de tres a seis meses de prisión y multa desde dos a doscientas veces el salario mínimo."

13 Art. 8. Ley No. 53-07 contra Crímenes y Delitos de Alta Tecnología de 23 de abril de 2007. "*Dispositivos Fraudulentos. El hecho de producir usar, poseer, traficar o distribuir, sin autoridad o causa legítima, programas informáticos, equipos, materiales o dispositivos cuyo único uso o uso fundamental sea el de emplearse como herramienta para cometer crímenes y delitos de alta tecnología, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo*."

14 Artículo 9. Ley No. 53-07 contra Crímenes y Delitos de Alta Tecnología de 23 de abril de 2007. "*Interceptación e Intervención de Datos o Señales. El hecho de interceptar, intervenir, injerir, detener, espiar, escuchar, desviar, grabar u observar, en cualquier forma, un dato, una señal o una transmisión de datos o señales, perteneciente a otra persona por propia cuenta o por encargo de otro, sin autorización previa de un juez competente, desde, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones, o de las emisiones originadas por éstos, materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas físicas o morales, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo, sin perjuicio de las sanciones administrativas que puedan resultar de leyes y reglamentos especiales*."

15 CEDH. *Deuxième Section. Affaire Société Colas est et autres c. France. (Requête No. 37971/97). Arrêt Strasbourg 16 avril 2002. Définitif 16/07/2002.* Recuérdese a este respecto la importante influencia francesa de la normativa dominicana.

16 Artículo 10. Ley No. 53-07 contra Crímenes y Delitos de Alta Tecnología de 23 de abril de 2007. "*Daño o Alteración de Datos. El hecho de borrar, afectar, introducir, copiar, mutilar, editar, alterar o eliminar datos y componentes presentes en sistemas electrónicos, informáticos, telemáticos, o de telecomunicaciones, o transmitidos a través de uno de éstos, con fines fraudulentos, se sancionará con penas de tres meses a un año de prisión y multa desde tres hasta quinientas veces el salario mínimo.*

Párrafo. Cuando este hecho sea realizado por un empleado, exempleado o una persona que preste servicios directa o indirectamente a la persona física o jurídica afectada, las penas se elevarán desde uno a tres años de prisión y multa desde seis hasta quinientas veces el salario mínimo."

17 Artículo 11. Ley No. 53-07 contra Crímenes y Delitos de Alta Tecnología de 23 de abril de 2007. "Sabotaje. El hecho de alterar, maltratar, trabar, inutilizar, causar mal funcionamiento, dañar o destruir un sistema electrónico, informático, telemático o de telecomunicaciones, o de los programas y operaciones lógicas que lo rigen, se sancionará con las penas de tres meses a dos años de prisión y multa desde tres hasta quinientas veces el salario mínimo."

domicilio. Intereses muy diversos están involucrados en cada uno de ellos.

(V)

En el Capítulo II de la sección de Derecho sustantivo es donde la Ley 53-07 hace referencia a los denominados "delitos de contenido". Ésta es también una variante interesante de la legislación dominicana frente a otras, al preverse específicamente un apartado para la sanción de aquellas conductas realizadas a través de la informática pero que atentan contra bienes jurídicos tradicionales. Esto, independientemente de que algunos de ellos se vean protegidos también indirectamente por otro articulado. Parecería que el legislador busca diferenciar los que pueden considerarse delitos informáticos de los delitos cometidos a través de la informática.

Entre éstos, el primero de ellos es el atentado contra la vida de las personas del Art. 12, que contempla las mismas sanciones que en el caso de homicidio intencional o inintencional cuando se atenta contra la vida o se provoque la muerte de una persona utilizando sistemas de carácter electrónico, informático, telemático o de telecomunicaciones o sus componentes. En principio, este artículo parecería redundante, pues el Código Penal Dominicano (Art. 295 y siguientes) al definir el homicidio (y sus diferentes vertientes) no limita los medios para atentar contra la vida de una persona; sin embargo, el legislador quiso recalcar la protección de la misma también en esta ley especial 53-07.

El Art. 13 de la Ley 53-07 comienza a introducir los crímenes y delitos contra la propiedad. Este artículo sanciona el robo cometido utilizando sistemas o dispositivos electrónicos, informáticos, telemáticos o de telecomunicaciones, para inhabilitar o inhibir los mecanismos de alarma o guarda, u otros semejantes; o cuando para tener acceso a casas, locales o muebles, se utilizan los mismos medios o medios distintos de los destinados por su propietario para tales fines; o por el uso de tarjetas, magnéticas o perforadas, o de mandos, o instrumentos para apertura a distancia o cualquier otro mecanismo o herramienta que utilice alta tecnología. Establece una pena de dos (2) a cinco (5) años de prisión y multa de veinte (20) quinientas (500) veces el salario mínimo.

Como vemos, este artículo se focaliza en la utilización de medios tecnológicos para violentar sistemas de seguridad que permitan acceder a lugares donde se cometerá el robo, es decir para obtener el acceso ilícito a un espacio físico donde se cometerá el hecho sancionable. Resulta curioso que las penas sean inferiores a las normalmente impuestas por el robo agravado (aquél cometido de noche, en una casa habitada o centro religioso, con fractura, llaves falsas, escalamiento, con violencia o uso armas), que llegan hasta los 20 años de prisión, aunque se establecen multas considerables inexistentes en el Código Penal (Art. 379 y siguientes).

Por otra parte, habrá que dilucidar qué precepto será de aplicación en casos de concurrencia de elementos comunes. Así, ¿podía considerarse la violación a la seguridad y el acceso ilícito al lugar utilizando dispositivos de "alta tecnología" como una fractura o uso de llaves falsas ya estipulada en la legislación penal y, consiguientemente, aceptarse como uno de los elementos que podría agravar la pena o, por el contrario, siempre que el elemento de alta tecnología concurra se descartará la normativa penal general? Queda por ver cómo interpreta estas cuestiones la jurisprudencia dominicana.

El Art. 14 de la Ley 53-07 sanciona la obtención ilícita de fondos, créditos o valores a través del constreñimiento del usuario legítimo de un servicio financiero informático, electrónico, telemático o de telecomunicaciones, con la pena de tres (3) a diez (10) años de prisión y multa de cien (100) a quinientas (500) veces el salario mínimo.

Resulta curioso que para que se sancione la conducta sea necesaria la coerción del usuario, es decir, la interacción con el sujeto pasivo como parte del elemento material del delito. Así, este precepto suscita la problemática del tratamiento de los robos realizados en el mismo entorno informático frente al desarrollo de la banca electrónica y el manejo de los fondos a través de sistemas informáticos, sin que necesariamente haya contacto alguno con el sujeto pasivo; caso de apropiación de bienes que no pertenecen al sujeto activo pero sin necesidad de irrumpir en un espacio físico ajeno o constreñimiento personal alguno, sino a través del mismo sistema.

El párrafo del Art. 14 es el que viene a lidiar con esta realidad, sancionado la transferencia electrónica de fondos a través de la utilización ilícita de códigos de acceso o de cualquier otro mecanismo similar con pena de uno (1) a cinco (5) años de prisión y multa de dos (2) a doscientas (200) veces el salario mínimo.

El Art. 15 de la Ley, por su parte, sanciona la estafa realizada por medios electrónicos, informáticos, telemáticos o de telecomunicaciones sancionándola con pena de tres (3) meses a siete (7) años de prisión y multa de diez (10) a quinientas (500) veces el salario mínimo. Se establece así una pena agravada frente a

la clásica estafa del Código Penal, cuya pena máxima llega a los dos años de prisión correccional y 200 pesos de multa (Art. 405 y siguientes).

El Art. 16 sanciona el chantaje realizado a través del uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de sus componentes, y/o con el propósito de obtener fondos, valores, la firma, entrega de algún documento, sean digitales o no, o de un código de acceso o algún otro componente de los sistemas de información, con la pena de uno (1) a cinco (5) años de prisión y multa de diez (10) a doscientas (200) veces el salario mínimo. La formulación del mismo presenta una particularidad digna de resaltar cual es la de que el simple hecho de utilizar los sistemas de alta tecnología para este fin de chantaje, independientemente del propósito del mismo, ya integra la infracción.

El Art. 17 de la Ley 53-07 deja atrás los delitos contra la propiedad y se centra en la tutela de la identidad de las personas. Penaliza la suplantación a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, con penas de tres (3) meses a siete (7) años de prisión y multa de dos (2) a doscientas (200) veces el salario mínimo. Precepto interesante en la medida en que para "robar" la identidad se hace necesaria la manipulación de datos privados del individuo[18]. Cabe destacar que esta "identidad" no se limita a la de personas físicas, sino que puede también englobarse en ella la de las personas jurídicas y servir como base para la sanción de conductas reprensibles como el *phishing* o el *spoofing*, que son de lo más comunes en República Dominicana.

El Art. 18 de la Ley, por su parte, busca sancionar a todo aquel que falsifique, desencripte, decodifique o de cualquier modo descifre, divulgue o trafique, con documentos, firmas, certificados, sean digitales o electrónicos, estableciendo una pena de uno (1) a tres (3) años de prisión y multa de cincuenta (50) a doscientas (200) veces el salario mínimo. Penas que resultan inferiores a las tradicionalmente establecidas por el Código penal general, que llegan hasta los 10 años de prisión, aunque aquí no se contemplan multas.

Vamos viendo con ello como, en algunas sanciones, si bien se reducen considerablemente las penas privativas de libertad, se aumenta considerablemente la cuantía de las multas, al entenderse que puede jugar un rol persuasivo importante el impacto pecuniario en esta nueva generación de criminales, que pertenecen generalmente a estratos sociales de clase media.

El Art. 19 introduce una disposición particularmente interesante al sancionar el uso de equipos para la invasión de la privacidad. Establece el precepto que el uso, sin causa legítima o autorización de la entidad legalmente competente, de sistemas electrónicos, informáticos, telemáticos, de telecomunicaciones o dispositivos que puedan servir para realizar operaciones que atenten contra la privacidad en cualquiera de sus formas, se sancionará con la pena de seis (6) meses a dos (2) años de prisión y multa de cinco (5) a quinientas (500) veces el salario mínimo.

Decimos que es interesante porque se crea una especie de artículo general, el cual puede servir para penalizar cualquier uso de las nuevas tecnologías que vulnere el derecho a la privacidad. El concepto de neutralidad tecnológica queda en este artículo, con ello, elevado a su máxima expresión, al preverse un tipo "abierto" que permite sancionar "cualquier" atentado contra la vida privada cometido a través de la denominada "alta tecnología".

El precepto podría servir de fundamento, así, para sancionar la recolección y tratamiento masivo no autorizado de información a través de sistemas electrónicos, informáticos, telemáticos, de telecomunicaciones, o dispositivos, como por ejemplo en los proceso de *data mining* o la apropiación de informaciones residuales (*scavenging*) y su tratamiento, así como cualquier otro tratamiento ilegitimo de datos. Esto así por la definición establecida en el Art. 44 de la Constitución Dominicana, en la que se da carácter constitucional las *Fair Informational Practices*, como parte de los elementos esenciales del derecho a la vida privada.

Sin embargo, acaba surgiendo la duda de si la configuración de un tipo penal tan abierto, en que cabe "todo" y "nada", puede conllevar que el mismo se vuelva inaplicable: ¿acaso todas las vulneraciones a la vida privada por la vía de las TICs son sancionables penalmente?

18 Resulta particular el enfoque dado por el Juzgado de Primera Instancia del Distrito Nacional Primer Tribunal Colegiado de la Cámara Penal, en su Sentencia de 29 de abril de 2010, n.º 148-2010, en cuando no considera un robo de identidad el hecho de que un individuo a fin de activar líneas telefónicas utilizara el nombre de diversas personas, sin su autorización, poseyendo las distintas cédulas de identidad para obtener la activación de las tarjetas SIM. Es decir haciéndose pasar por ellas. El Tribunal justifica esto en que "*no ha sido probado que (…) se haya valido de una identidad ajena a la suya para cometer el ilícito*", considerando que sí había, en cambio, una violación de los Arts. 7, 20 y 26 de la Ley N.º 53-07 contra Crímenes y Delitos de Alta Tecnología, de 23 abril de 2007.

El Art. 20 de la Ley 53-07 sanciona la comercialización no autorizada o ilícita de bienes y servicios, a través de Internet o de cualquiera de los componentes de un sistema de información, con la pena de tres (3) meses a cinco (5) años de prisión y multa de cinco (5) a quinientas (500) veces el salario mínimo. Asimismo, en su párrafo hace referencia al tráfico de humanos, inmigrantes, a los delitos de trata de personas y a la venta de drogas o sustancias controladas, remitiendo su sanción a las legislaciones especiales de esas materias independientemente del componente tecnológico que vehicule su comisión.

El precepto puede llegar a plantear interesantes discusiones en el ámbito de aplicación de la ley, en un espacio virtual que no conoce las fronteras nacionales y en el que una persona puede estar ofreciendo servicios o productos prohibidos en el territorio dominicano pero no en su propio país de origen.

Los Arts. 21 y 22 introducen penas agravadas para la difamación y la injuria cometidas a través de medios electrónicos, informáticos, telemáticos, de telecomunicaciones o audiovisuales. Y establece sanciones de tres (3) meses a un año (1) de prisión y multa de cinco (5) a quinientas (500) veces el salario mínimo. Esto se justifica en el hecho de la facilidad de difusión incluso fuera de las fronteras nacionales y la masificación de estos medios.

Los últimos artículos del Capítulo se dedican, finalmente, la protección de los menores y/o personas particularmente vulnerables.

Así, el Art. 23 de la Ley 53-07 sanciona el atentando sexual contra un niño, niña, adolescente, incapacitado o enajenado mental, mediante la utilización de un sistema de información o cualquiera de sus componentes, con las penas de tres (3) a diez (10) años de prisión y multa desde cinco (5) a doscientas (200) veces el salario mínimo, penas equiparables a las establecidas en el Código Penal.

El Art. 24 sanciona la pornografía infantil, penalizando no sólo su producción, difusión, venta y cualquier tipo de comercialización (se sancionará con penas de dos a cuatro años de prisión y multa de diez a quinientas veces el salario mínimo), sino también su adquisición y posesión aun inintencional (tres meses a un año de prisión y multa de dos a doscientas veces el salario mínimo), disposición esta última un tanto desproporcionada, pues implicaría que, aun sin consentimiento, la recepción de un *spam* con pornografía infantil permitiría la sanción del receptor, en posesión de la información no permitida.

Cabe preguntar aquí qué medidas podían tomar las empresas frente a un potencial mal uso de los recursos tecnológicos puestos a disposición de los empelados y si podría hablarse de una responsabilidad compartida en esos casos. O cómo tratar los puntos de acceso público a Internet, responsables de los contenidos a los que se permite[19].

(VI)

Es interesante ponderar la evolución de la aplicación de la Ley 53-07 y su paulatina conocimiento y/o aceptación por parte de la población. Así, de un total de 60 querellas presentadas en el año 2007 en relación con su contenido se ha pasado a 224 en el año 2008, a 986 en el año 2009 y a 684 en 2010[20], destacándose el *phising*, el *hacking*, el robo de *emails* y el robo de identidad, así como las llamadas molestas o amenazantes y la interceptación telefónica como principales conductas denunciadas.

Para su aplicación, la Ley 53-07 creó una Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT) y un Departamento Investigación de Crímenes de Alta Tecnología (DICAT)[21], como órgano especializado de investigación.

Lamentablemente, aún los tribunales penales dominicanos, cuando conocen de casos relativos a la violación de la Ley No. 53-07, se focalizan más en el perjuicio económico que en otro tipo de consideración, obviando en muchos casos la posible vulneración que se produce, por ejemplo, de la vida privada, lo que responde también a que muchas veces el atentado a la misma es ignorado por el propio Ministerio Público o, incluso, por el mismo sujeto perjudicado[22].

19 Ver Art. 16 República Dominicana. Instituto Dominicano de las Telecomunicaciones (INDOTEL). Resolución No. 086-11, que aprueba el reglamento para la obtención y preservación de datos e informaciones por parte de los proveedores de servicios en la aplicación de las disposiciones de la ley 53-07, sobre crímenes y delitos de alta tecnología, 19 de diciembre de 2000.

20 Ver estadísticas de la Policía Nacional, Dirección Central de Investigaciones Criminales. Departamento de Investigación de Crímenes y Delitos de Alta Tecnología. Santo Domingo, 2007-2010.

21 Ver http://www.policianacional.gob.do/v2/dicrim/departamentos/20110224-dicat.ashx.

22 Véanse, Juzgado de Primera Instancia del Distrito Nacional. (República Dominicana). Primer Tribunal Colegiado de la Cámara Penal, Sentencia de 29 abril 2010, No. 148-2010 (activación de planes en telefónica a nombre de otras personas, desviación del servicio y

(VII)

Cabe destacar, finalmente, que la Ley pretende completarse con la existencia de un anteproyecto de ley que busca regular el envío de correo electrónicos comerciales o "*spam"* no solicitados, de noviembre de 2010[23].

En él se da preferencia al "*opt in*" frente al "*opt out*", estableciéndose que debe mediar antes de cualquier comunicación comercial un consentimiento expreso de la persona a la que va dirigida. La excepción a la regla surge en el caso en que esta comunicación provenga de remitentes con los que se tenga una relación contractual previa, siempre que guarde relación con los servicios inicialmente contratados. Se excluyen también los correos provenientes de entidades públicas.

El anteproyecto establece también prohibiciones interesantes como son la de vender los correos electrónicos, así como su recolección de forma fraudulenta y maliciosa en lugares públicos y la creación, venta, préstamo, intercambio o cualquier otro tipo de transferencia de listas de correos electrónicos para el envío comercial que haya sido creada ilegalmente o sin el consentimiento del receptor o emisor del correo.

Como vemos quedaría penalizada la posibilidad de obtener información extrayéndola de la red sin el consentimiento de las partes, aun cuando estén en lugares de acceso "público".

Esto reforzaría la protección de los datos frente a la posibilidad de obtenerlos "escarbando" en la red o adquiriéndolos sin el consentimiento de la persona concernida.

(VIII)

En definitiva, se presenta en la legislación penal dominicana un modelo, en el cual convive la protección de bienes jurídicos clásicos con la de bienes jurídicos de nuevo cuño, que responde a la necesidad de sancionar las nuevas conductas reprochables que traen consigo las llamadas "altas tecnologías", buscándose así tutelar no solamente los intereses individuales las personas, sino un nuevo estilo de interacción social en el cual los sistemas de información y electrónicos se han transformado en una parte esencial de la vida de las personas. La cuestión seguirá siendo, sin embargo, la de qué queremos realmente tutelar, a fin de no perdernos en los medios sin llegar al fin, teniendo siempre presente que lo que al fin y al cabo importa es la protección de las personas, de sus derechos y de sus libertades.

venta de minutos); Juzgado de Primera Instancia del Distrito Nacional. (República Dominicana). Cuarto Tribunal Colegiado de la Cámara Penal, Sentencia de 21 abril 2010, No. 67-2010 (caso de fraude al sistema informático de una telefónica, se violentaron cabinas y líneas de clientes); Juzgado de Primera Instancia del Distrito Nacional. (República Dominicana). Cuarto Tribunal Colegiado de la Cámara Penal, Sentencia de 28 abril 2011, No. 79-2011 (falsificación de tarjetas de crédito de otras personas); Juzgado de Primera Instancia del Distrito Nacional. (República Dominicana). Cuarto Tribunal Colegiado de la Cámara Penal, Sentencia de 21 julio 2011, No. 143-2011 (caso de *phishing*); Juzgado de Primera Instancia del Distrito Nacional. (República Dominicana). Cuarto Tribunal Colegiado de la Cámara Penal, Sentencia de 26 mayo 2011, No. 115-2011 (se produjo la clonación de tarjetas de crédito y la posesión de un documento de identidad ajeno); Juzgado de Primera Instancia del Distrito Nacional. (República Dominicana). Cuarto Tribunal Colegiado de la Cámara Penal, Sentencia de 17 marzo 2011, No. 44-2011 (en el caso se encontró instalado un programa que puede ser usado para alterar documentos, existiendo diversos archivos digitales de cédulas de identidad y facturas de la Dirección General de Impuesto Internos); Juzgado de Primera Instancia del Distrito Nacional. (República Dominicana). Cuarto Tribunal Colegiado de la Cámara Penal, Sentencia de 26 abril 2011, No. 73-2010 (caso de *phishing*).

23 El mismo fue aprobado en segunda lectura por la Cámara de Diputados en septiembre de 2011 y se encuentra, en la fecha en que se escriben estas líneas, en la Cámara de Senadores.