Los delitos informáticos en el Derecho penal de México y España*

Graciela M. Landa Durán**

I. Introducción

En la actualidad, países como México y España se han incorporado a las ventajas que reporta la "era de la informática", pero también a sus riesgos y, consecuentemente, a la comisión de delitos en esta materia.

---

* El presente artículo es una síntesis del trabajo de investigación elaborado por la magistrada Graciela M. Landa Durán, durante el curso de posgrado "Derecho Penal Económico: Cuestiones de Parte General y Especial", cursado en la Universidad de Castilla-La Mancha, Toledo, España, en abril de 2007. La síntesis fue realizada por el doctor Carlos Barrientos Sánchez, secretario técnico en el Instituto de la Judicatura Federal.

** Magistrada del Segundo Tribunal Colegiado del Décimo Quinto Circuito.

La dinámica que ello propicia ha motivado la elaboración del presente trabajo.

Si bien es cierto que no existe ningún campo del actuar humano en el que la seguridad esté garantizada plenamente, la lucha frente a la criminalidad informática desborda los límites del Derecho penal, pues se trata de un fenómeno cuyo control reclama instrumentos más amplios y complejos, no sólo de naturaleza jurídica, sino de carácter técnico, formativo y cultural, por mencionar algunos.

En consecuencia, se impone analizar las implicaciones penales de las nuevas tecnologías informáticas, ya que, de forma paralela al avance tecnológico, van surgiendo nuevas formas de conducta antisocial que, irónicamente, han hecho de los equipos y sistemas informáticos, considerados como sello distintivo del desarrollo humano, instrumentos para delinquir.

II. Conceptualización y caracterización

La revolución informática ha incidido de forma insospechada en el concepto tradicional de "información", revitalizándolo e incrementando su valor.

Tal como lo apuntaba Luis Arroyo Zapatero en su obra *Estudios de Derecho penal económico*, este fenómeno tiene lugar en toda sociedad donde ha irrumpido de forma espectacular la informática; sin embargo, un sector particularmente impactado por las nuevas tecnologías es el empresarial.

Pues bien, las peculiares características de los sistemas informáticos y de su funcionamiento, la todavía notable desprotección material y logística de las bases de datos informatizadas y la importancia que para el tráfico económico empresarial poseen los programas y la información almacenada en soportes informáticos hacen de ésta una materia especialmente vulnerable ante conductas ilícitas de diversa índole.

En este sentido, como interés social valioso, digno de la tutela penal, nos acercaremos a las vías instauradas por el Derecho punitivo, tanto español como mexicano, para su protección, frente a los comportamientos ilícitos que más gravemente pueden atacarlo, conductas susceptibles de encuadrar en alguna de estas tres grandes categorías:

- El espionaje informático industrial o comercial.
- Las conductas de daños o sabotaje informático.
- Las conductas de mero intrusismo, también conocidas con el término anglosajón "*hacking*".

III. Definición de delito informático

La vertiginosa carrera tecnológica de la naciente sociedad de la información genera, inevitablemente, relaciones jurídicas y problemas novedosos para el campo del derecho, frente a los cuales algunos tratadistas no ocultan su contrariedad, al obligarles, como lo afirma Pérez Luño (cit. Palomino, 2006), a realizar un esfuerzo para superar la tendencia congénita de escanciar el vino nuevo de las cuestiones que emergen del cambio social y tecnológico, en los viejos odres conceptuales y metodológicos de la dogmática jurídica tradicional.

En el campo del Derecho penal informático, entendido como postrero instrumento de protección ante la lesión o puesta en peligro de esos nuevos valores, bienes y derechos que surgen de las tecnologías de la información y de la comunicación, cuando los otros instrumentos han resultado ineficaces o insuficientes para ello, son diversos los retos que se plantean, propios de un sector incipiente: unos, de carácter estrictamente terminológico, tendentes a consolidar una definición que sea comúnmente aceptada; otros, de determinación de sus peculiaridades y contenidos.

Carlos María Romeo Casabona afirma que el debate relativo a la rúbrica que debiera identificar esta área del conocimiento tiene su origen en la generalizada oposición, por parte de la doctrina, de admitir la expresión "delito informático" como definidora de las relaciones entre el Derecho penal y la informática. En algunos casos, por estimar que tal concepto no describe fielmente el conjunto de esas relaciones y, en otros, por considerar que ese delito no existe como tal entre las conductas tipificadas en las leyes penales, sean de carácter general o especial.

Igual suerte han corrido las diversas expresiones como "criminalidad informática" y "criminalidad por computadora", traducciones de las

locuciones "*crime by computer*" y "*Computer-Kriminalität*", acuñadas en los derechos anglosajón y centroeuropeo, así como "ciber-delito" o "ciber-crimen", en relación con la red de información. Unas y otras expresiones provienen más del área computacional o de la filosofía del derecho que de la ciencia jurídico-penal, lo que no es de extrañar dado el mayor interés demostrado por aquellas disciplinas en todos los órdenes del saber informático frente a la ciencia penal.

Para la mayoría de los autores, la denominación más acertada es la de "delitos informáticos" o "Derecho penal informático", por ser síntesis y especie a la vez de los géneros Derecho penal y Derecho informático, así como por considerar que responde adecuadamente a los contenidos y finalidades del estudio de este sector del ordenamiento jurídico penal.

La anterior precisión conceptual no obsta para que en el presente trabajo se haga uso de las expresiones "criminalidad informática" o "delincuencia informática", aludiendo al fenómeno delictivo específico, y obviamente la de "delitos informáticos" en sentido amplio y plural, que abarca todos los tipos penales que hagan referencia a las tecnologías de la información o de la comunicación, y no en términos estrictos.

En ese contexto, conceptualizar la expresión "delito cibernético" no es fácil, ya que para hablar de "delito" en el sentido de acción tipificada o contemplada en un ordenamiento jurídico-penal, se hace necesario que la propia expresión "delito cibernético" o "delito informático" esté consignada en el código punitivo; sin embargo, muchos especialistas en Derecho informático emplean estas alusiones indistintamente.

Así, para el maestro mexicano Julio Téllez Valdés (2003: p. 105), los delitos informáticos son conductas típicas, antijurídicas y culpables, en las cuales las computadoras pueden ser el instrumento o el fin. Nidia Callegari (1985: p. 115) define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas". Rafael Fernández Calvo (1996: p. 1150) lo define como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando el elemento informático o telemático contra los derechos y libertades de los ciudadanos

definidos en el título 1 de la Constitución Española". María de la Luz Lima (1984: pp. 99 y 100) sostiene que el delito electrónico, en sentido amplio, es "cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin" y que, en sentido estricto, "el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

Para el tratadista italiano Carlos Sarzana (1979: p. 59), el delito informático es: "cualquier comportamiento criminógeno en el que la computadora está involucrada como material, objeto o mero símbolo".

IV. Características de los delitos informáticos

Para el tratadista Julio Téllez Valdés (2003: pp. 105 y 106), los delitos cibernéticos o informáticos tienen las siguientes características:

- Son conductas criminógenas de cuello blanco (*white collar crimes*), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
- Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se encuentra trabajando.
- Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas.
- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, debido a su mismo carácter técnico.
- Ofrecen facilidades para su comisión a los menores de edad.

- Por el momento, muchos siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Para el tratadista José Ma. Palomino Martín (2006), la criminalidad informática se caracteriza, además, por otras notas distintivas:

- En el orden espacial, por su naturaleza transfronteriza, lo que exige la necesaria armonización de la legislación penal internacional.
- En el aspecto temporal, por tratarse de categorías penales tan efímeras, fluctuantes y volátiles como la propia telecomunicación.
- En el ámbito procesal, por las dificultades que supone su descubrimiento y acreditación.

Acerca de estas dificultades probatorias, particularmente en los delitos cometidos por medio de la red, la impunidad tendrá su origen, más que en vacíos de tipicidad, en obstáculos de perseguibilidad. La tipicidad se resuelve sin grandes dificultades, desplazando el núcleo del problema, que se centra en la formulación legal del tipo; sin embargo, consideramos que la perseguibilidad presenta obstáculos de carácter tecnológico en los que, además, el tiempo es un factor determinante para poder detectar el origen del ilícito, así como para impedir que siga causando sus perjudiciales efectos.

Las modalidades de la criminalidad informática pueden agruparse en función de tres corrientes de opinión:

- Aquella que ha puesto de relieve el aspecto subjetivo como elemento aglutinador de las conductas, en atención a una supuesta personalidad peculiar de los sujetos activos (*hackers, outsiders, insiders*), tendencia de autor hoy superada.
- Aquella otra que resalta o se fundamenta en el elemento objetivo lesionado (los bienes informáticos), con lo que reduce su ámbito de actuación a los ilícitos patrimoniales sobre los equipos y programas o sistemas.

- La más adecuada orientación funcional, que considera delincuencia informática aquella para la que las nuevas tecnologías son un "medio" de comisión o un "fin" en sí mismo. Se sirve de ellas como instrumento para lesionar otros bienes jurídicos o, por el contrario, el objeto material de la infracción son precisamente los equipos, los programas y las comunicaciones tecnológicas.

Todo lo expuesto pone de relieve la necesidad de mantener permanentemente actualizados los instrumentos penales, para la adecuada tutela del bien jurídico protegido y la eficaz prevención y, en su caso, sanción de conductas que se caracterizan por su dinamismo y mutación. Frente a ellas se impone establecer una política criminal ágil y eficaz, que evite el riesgo de observar un Derecho penal y procesal obsoleto.

Las alternativas para la protección penal frente a tales conductas son diversas, desde la reinterpretación jurisprudencial hasta la incorporación de nuevos tipos en leyes penales especiales o en los propios códigos penales.

España y México no han permanecido ajenos a estos procesos de adaptación, pues los avances tecnológicos han tenido su obligado reflejo en las reformas legales de 1995 y 1999, respectivamente, en las que se ha hecho mención explícita de los soportes informáticos, sea como objeto material del delito, o sea como medio para la realización de conductas que lesionan o ponen en peligro bienes jurídicos tutelados por las normas penales.

V. Naturaleza jurídica de los delitos informáticos en México

La determinación de los hechos que alcanzan relevancia penal entre los múltiples comportamientos irregulares que permiten las nuevas tecnologías es fundamental; es decir, se debe especificar la zona punible. Para ello es necesaria la selección de hechos que van surgiendo en el desarrollo de la vida moderna, vinculados con la informática, y que van a resultar relevantes para la adecuación de los tipos penales

ya existentes a las nuevas situaciones relacionadas con el uso de los sistemas informáticos.

Un diverso problema lo constituye la individualización de la responsabilidad criminal en el ámbito de los hechos punibles cometidos en Internet. No resultará fácil la determinación de la responsabilidad de los diversos sujetos que aparecen en el contexto general de la red, sea como operadores o como usuarios. Para ello es necesario distinguir entre hechos propios y ajenos, y determinar también la posible responsabilidad de quienes, como intermediarios de servicios facilitan o impiden ilegalmente el acceso y transmisión de información a través de la red.

Por otra parte, las posibilidades técnicas de las nuevas tecnologías obligan a abandonar la concepción del Derecho penal como cuerpo legislativo vigente para un determinado y exclusivo territorio, ya que se hacen patentes las limitaciones para la persecución de este tipo de hechos, derivadas de la aplicación puramente territorial de la ley penal.

De esta problemática se desprende la necesidad de armonizar y concertar legislaciones y mecanismos efectivos de cooperación internacional, a fin de evitar la fragmentación y aplicación territorial del derecho en una materia que se caracteriza por la transnacionalidad de sus efectos, atravesando fronteras como una de sus notas distintivas.

VI. Los delitos informáticos y las reformas penales de 1999

La creciente utilización de la tecnología en materia informática ha traído consigo el uso indebido de la información que se procesa a través de la computación; de ahí la necesidad de establecer tipos penales que sancionen esa ilícita conducta.

El interés jurídico a tutelar es la información que se procesa y almacena en un sistema informático, resultando indispensable contar con normas que prevean las penas aplicables para quienes desplieguen conductas que atenten contra la privacidad e integridad de esa información.

El concepto "sistema informático" está estrechamente vinculado con la definición de "informática" que encontramos en la Ley de

Información, Estadística y Geográfica, la cual señala que la informática comprende la tecnología para el tratamiento sistemático y racional de la información mediante el procesamiento electrónico de datos (artículo 3°, fracción VII).

El Estado mexicano, obligado a proteger los bienes jurídicos de los sectores que utilizan la informática como instrumento de desarrollo, requería un marco jurídico acorde al avance tecnológico, que permitiera prevenir y sancionar conductas que lesionaran o pusieran en peligro tales bienes.

Con anterioridad a la reforma al Código Penal Federal de 1999, sólo algunos estados de la República, como Sinaloa, Morelos y Tabasco, conscientes de la necesidad de legislar en esta materia, habían incorporado en sus ordenamientos penales normas tendentes a la protección de la información mediante la tipificación del delito informático y del de violación a la intimidad personal.

La inexistencia, hasta antes de 1999, de tipos penales exactamente aplicables a esas conductas ilícitas daba lugar a la impunidad, de manera que resultaba imperativo prever en la ley estas nuevas formas de delincuencia. La magnitud de los daños que esas conductas pueden ocasionar depende de la información que se vulnere, la cual puede tener un fuerte impacto en el desarrollo de la economía y la seguridad nacionales, o en las relaciones comerciales, tanto públicas como privadas.

Por tal motivo, resultaba necesario proteger la privacidad e integridad de la información contenida en sistemas y equipos de cómputo, así como su almacenamiento o procesamiento. Tal situación impelía a establecer normas que sancionaran a quienes, sin tener derecho a ello, accedieran a los equipos y sistemas de terceras personas para vulnerar la privacidad de la información, dañarla, alterarla o provocar su pérdida.

La iniciativa que presentó el Congreso mexicano y que dio origen a las reformas publicadas en el *Diario Oficial de la Federación* el 17 de mayo de 1999, propuso adicionar un capítulo al Código Penal Federal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer, copiar, modificar o provocar la pérdida de información que contengan. Esta iniciativa dio origen al capítulo

denominado "Acceso ilícito a sistemas y equipos de informática", que comprende los artículos 211 bis 1 al 211 bis 7, tutelándose así, a partir de dicha reforma, el bien jurídico consistente en la privacidad y la integridad de la información.

Asimismo, se propuso establecer una pena mayor cuando las conductas son cometidas en agravio del Estado, pues la utilización de sistemas de cómputo, computadoras, bases de datos y programas informáticos es cada vez mayor, como lo es la regulación por las leyes federales; tal es el caso de la Ley de Información, Estadística y Geográfica, la Ley del Mercado de Valores, la Ley que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública y la Ley Federal para el Control de Precursores Químicos, Productos Químicos Esenciales y Máquinas para Elaborar Cápsulas, Tabletas o Comprimidos, entre otras.

Además, en virtud de que las instituciones que integran el sistema financiero han sido con mayor frecuencia las víctimas por la comisión de estas conductas, se creó un artículo específico para proteger la información propiedad de aquéllas, el cual permite aumentar la pena hasta en una mitad cuando las conductas previstas sean cometidas por miembros de las propias instituciones.

Las referidas disposiciones, que fueron adicionadas al Código Penal Federal en el año de 1999, esencialmente tipifican comportamientos de quienes son conocidos en el ámbito de la informática como *hackers o crackers*, personas que atentan contra sistemas de cómputo.

Jesús Antonio Molina Salgado (cit. Nava, 2005: p. 80) señala: "La legislación mexicana en materia de delitos informáticos dista mucho de ser perfecta, es sólo el primer paso para lograr un ambiente sano y seguro para los negocios y comunicaciones electrónicas en nuestro país".

Algunas críticas que diversos tratadistas hacen a estas disposiciones, se pueden resumir en los siguientes términos:

- Se constituye el delito sólo si se accede a un sistema informático protegido por un mecanismo de seguridad. Esto es tan absurdo como si dijéramos que para que se actualice el delito de allanamiento de morada es necesario que la casa habitación

cuente con un candado, llave, portón o cadena protectora. La justicia no puede limitarse a quienes tienen los medios económicos para proteger su computadora con un mecanismo de seguridad.

- El ordenamiento penal no define lo que debe entenderse por "mecanismo de seguridad" de un sistema informático. ¿Debemos entender por ello una clave de acceso (*password*)?, ¿un candado contra robo (físico)?, ¿un sistema criptográfico de llave pública?, o simplemente ¿tener la computadora encerrada en un cuarto bajo llave? Esta falta de precisión originará sin duda innumerables problemas de interpretación.
- Nuestro código no contempla todos los tipos más comunes de ataques informáticos.
- El capítulo adicionado en virtud de la reforma del 17 de mayo de 1999 se denomina incorrectamente: "Acceso ilícito a sistemas y equipos de informática", ya que su articulado no se refiere exclusivamente a esa conducta.
- Además, muchos ataques informáticos se perpetran sin necesidad de acceder directamente a un sistema informático. El mejor ejemplo es la "denegación de servicios" (*denial of services* o *distributed denial of services*), cuyo objetivo no es "modificar, destruir o provocar pérdida de la información", como reiteradamente lo establece el Código Penal Federal, sino simplemente imposibilitar o inhabilitar temporalmente un servidor para que sus páginas o contenidos no puedan ser consultados mientras el servidor esté fuera de servicio o "caído".

Por su parte, el prestigiado jurista mexicano Raúl Carrancá y Rivas (2000: p. 574) escribe sobre esta reforma en la nota referente al artículo 211 bis 7: "En la especie, y en cuanto hace a la acción delictiva, no hay a mi juicio sino tres posibilidades: que se actúe terroristamente, en provecho propio o en provecho ajeno. Si se trata de lo primero, habría que remitirse al artículo 139 del Código Penal, siendo innecesaria, en consecuencia, la inclusión en el Código de este nuevo tipo. Mas por lo que atañe a la información obtenida y utilizada en provecho propio o ajeno, excepción hecha del terrorismo como ya queda dicho, a mi

juicio es evidente que se da en todos los casos, o sea, es parte substancial de la acción delictiva. No es un añadido, un agregado de la acción. En consecuencia ¿para qué agravar las penas?"

Otros autores disienten de la posición del doctor Carrancá y Rivas, aduciendo que, si bien en su mayoría son organizaciones delictivas las que realizan este tipo de conductas, también es cierto que existen particulares que no obtienen provecho alguno con el acceso a ciertos bancos de información, como es el caso de quien ingresa de manera ilícita al correo electrónico de otra persona para conocer el contenido de sus comunicaciones, transgrediendo así el ámbito de su intimidad, por lo que la conducta ilícita puede ocurrir fuera del contexto precisado por el doctor Carrancá.

En otro orden de ideas, conviene precisar que en el Código Penal Federal regularmente se establece, bajo el título correspondiente, el bien jurídico que se tutela, por ejemplo,: "Título Décimo Noveno: Delitos contra la vida y la integridad corporal", "Título Octavo: Delitos contra la moral pública y las buenas costumbres", "Título Séptimo: Delitos contra la salud", etcétera, pero en el caso que nos ocupa, el título se denomina "Revelación de secretos y acceso ilícito a sistemas y equipos de informática".

Lo anterior genera confusión en cuanto al bien jurídico tutelado, porque si éste fuera el patrimonio de las personas, la ubicación del capítulo relativo sería errónea. A pesar de que una de las conductas previstas es el daño a los sistemas, en la exposición de motivos de la multicitada reforma de 1999 se precisa que el bien jurídico tutelado es la privacidad y la integridad de la información.

Otro aspecto a destacar es el hecho de que en la legislación mexicana existen algunos códigos penales locales que contemplan a los delitos informáticos, aun cuando de manera genérica, y otros ordenamientos punitivos que no contienen ninguna disposición sobre este particular.

Así tenemos que los códigos penales de Aguascalientes y Tabasco establecen dichas figuras entre los delitos contra la seguridad en los medios informáticos y magnéticos; Baja California, en los delitos contra la inviolabilidad del secreto; Chiapas, Puebla, Querétaro, Zacatecas y Morelos, en los delitos contra la moral pública; Oaxaca, en los

delitos contra la moral pública y en los delitos contra la libertad y violación de otras garantías, y Tamaulipas, en los delitos de revelación de secretos y de acceso ilícito a sistemas y equipos de informática. A su vez, el Código Penal para el Distrito Federal contiene una supuesta figura de fraude informático en los artículos 230 y 231, fracción XIV.

Por su parte, los códigos penales de Baja California Sur, Campeche, Chihuahua, Coahuila, Durango, Estado de México, Guanajuato, Guerrero, Hidalgo, Jalisco, Michoacán, Nayarit, Nuevo León, Quintana Roo, San Luis Potosí, Sonora, Tlaxcala, Veracruz y Yucatán no contienen disposición alguna al respecto.

VII. La cibercriminalidad en el Derecho español

Con la aparición en las últimas décadas del fenómeno informático y las nuevas tecnologías se plantea el tratamiento penal que debe aplicarse a hechos delictuosos que lesionen intereses de particulares y de la comunidad en general, y que se cometan a través de estos medios.

En el momento de aplicar normas ya existentes a los nuevos sucesos, el surgimiento de problemas no se hace esperar, al tratarse de una legislación que, pese a diversas reformas, está situada en el contexto histórico y tecnológico del siglo XIX. Así, el primer problema fue dilucidar si los nuevos hechos delictuosos podían sancionarse con las viejas normas.

Ante la duda sobre la posible aplicación de la legislación vigente, el legislador español, al aprobar el Código Penal de 1995, lo que hizo fundamentalmente fue complementar la regulación existente incorporando supuestos concretos relacionados con la informática.

Así, junto a la estafa clásica, se situó la estafa electrónica y, a los daños ya previstos, se incorporaron los daños sobre elementos informáticos. Pocos fueron los hechos punibles completamente nuevos, si acaso el previsto en el artículo 256, que a continuación se transcribe:

> 256. El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

Con ello se consiguió una mayor seguridad jurídica a fin de que los tribunales puedan aplicar estas nuevas normas a la delincuencia informática.

VIII. El Código Penal español de 1995

El Código Penal español de 1995 aborda de diferentes maneras el fenómeno de la criminalidad informática, a la que trata de dar respuesta con la nueva regulación. En algunos tipos, incrimina determinados supuestos de forma paralela a los delitos convencionales ya existentes. En este caso, el elemento informático puede consistir en un medio especialmente relevante para la ejecución del hecho punible, o bien actuar como elemento especialmente cualificado sobre el que se dirige la acción delictiva. Para este grupo de supuestos se incriminan específicamente aquellas conductas que tienen que ver con la informática, como se ha dicho, en su papel de cualificado medio de ejecución (para el caso de la estafa informática o electrónica), o de otra manera, como cualificado objeto material sobre el que actúa el autor del delito (delito de daños).

Pero en realidad, la relevancia de los objetos informáticos no acaba con estas dos categorías (como medio de ejecución o como objeto material particularmente determinados), ya que en otros casos el legislador no establece expresamente la posibilidad de que intervengan elementos informáticos en determinados supuestos delictivos.

En otros tipos penales nada se especifica sobre la posible concurrencia de estos elementos, pero en realidad nada impide su presencia. Tipos, por lo tanto, en los que no hay previsión legal específica, pero que pueden realizarse a través de las nuevas tecnologías (amenazas, injurias, calumnias, publicidad engañosa, daños a la propiedad intelectual y a la propiedad industrial, difusión de pornografía, etcétera).

No es propósito de este trabajo efectuar un análisis de cada uno de los preceptos de la legislación española en la materia; sin embargo, dada la normativa que contiene el Código Penal de 1995, se advierte que los tipos penales relacionados con la informática pueden agruparse en dos apartados:

- Las infracciones penales que hacen mención explícita a las nuevas tecnologías de la información o de la comunicación, considerando el soporte tecnológico como objeto material del delito o como medio para la lesión o puesta en peligro de bienes jurídicos.
- Todos aquellos delitos comunes que, pese a no estar expresamente relacionados con las nuevas tecnologías, pueden cometerse a través de la informática o la telemática.

A su vez, los supuestos en los que de alguna manera los elementos informáticos pueden constituir parte del hecho punible, aparecen fundamentalmente en tres grupos de delitos:

1. Delitos contra el derecho a la intimidad y a la propia imagen, realizados por vía del descubrimiento o la revelación de datos contenidos en soportes informáticos o telemáticos, previstos en los artículos 197 a 201 del Código Penal español.
2. Delitos que constituyen lo que la doctrina denomina falsedades documentales, cometidas por medio de programas informáticos, previstas en el artículo 400 del Código Penal español.
3. Delitos contra el patrimonio y el orden socioeconómico perpretados sobre o mediante equipos y programas informáticos o telemáticos, entre los que se encuentran los siguientes ilícitos:
   - Robo mediante tarjeta (artículos 237 y 239).
   - Estafa por medios informáticos (artículo 248).
   - Defraudación mediante telecomunicación y uso ilegal de equipo terminal de telecomunicación (artículos 255, 256 y 623.4).
   - Daños a datos, programas o documentos electrónicos (artículo 264.2).
   - Delitos contra la propiedad intelectual de los programas o contra la neutralización de sus dispositivos de protección (artículo 270).
   - Delitos contra la propiedad industrial (artículo 273.3).
   - Delitos de descubrimiento y difusión de secreto de empresa, que afectan la libre competencia (278).

- Delitos relativos al acceso ilegal a los servicios de radiodifusión sonora, televisiva o interactiva (artículo 286).

Por último, entre los delitos que se pueden cometer por medios tecnológicos, destacan los siguientes:

- Publicidad engañosa por medio de la red (artículo 282).
- Delitos y faltas contra la libertad por medios informáticos o telemáticos (artículo 169 y siguientes, y 620).
- Delitos contra la libertad e indemnidad sexuales cometidos por medios electrónicos (artículo 184 y siguientes), particularmente la difusión de pornografía infantil a través de la red (artículo 189).
- Delitos contra el honor cometidos mediante transmisiones electrónicas (artículos 30, 205 y siguientes).
- Falsificación de cuentas de una sociedad y blanqueo de capitales por medios informáticos o telemáticos (artículos 290 y 301).
- Apología de conductas terroristas, genocidas, xenófobas o discriminatorias (artículo 18 en relación con los diversos artículos 510, 578 y 607.2).

IX. Individualización de la responsabilidad penal

Desde el primer momento en que aparecen las nuevas tecnologías y particularmente el mundo de Internet se plantean los límites y posibles responsabilidades derivadas de un uso irregular o ilícito de estos mecanismos. Dentro del debate general sobre la regulación de estos nuevos medios de comunicación y difusión, uno de los aspectos más complejos y delicados es el de correcta determinación de posibles responsabilidades para cada uno de los sujetos que intervienen en una compleja amalgama de partes que se suman e interactúan en el proceso total.

Efectivamente, la individualización de responsabilidades por hechos ilícitos se dificulta por tratarse de un campo con características muy específicas. Por lo reciente, y también por su complejidad, en muchas ocasiones estamos frente a un ámbito carente de regulación

jurídica, en general y no tan solo penal, o bien parcialmente regulado. Por su propia naturaleza, Internet es una red que no cuenta con autoridades o dirigentes, y su uso implica efectos trasnacionales. Internet realmente no sólo rebasa las fronteras nacionales, sino que además puede relacionar puntos del planeta distantes en lo geográfico, en lo cultural y en lo jurídico, lo que añade sin duda mayores dificultades para la implementación de una normativa aplicable y eficaz. Además, en el proceso de selección de ámbitos de responsabilidad surgen dificultades suplementarias debido a la confluencia de agentes con papales diversos, dado que entre usuarios y destinatarios existe un gran número de intermediarios.

En esta situación de relevantes singularidades y dificultades se cuestiona cuál debe ser el modelo de responsabilidad a seguir que represente mayor seguridad jurídica para los usuarios y permita la debida aplicación de la ley por parte de los tribunales. Esta problemática ha sido abordada en España, por lo que en seguida se reseñan tres alternativas posibles en cuanto a la individualización de la responsabilidad por ilícitos penales que podrían cometerse a través de la red:

a) Un primer modelo de responsabilidad corresponde al modelo tradicional de autoría en medios de comunicación de masas establecido en el artículo 30 del Código Penal español. Este artículo básicamente establece un mecanismo jurídico de responsabilidad escalonada (responsabilidad en cascada), que atribuye responsabilidad sucesivamente a quien se encuentre en las distintas posiciones que se determinan siguiendo el orden establecido legalmente. En este caso no es posible atribuirle responsabilidad a sujetos situados en distintos escalones, pues únicamente cabe exigir responsabilidad a los integrantes de un escalón si no es posible exigírsela a los del escalón previo.

Algunos autores estiman que la fórmula del artículo 30, referente a la utilización de "medios o soportes de difusión mecánicos", deja fuera a Internet, así como a un conjunto de medios de comunicación que en la actualidad ya no trabajan con medios mecánicos, sino que disponen de sistemas informáticos. Sin embargo, la mayoría de los tratadistas coincide en que no hay razón para limitar la aplicación del

artículo 30 a los tradicionales medios de comunicación, pues el sentido del concepto mecánico sería el de "ingenio, reproductor que el ser humano utiliza y que de él se diferencia, abarca de la más primitiva técnica de imprenta hasta la captación de imágenes o sonido vía satélite".

Sin embargo, desde un punto de vista material, el uso de Internet representa una mayor complejidad debido, como ya se ha mencionado, a la ausencia de organización jerárquica, a la que en buena medida responde el artículo 30.

b) En la actualidad, el Derecho penal español cuenta con un sistema de responsabilidad legal que no tiene el carácter de pena, previsto en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, de 11 de junio de 2002.

En el texto de la ley se señala que "los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico", por lo que determina la responsabilidad de los prestadores de servicios por el ejercicio de actividades de intermediación (artículo 13).

La mencionada ley establece las condiciones de responsabilidad para cada una de las modalidades de intermediación que regula: operadores de redes proveedores de acceso (artículo 14), servicios de copia temporal de datos solicitados por el usuario (artículo 15), servicio de alojamiento o almacenamiento de datos (artículo 16), servicios de enlace a contenidos o instrumentos de búsqueda (artículo 17), atribuyendo la responsabilidad por actos o contenidos propios y por actos o contenidos ajenos.

La responsabilidad por contenidos propios (autoría), según el mencionado ordenamiento legal, se refiere a contenidos realizados por el operador que efectúa la transmisión, bien que haya originado la transmisión, bien modificado los datos objeto de transmisión o bien efectuado la selección de los datos o de los destinatarios de los mismos. En estos casos, la ley prevé que debe responderse como si se tratara de contenido propio, es decir, como si se tratara del autor material de los datos ilícitos.

Para poder exigir algún tipo de responsabilidad en los casos de contenidos ajenos se requiere la existencia del conocimiento efectivo de la ilicitud o de la lesión de bienes o derechos de un tercero, o una actuación no diligente para impedir el acceso de terceros a los mismos.

c) Ante las dificultades para la aplicación de los dos modelos anteriores y las necesidades particulares en la materia, la doctrina española propone, desde una perspectiva político-criminal, un modelo de responsabilidad penal en el ámbito de Internet, partiendo de las bases generales de la imputación, pero teniendo en cuenta los principales aspectos de los dos modelos, tanto del relativo a los delitos cometidos en medios de comunicación en masas, como de los criterios establecidos en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.

En primer lugar, se estima adecuado el castigo únicamente de conductas de autoría (directa, mediata y coautoría) y no de mera complicidad o favorecimiento, como en los supuestos del artículo 30 del Código Penal. El fundamento de esta exclusión sería semejante al sostenido para los delitos sometidos al régimen del citado artículo. Se trataría de evitar un ahogamiento excesivo de las libertades fundamentales que pueden tener su vía de expresión a través de estos medios de comunicación.

En cuanto a la responsabilidad por contenidos y actividades propias se incluyen, en el sentido que lo hace la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, los supuestos en los que el operador de Internet haya originado la transmisión, modificado los datos de transmisión, efectuado la selección de los datos o de los destinatarios. En estos casos se debe considerar autor del ilícito correspondiente y responsable al operador en Internet por tratarse de hechos propios.

La responsabilidad por contenidos y actividades ajenas es la que entraña mayores dificultades al momento de su apreciación e individualización. Descartada, por su imposibilidad práctica, la vigilancia general sobre los contenidos a los que sirve como intermediario, queda claro, en principio, la inexistencia de una obligación general de control por parte del proveedor en relación con los contenidos y

actividades ajenos. De tal forma, el presupuesto inicial para una posible responsabilidad del prestador de servicios es el de un auténtico conocimiento efectivo del hecho o actividad ilícita. Así pues, el conocimiento previo y efectivo resulta imprescindible para generar algún tipo de responsabilidad penal, que por tanto no puede basarse en un conocimiento meramente hipotético del acto constitutivo del ilícito penal.

Sobre la base de ese conocimiento del responsable de la prestación de determinados servicios se puede plantear una modalidad dolosa de responsabilidad penal, si en el caso particular decide no retirar los contenidos o no hacerlos inaccesibles, omitiendo por tanto cualquier género de actividad de control sobre éstos.

También puede producirse un hecho que genere responsabilidad basado en la actuación imprudente, siempre sobre la base del conocimiento efectivo, consistente en la no actuación suficientemente diligente para retirar los contenidos o impedir el acceso a los mismos. Se trata de un supuesto de imprudencia por omisión, en el que será necesario establecer los parámetros de diligencia para retirar o impedir el acceso a los contenidos ilícitos, la constatación del tiempo necesario para llevar a cabo la acción de control sobre los contenidos no será de fácil concreción y, a su vez, será determinante para fijar el momento de la consumación del hecho delictivo.

IX. Nueva legislación penal: el Convenio de Cibercrimen (Budapest, 23.11.2001)

La cooperación internacional para la atención de delitos informáticos, los cuales traspasan con gran facilidad los límites nacionales, es indispensable. Por ello, distintos grupos de trabajo unen esfuerzos a fin de implementar instrumentos aptos para combatir una forma de delincuencia claramente trasnacional.

Dentro de la actividad legislativa para lograr el más adecuado tratamiento jurídico-penal de los nuevos hechos ilícitos vinculados con la informática se han desplegado intensos esfuerzos en distintos organismos internacionales, cuyo logro más notable es el Convenio de Cibercrimen, de 23 de noviembre de 2001. Redactado en el

marco de la actividad del Consejo de Europa, pero abierto a la firma de cualquier país, representa por el momento el instrumento internacional más válido frente a la cibercriminalidad; sin embargo, a pesar de estar firmado por más de treinta países, no cuenta con el número suficiente de ratificaciones para su entrada en vigor. Tal circunstancia no puede ser impedimento para su análisis, advirtiéndose que la finalidad que persigue es la armonización de los hechos punibles vinculados a la informática, que deben estar penalizados en los países firmantes.

Así, el Convenio de Cibercrimen propone varias infracciones que deben estar incorporadas a las legislaciones nacionales y que clasifica en cuatro grandes grupos de ilícitos penales:

Un primer grupo lo constituyen los hechos contrarios a la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Dentro de este grupo se incluyen las conductas de acceso ilegal, injustificado, a todo o parte de un sistema informático (artículo 2). El convenio permite que las partes firmantes modulen la incriminación de este supuesto mediante diferentes formas, por lo que es posible vincular la punibilidad de esa conducta a la violación de medidas de seguridad, por ejemplo. También se abarcan los supuestos de interceptación ilegal de comunicaciones entre sistemas informáticos o en el interior del mismo sistema, mediante el empleo de medios técnicos (artículo 3).

Al segundo grupo de conductas, el convenio las denomina infracciones informáticas, y en ellas incluye la falsedad informática y el fraude informático.

El tercer grupo se refiere a las infracciones relativas al contenido, que incluyen múltiples conductas realizadas sobre materiales de pornografía infantil. Se incluyen conductas de producción, ofrecimiento, difusión, transmisión o procuración para otro, por medio de un sistema informático, de pornografía infantil. Se extiende la incriminación a la obtención para sí mismo de estos materiales mediante un sistema informático (artículo 9.1,d) o la mera posesión del material en un sistema informático o de almacenamiento de datos informáticos (artículo 9.1,e).

Por último, en el cuarto grupo, la propiedad intelectual y los derechos conexos son objeto de protección penal mediante lo dispuesto

en el artículo 10 de la convención. Se pretende incriminar los atentados a la propiedad intelectual y derecho conexos definidos en los acuerdos internacionales, cometidos deliberadamente con fines comerciales por medio de sistemas informáticos. El convenio deja a salvo la posibilidad de que alguno de los países firmantes no incriminen estas conductas a condición de que se dispongan de otros recursos eficaces para su tutela y que tal falta de incriminación no suponga el incumplimiento de obligaciones internacionales que incumban a esa parte.

Con carácter adicional y complementario al convenio sobre cibercriminalidad, el 28 de enero de 2003 se firmó en Estrasburgo un protocolo sobre incriminación de actos de naturaleza racista y xenófoba, así como de actos por los que se trate de negar o justificar el genocidio o los crímenes contra la humanidad, llevados a cabo por medio de sistemas informáticos.

Conclusión

Paralelamente al avance y al desarrollo tecnológico de los países surgen nuevas formas de conducta antisocial que han hecho de los equipos y sistemas informáticos instrumentos para delinquir. México y España no son ajenos a este problema.

Con motivo de las limitantes que existen, de muy diversa índole, para la persecución de los delitos informáticos, debido fundamentalmente a sus efectos trasnacionales, es imprescindible la actualización de legislaciones y la concertación de mecanismos efectivos de cooperación internacional.

La problemática que representa el "cibercrimen", aludiendo con tal vocablo a todo lo relacionado con los delitos informáticos y sus nocivos efectos, los cuales pueden llegar a ser incluso devastadores para la economía de cualquier país del mundo, tomando en consideración que la delincuencia organizada cuenta con la tecnología más moderna y sofisticada, constituye una amenaza latente para la humanidad. Por tal motivo, se requiere la atención permanente del legislador a fin de diseñar normas adecuadas y eficaces para su tratamiento, tanto preventivo como sancionador.

Además, los efectos trasnacionales de este flagelo de la era moderna llaman a reflexionar sobre los problemas que generan la fragmentación y la aplicación territorial del derecho, lo que hace imperativo contar con mecanismos efectivos de cooperación internacional, que evidencien el concierto de las naciones en la lucha contra la delincuencia informática.

Referencias

obras generales

Grupo Anaya, *Diccionario Anaya de la Lengua*, Madrid, Grupo Anaya, 1991.

Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, *Diccionario jurídico mexicano*, México, Porrúa, 2001.

Obras particulares

Anarte Borrallo, Enrique (2002): "Sobre los límites de la protección personal de datos personales", en *Derecho y conocimiento. Anuario jurídico sobre la sociedad de la información y del conocimiento*, volumen 2, Universidad de Huelva.

Arroyo Zapatero, Luis y Klaus Tiedmann (1994): *Estudios de Derecho penal económico*, Cuenca, Ediciones de la Universidad de Castilla-La Mancha.

Barrios Garrido, Gabriela (1998): *Internet y Derecho en México*, México, Mc Graw-Hill.

Callegari, Nidia (1985): "Delitos informáticos", en *Revista de la Facultad de Derecho y Ciencias Políticas* de la UPB, Colombia, núm. 70, julio-septiembre.

Carrancá y Trujillo, Raúl y Raúl Carrancá y Rivas (2000): *Código Penal anotado*, México, Porrúa.

Choclán Montalvo, José Antonio (2006): *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político criminales*, Granada, Comares.

Fernández Calvo, Rafael (1996): "El tratamiento del llamado delito informático en el proyecto de Ley orgánica del Código Penal: reflexiones y propuestas de la CLI (Comisión de Libertades e Informática)", en *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, España, UNED, Centro Regional de Extremadura, núms. 12-15.

Lima Malvado, María de la Luz (1984): "Delitos electrónicos", en *Criminalia*, México, Academia Mexicana de Ciencias Penales, núms. 1-6, enero-junio.

López-Muñiz Goñi, Miguel (1984): *Informática jurídica documental*, Madrid, Díaz de Santos.

Nava Garcés, Alberto Enrique (2005): *Análisis de los delitos informáticos*, México, Porrúa.

Palomino Martín, José María (2006): *Derecho penal y nuevas tecnologías*, Valencia, Tirant lo Blanch.

Ríos Estavillo, Juan José (1997): *Derecho e informática en México*, México, UNAM.

Ruiz Miguel, Carlos *et al.* (2004): *Temas de Direito da informática e da internet*, Coimbra, CoimbraEditora/Ordem dos Advogados [Conselho Distrital do Porto].

Sarzana, Carlos (1979): "Criminalità e tecnologia: il caso del computer crime", en *Rassegna Penitenziaria e Criminología,* Roma, núms. 1-2, año 1.

Téllez Valdés, Julio (2003): *Derecho informático*, México, Mc-Graw Hill.