

Consejo Editorial de la revista Cubalex

Directora: Dra. Ivonne Pérez Gutiérrez

Profesora Titular de Derecho Procesal de la Facultad de Derecho de la Universidad de La Habana y Secretaria de la Sociedad Cubana de Derecho procesal.

E. mail: ivonne@lex.uh.cu // ivonnep66@gmail.com

Consejo Editorial

Presidente: Dr. Arnel Medina Cuenca

Profesor Titular de Derecho Penal de la Facultad de Derecho de la Universidad de La Habana y vicepresidente de la Sociedad Cubana de Ciencias Penales.

E. mail: arnel@lex.uh.cu // arnelmedinacuenca@yahoo.es

Secretario: Lic. Luis Alberto Hierro Sánchez

Profesor Asistente de Derecho Procesal de la Facultad de Derecho de la Universidad de La Habana. Miembro de la Sociedad Cubana de Derecho Procesal.

E. mail: hierro@lex.uh.cu // labsanchez90@gmail.com

Miembros del Consejo Editorial

Dra. Yamila González Ferrer

Vicepresidenta de la JDN de la UNJC y de la Sociedad cubana de Derecho Civil y de Familia. Profesora Auxiliar de Derecho de Familia de la Facultad de Derecho de la Universidad de la Habana.

E. mail: degijoya@yahoo.com // secretaria@unjc.co.cu

Lic. Emiliano Manresa Porto

Funcionario de la Sede nacional de la UNJC y Vicepresidente de la Sociedad Cubana de Derecho e Informática.

E. mail: emanresap@gmail.com // manresa@unjc.co.cu

MSc. Ana María Pozo Armenteros

Mediadora de la Corte Cubana de Arbitraje Comercial Internacional.

E. mail: ampa_lawyer@yahoo.es

Versión Electrónica disponible en: <http://vlex.com/source/revista-cubalex-12125>

Redacción y Administración Calle 21, No.552, esq. a D, Apartado Postal 4161, Vedado, La Habana. CP 10400, La Habana, Cuba.

Teléfonos:(53)7832-6209/ 7832-9680/ 7832-7562/ 7832-6513/ 7832-6514/ 7832-6616.

Email: unjc@unjc.co.cu Web: www.unjc.co.cu RNPS- 1816, ISSN 1028-8988.

Nota: Los artículos publicados expresan exclusivamente la opinión del autor y no constituyen el criterio oficial de la Editorial UNJURIS.

ÍNDICE

Artículos

El Derecho penal en la actualidad / 1

Dra. C. Ana Isabel Pérez Cepeda, España

Gestación subrogada como derecho humano, omisión legislativa en México / 22

Dra. Guadalupe Romano Casas, México

El delito informático. Pautas en su configuración normativa / 46

Dr. C. Rodolfo Máximo Fernández Romo, Cuba

Dr. C. Waldemar Paulo da Silva José, Angola

Dr. C. Juan Antonio Peña Aguirre, Ecuador

Regulación jurídica de los procedimientos administrativos tributarios. Una visión desde el escenario de reforma económica en Cuba / 65

Esp. Damaris Carbonell Martínez, Cuba

Los principios informadores de la ejecución de la pena privativa de libertad ante la futura Ley de Ejecución Penal cubana / 103

MSc. Yoel Quinta Arango, Cuba

De la política criminal a los fundamentos constitucionales que amparan el principio procesal de Oportunidad / 122

Dra. C. Rufina de la C. Hernández Rodríguez, Cuba

Sistema multilateral de comercio y empleo. Análisis desde la visión conjunta OMC y OIT / 144

MSc Desiree Llaguno Cerezo, Cuba

MSc. Elizabeth Valdés-Miranda Fernández, Cuba

Apuntes para un punto de partida: La conciliación en el proceso penal cubano / 156

Dra. C. Darina Ortega León, Cuba

Dra. C. María Elvira Batista Ojeda, Cuba

El matrimonio entre el mismo sexo en México: un derecho denegado / 179

Dr. C. Eduardo Ramírez Patiño, México

Dra. C. Lizbeth García Montoya, México

Compliance laboral: una mirada desde de los fundamentos jurídicos cubanos / 199

MSc. Guillermo Ferriol Molina, Cuba

La Reforma Penal en Cuba. A propósito del ámbito de intervención en la Economía / 216

Esp. Mariano Rodríguez García, Cuba

Mujeres étnicas víctimas de violencia en un contexto cultural. Estudio victimológico / 236

Dra. C. Lizbeth García Montoya, México

Dr. Gonzalo Armienta Hernández, México

Diagnóstico del estado de la prostitución en relación con las principales agencias de control social del municipio San José de las Lajas, provincia Mayabeque durante el año 2017 / 264

Dra. Elia Esther Rega Ferrán, Cuba

MSc. Yuliett Valdés Acosta, Cuba

La mediación en el plexo del contrato de acogimiento familiar de personas mayores. Una propuesta razonable para Cuba / 282

Dra. C. Noadis Milán Morales, Cuba

Dra. C. Celia Araujo Quintero, Cuba

Breves acotaciones en torno al legado de bien común / 305

Dr. Freddy Andrés Hung Gil, Cuba

MSc. Washington Javier Bazantes Escobar, Ecuador

La Organización Internacional del Trabajo ante la Agenda 2030. El caso del Objetivo 16 / 313

Lic. Ernesto Moreira Sardiñas, Cuba

El trabajo infantil y la importancia del marco normativo y social para su enfrentamiento y prevención en el Ecuador / 324

Dra. C. Katherine Elizabeth Sandoval Escobar, Ecuador

Dra. C. Angela Gómez Pérez, Cuba

Sección estudiantil

Comentarios en torno a las acciones de cumplimiento de los Objetivos de Desarrollo Sostenible en el entorno Energético Cubano / 340

Marian Cordero Pío, Cuba

Crónicas de legislación

Cortesía de la Revista Cubana de Derecho / 352

Dr. Leonardo B. Pérez Gallardo, Cuba y Dr. Carlos A. Pérez Inclán, Cuba

Selección de Normas Jurídicas publicadas en la Gaceta Oficial de la República de Cuba, de enero de 2019 a diciembre de 2019 / 354

MSc. Ana María Pozo Armenteros

Crónicas de sentencias

Cortesía de la Revista Cubana de Derecho / 399

Dr. Leonardo B. Pérez Gallardo, Cuba

La vinculación del Tribunal de instancia al resultado de las pruebas de libre valoración y su control casacional. Análisis de la sentencia 84 de 27 de febrero de 2017 del Tribunal Supremo Popular / 403

Dra. Nilda Haydeé Rizo Pérez, Cuba

Esp. Adriana Cristina Morales Atala, Cuba

Lic. Daniel Ramis González, Cuba

Reseñas bibliográficas

Editorial UNIJURIS de la UNJC / 413

Cortesía de la Revista Derecho, Empresa y Sociedad (REDS) No. 13, época II, julio- diciembre 2018, pp. 368 – 376 / 428

Cortesía de la Revista Cubana de Derecho, IV Época No. 53, enero - junio de 2019, pp. 153 - 210 / 456

El jurista en la sociedad, dedicada a destacar los premios y reconocimientos relevantes recibidos por los juristas cubanos

Premio Nacional de Derecho Carlos Manuel de Céspedes 2019.

Dra. Martha Prieto Valdés / 480

Premio al Jurista Joven 2019 "José Garcerán de Vall Vera".

Dra. Orisel Hernández Aguilar / 484

Publicaciones de la Editorial UNIJURIS

Hasta el I Semestre de 2020

Destinada a facilitar a los investigadores y profesionales del Derecho la información sobre las publicaciones de la Editorial UNIJURIS / 486

Comité científico / 493

Normas editoriales / 498

Artículos

El delito informático. Pautas en su configuración normativa

The Computer Crime: guidelines of its regulatory configuration

Recibido: 23 de febrero de 2020

Aprobado: 21 de marzo de 2020

DR. C. RODOLFO MÁXIMO FERNÁNDEZ ROMO*

CUBA

DR. C. WALDEMAR PAULO DA SILVA JOSÉ**

ANGOLA

DR. C. JUAN ANTONIO PEÑA AGUIRRE***

ECUADOR

Sumario

1. Introducción
2. Del bien jurídico y los delitos informáticos
 - 2.1. La información como bien jurídico tutelado
 - 2.2. Posibles bienes jurídicos generales que exigen tutela
 - 2.2.1. Seguridad informática
 - 2.2.2. Integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos
 - 2.2.3. Intimidad informática
3. Posibles bienes jurídicos particulares que exigen tutela
 - 3.1. Propiedad intelectual
 - 3.2. La indemnidad sexual
4. Conclusiones

* Doctor en Ciencias Jurídicas. Especialista en Derecho Penal. Profesor Titular de Derecho Procesal y Criminalística de la Facultad de Derecho de la Universidad de La Habana. Cuba. rfr6311@gmail.com. Registro ORCID: <https://orcid.org/0000-0003-4015-2837>

** Doctor en Ciencias Jurídicas. Máster en Criminalística. Subcomisario de la Policía Nacional de Angola, Vice Director General del Instituto Superior de Ciencias Policiales y Criminales. foxwadas@hotmail.com Registro ORCID: <https://orcid.org/0000-0002-9346-9232>

*** Máster en Informática y Derecho. Doctor en Ciencias Jurídicas. Profesor Titular de la Facultad de Jurisprudencia, Ciencias Políticas y Sociales de la Universidad de Cuenca. Ecuador. documentologiacuenca@hotmail.com Registro ORCID: <https://orcid.org/0000-0003-2156-7092>

Resumen

El uso de las tecnologías de la información y las comunicaciones genera un desarrollo incuestionable en diferentes espacios de las sociedades modernas, pero también se utiliza para la comisión de supuestas actividades ilegales de diversa naturaleza, particularidad que pone de relieve un polémico debate respecto al bien jurídico que se debe proteger desde el derecho penal, lo que se cuestiona teóricamente en el presente artículo a los efectos de su coherente regulación normativa.

Palabras clave

Delito informático, bien jurídico, Derecho penal.

Abstract

The use of information and communication technologies generates an unquestionable development in different areas of modern societies, but it is also used for the commission of alleged illegal activities of various kinds, a feature that highlights a controversial debate regarding the legal right that must be protected from criminal law, which is theoretically questioned in this article to the effects of its coherent normative regulation.

Keywords

Computer crime, legal asset, criminal law

1. Introducción

El desarrollo de las tecnologías de la información y las comunicaciones generan la creación de sistemas telemáticos que facilitan el aumento de las capacidades de almacenamiento y procesamiento de datos de diversa naturaleza, lo que hace suponer en primer orden que se vive en la “era de la información” y en segundo lugar, que mucha de esa información puede ser cuestionada a los efectos de su vinculación con una posible responsabilidad penal.

El tratamiento automático de la información y de las modernas tecnologías de las telecomunicaciones, plantean también problemas de importancia crucial para el funcionamiento y la seguridad de los sistemas informáticos y telemáticos en los negocios y relaciones comerciales, en la administración y en la sociedad en general, ya que en casi todos los ámbitos de la vida hoy se depende de la tecnología informática, la telemática y de los bancos de datos.

Desde las perspectivas descritas se advierte de forma clara que los soportes en los que se desarrollan las tecnologías de la información son cada vez más variados, los que pueden ser utilizados para la ejecución de acciones ilegales en carácter de delitos informáticos o como medios o vías de la comisión de otros tipos penales tradicionales.

A los efectos de poder atribuir a determinada persona la comisión de un supuesto delito informático o el haber hecho uso de este soporte para la ejecución de un delito

tradicional, se impone delimitar un aspecto esencial que va dirigido a la consideración del bien jurídico que protegen los hoy denominados delitos informáticos, particular que genera polémica por la diversidad de criterios y distinta forma que desde lo normativo lo han asumido las diferentes legislaciones nacionales.

2. Del bien jurídico y los delitos informáticos

Para una correcta delimitación de los bienes jurídicos que debe proteger el Derecho penal en acciones presuntamente ilegales vinculados al uso de la informática y a las nuevas tecnologías de la información es preciso determinar los riesgos posibles de los hechos que se ejecutan y en tanto qué conductas deben ser prohibidas por la norma; advirtiéndose, en lo fundamental, dos criterios que sirven de sustento en el ámbito teórico y de base de los diferentes movimientos legislativos.

Un primer criterio, partidario de incorporar a la tutela penal los “nuevos” bienes jurídicos que han nacido como resultado de la generalización y consolidación de los medios y procedimientos informáticos y que tendrían la suficiente importancia para merecer la intervención penal; todo partiendo del criterio de la insuficiencia demostrada de las previsiones penales actuales disponibles para enfrentar los problemas de punición que presentan las acciones reputadas de ilegales y vinculadas a la informática¹.

El otro criterio, partidario de agotar las posibilidades de protección que ofrece el derecho vigente, sobre la base de los bienes jurídicos “tradicionales”; sin perjuicio, naturalmente, de introducir, en la medida en que resulten precisas, las modificaciones concretas necesarias².

La posición más caracterizada del primer criterio doctrinal es la de quienes mantienen la conveniencia de destacar su protección como sector autónomo del ordenamiento y de la dogmática penal, el que se denomina “Derecho penal de la informática” o “Derecho penal informático”³.

Sin embargo, se debe admitir que a pesar de que las normas penales que se ocupan ahora de la criminalidad informática constituyen un conjunto heterogéneo, con una clara visión sectorial y fragmentaria, lo cual hace necesario un tratamiento conceptual que tenga en cuenta los puntos comunes, las semejanzas entre unas y otras normas,

¹ MATA y MARTÍN, R. M., “La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías”. En: *Revista Penal*. Nº 18, julio 2006, p. 14. MORÓN LERMA, Esther. Internet y Derecho penal: hacking y otras conductas ilícitas en la red. Aranzadi. Pamplona, 2002, p. 3.

² ROVIRA DEL CANTO, E; Delincuencia Informática y fraudes informáticos. Comares. Granada. 2002 p.16; ROMERO CASABONA, C.,. “Los delitos de daños en el ámbito informático”. En: *Cuadernos de Política Criminal*. Coímbra editora, 1991, p. 28.

³ ZÚÑIGA RODRÍGUEZ, L., Derecho Penal, sociedad y nuevas tecnologías. Colex. Madrid, 2001, p. 43.

para poner un cierto orden en la materia y poder contar realmente con un sector autónomo⁴.

Sobre las bases expuestas se construiría lo que se podría denominar directamente el “Derecho penal de la informática”. El criterio en torno al que se construiría el mismo es, en primer lugar, el bien jurídico protegido, y, como elemento auxiliar, la clasificación sistemática de las figuras; así como la propia evolución legislativa y el análisis de las razones que determinaron su incorporación al Código penal.

Siguiendo la posición que admite la existencia de un Derecho penal de la informática y dando por sentado los inconvenientes que puede presentar una solución de esta naturaleza en relación con la dispersión del bien o bienes jurídicos implicados y la lejanía de la referencia de éstos si se configura el nuevo delito como de simple actividad (de peligro abstracto o de peligro abstracto concreto) la elaboración de un bien jurídico en los ámbitos que se analiza podría contribuir a mitigar parte de estos obstáculos.

Otro aspecto sobre el que debería reflexionarse antes de tomar una decisión de política legislativa al respecto sería la valoración de posible concurrencia de determinados elementos subjetivos, que podrían dar lugar a un diferenciado desvalor -entre sí- de lo injusto, con su correspondiente repercusión agravatoria del marco punitivo. Ello especialmente referido a las intromisiones en los ámbitos personales y lo que comportan los derechos inherentes a la personalidad.

También será necesario reflexionar sobre si en estos casos el recurso a la tipificación penal estará o no justificado en virtud de los principios de última ratio y de intervención mínima del Derecho penal, aquí entran en juego, por ejemplo, el acceso ilegítimo, sin el propósito de ocasionar daños determinados. Tampoco debería abusarse del recurso a los instrumentos punitivos, dado que a través de normas extrapenales podrían satisfacerse -al menos en buena medida- las necesidades de tutela jurídica.

Así puntualizan y nos refrescan la idea que, si el Derecho penal está llamado a intervenir, no es menos cierto que de forma paralela habrán de adoptarse otros bloques de medidas y regulaciones jurídicas en el ámbito del Derecho Administrativo, Internacional y del Derecho Procesal o revisar, en su caso, la eficiencia de las ya existentes -tareas que probablemente revisten todavía mayor complejidad-, como garantía para conseguir una intervención racional de aquél. De lo contrario, las posibilidades de éxito serán dudosas.

En este sentido, la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible. Para ello no puede desconocerse que los sistemas informáticos pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal

⁴ PICOTTI, L., “Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati”. En: *Enciclopedia Giuridica Treccani*. Volumen XXVI, 1999, p. 324.

desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas, etc.

Si a ello se agrega que en la actualidad existen cada vez más bancos de datos, empresas o entidades dedicadas a proporcionar cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares, no se hace difícil comprender que con ello se ponen en juego derechos individuales y colectivos y por tanto los consiguientes bienes jurídicos que el ordenamiento jurídico institucional debe proteger.

No es la amenaza potencial de la computadora sobre los individuos lo que provoca el peligro, sino la utilización real por los hombres de los sistemas de información con fines de espionaje. Así como no son los grandes sistemas de información los que afectan la vida privada, sino la manipulación o el consentimiento por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no está frente al peligro de la informática, sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

También se debe admitir que la protección de los sistemas informáticos puede abordarse no solo desde una perspectiva penal, sino con una visión civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen por qué ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas.

Por eso, dadas las características de esta problemática, sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar la eficaz defensa de los ataques a los sistemas informáticos y determinada seguridad jurídica en sus impactos, tanto para evitarlos como para perseguirlos y reprimir, a los fines propios del Derecho, frente a tales comportamientos.

Para puntualizar aspectos importantes que definen y determinan a este tipo de comportamiento se hace necesario esbozar que el elemento descriptivo de esta clase de delitos lo sería la computadora, las bases de datos o registros informáticos o bien los bienes materiales e inmateriales afectados a través de un sistema informático u ordenador, para citar algunos.

De cara al elemento normativo nos dice ZAFFARONI⁵ que aparecen cuando los tipos acuden a valoraciones jurídicas o éticas. Normalmente el tipo se vale de descripciones para individualizar programas, pero en ocasiones lo hace mediante estas remisiones a elementos de carácter valorativo.

⁵ ZAFFARONI, E. R., Comentarios al Derecho Penal. Parte General. Ediar. Buenos Aires. Argentina, 2000, p. 33.

Debe entenderse entonces que dicho elemento se aprecia intelectualmente y, en el caso en particular de los delitos informáticos, es necesario auxiliarse de la informática u otra ciencia para comprenderlos. En ese sentido dentro de los elementos normativos de este tipo de ilícitos tenemos los daños producidos a los equipos, a los programas o bases de datos, la pérdida patrimonial, la indemnidad sexual, etc.

En cualquiera de su redacción o formulación legal se constituye una modalidad propia de ilicitud informática porque el tipo legal ha de describir una conducta que sólo puede verificarse en relación con un sistema de tratamiento automatizado de datos o una representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático, los que aparecen como objeto del delito.

En una lectura de su conformación genérica es un delito de acción, de resultado instantáneo⁶. La conducta típica ha de consistir en acceder a un sistema o dato informático de acceso restringido, es decir, entrar al sistema o conocer el dato. Debido a ser un tipo penal de resultado, el acceso puede lograrse “por cualquier medio”, sea éste remoto –utilizando el sujeto activo las redes públicas de telefonía o transmisión de datos– o directo –sentándose el autor frente a una computadora e ingresando a ella tomando conocimiento de su contenido, leyendo el “dato” que está en la pantalla, o copiando archivos o software para acceder después a su contenido.

El tipo normativo ha de formularse de tal suerte que permite advertir, por sus características, la existencia de un elemento normativo jurídico expresivo de un eventual tipo de justificación genérica concurrente, pues, a diferencia de los tipos penales comunes, aquí el precepto penal reconoce y anuncia que la posible concurrencia de una causa de justificación genérica (prohibición, mandato o permiso fuerte), excluyente del tipo prohibitivo o preceptivo, no es excepcional. Es que el acceso debe darse sin la debida autorización o excediendo la que posea el sujeto activo.

La configuración del injusto en casi todas las legislaciones que reconocen el delito informático está sometida a un régimen de subsidiariedad expresa y relativa⁷; se aplica si no resultare un delito más severamente penado. Esta hipótesis se da cuando el comportamiento en sede informática pueda ser elemento integrante del tipo de otra figura o cuando el mismo hecho constituye el *corpus* del delito más grave. No se produce el desplazamiento si el otro delito tiene una pena inferior al del acceso ilegítimo a un sistema informático. Si éste, por fin, es un hecho distinto del otro delito, los dos hechos operan en concurso real.

Para una mejor comprensión de la existencia del delito informático, procede adentrarse en algunos parámetros importantes para discurrir en el análisis de la posible

⁶ PALAZZI, P., Los Delitos Informáticos en el Código Penal. 2a ed., Abeledo Perrot. Buenos Aires. 2012, p. 42.

⁷ SILVA SÁNCHEZ, J. M., La expansión del Derecho penal –Aspectos de la política criminal en las sociedades postindustriales-. 1ª edición, reimpresión. Madrid, 2006, p. 54.

tificación penal de los comportamientos contra los bienes informáticos, a los fines de su tratamiento expreso en los ordenamientos penales.

Para justificar la existencia del denominado delito informático se hace necesario adentrarse en algunas de las instituciones propias del Derecho Penal General que han de valorarse al momento de cualquier acción legislativa en el ámbito de cualquier tipo penal. Desde esta perspectiva el punto que más se repite en los estudios realizados es si se trata de una nueva categoría de delitos -para algunos es una realidad que hasta ha sido elevada a la categoría de “delito del futuro” - o si se trata solamente de nuevas formas de comisión de las tradicionales figuras delictivas y que -a lo sumo- configuran una nueva modalidad criminológica⁸.

2.1. La información como bien jurídico tutelado

Cualquier acción capaz de provocar una pérdida o daño en la confidencialidad, integridad o disponibilidad de los datos contenidos en soporte informático, constituye una amenaza de la seguridad de la información y, en esa medida, una conducta idónea para generar riesgo sobre el mantenimiento y seguridad de los sistemas informáticos y, por tanto, una conducta con capacidad de afectación del objeto jurídico protegido⁹.

Estas acciones pueden resumirse en comportamientos que atenten contra una de dichas características o contra varias de ellas. Así, suponen una amenaza de la confidencialidad de la información las conductas de accesos incontinentos a la información o de reproducción de esta. Entre las que suponen un riesgo sobre la integridad de los datos, se hallan la introducción de alguno de esos datos, la alteración, la ocultación, la supresión o borrado. Por último, atentan contra la disponibilidad de la información y la inutilización de esta, mediante su encriptación o mediante la inserción de alguna subrutina o bomba lógica de actuación retardada.

La tendencia y proyección mayoritaria es que la protección de estos comportamientos se haga desde la perspectiva de los delitos tradicionales, con una reinterpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto, sin duda, da como regla general que los bienes jurídicos protegidos serán los mismos que los delitos reinterpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

Otra vertiente doctrinaria supone que la emergente sociedad de la información hace totalmente necesaria la incorporación de valores inmateriales y de la información

⁸ MONTANO, P., “Las falsificaciones electrónicas”. En: *Revista del INUDEF*, Montevideo, 1988, Disponible: <http://revistaderecho.um.edu.uy/wp-content/uploads/2012/10/DERECHO-20.pdf>. Fecha de consulta: 12 de enero de 2020.

⁹ RIBAGORDA GARNACHO, A., “Seguridad de las tecnologías de la información”. En: **Ámbito jurídico de las tecnologías de la información**. Cuaderno de Derecho judicial, 1996, p. 33; COLOBRÁN HUGUET, M., Introducción a la seguridad informática. Planeta UOC, Barcelona, 2004, p. 46.

misma como bien jurídico de protección, tomando en cuenta las diferencias existentes, por ejemplo, entre la propiedad tangible e intangible, ya que la información no puede ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales que tienen un valor económico intrínseco; la información y otros bienes intangibles también son objetos de propiedad, lo cual goza de protección constitucional¹⁰.

En estos casos, los incidentes implican comportamientos dirigidos a ocasionar perturbaciones sobre los sistemas de información. Estos ataques persiguen sobrecargar o saturar, por medio de artificios informáticos (por ejemplo, creando redes de sistemas esclavos), algunos de los recursos limitados del sistema objeto del ataque hasta hacerlo inoperativo, logrando con ello el bloqueo o interrupción temporal de dicho servicio.

Precisamente, según el informe elaborado por *Recovery Labs*, empresa especializada en recuperación de datos, borrado seguro y peritaje informático, más del 60% de los casos para los que se solicita el servicio de peritaje informático están relacionados con sabotaje¹¹. Sentado lo anterior, debe hacerse hincapié en la importancia que revisten para la sociedad, como destinatario principal de la información contenida en soporte digital, los sistemas informáticos, como infraestructura imprescindible desde la que prestar servicios y operar con datos.

Cualquier acción idónea para dañar u obstaculizar gravemente el funcionamiento de los sistemas conlleva, también, riesgos para la seguridad de la información. Extremo este que impone la necesidad de ofrecer tutela penológica a su protección ante el ataque de conductas intencionadas y por qué no, imprudentes en algunos casos, que ocasionan lesiones irreparables, por las consecuencias que genera, los impactos criminales sobre los sistemas informáticos; siempre en estrecha relación con la importancia y aportación al bien jurídico máspreciado que es la sociedad, por su especial carácter global.

La protección de la información como bien jurídico tutelado debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la penalización de conductas se desenvuelve en el marco del principio de “dañosidad” o “lesividad”. Así, una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada.

El bien jurídico protegido en general es la información, pero considerada en diferentes formas, ya sea como un valor económico o como un valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales.

De esta forma, para un sector doctrinal, el delito informático es sólo la comisión de delitos mediante el uso de los computadores, pues considera que en realidad no existe un bien jurídico protegido en el delito informático, porque no existe como tal dicha

¹⁰ PALAZZI, P., Ob. Cit., p. 45.

¹¹ **Más del 60% de casos de peritaje informático se deben a sabotaje en las empresas, según *Recovery Labs*.** Disponible: <http://www.recoverylabs.com>. Fecha de consulta: 12 de enero de 2020.

conducta. Esto no es más que una nueva forma de ejecución de conductas que afecta bienes jurídicos que ya gozan de protección por el Derecho penal¹². De otro lado, coexisten los que sostienen que estos delitos tienen un contenido propio, afectando así un nuevo bien jurídico¹³.

Entre las primeras definiciones de “delito informático” que se han ido aportando por la doctrina, se encuentra la de BEQUAI¹⁴, quien sostiene que en la definición del mismo el acento debe ponerse en que los ordenadores pueden ser usados por el autor del delito no sólo como instrumentos para cometer el mismo, sino también como objeto del delito; la ofrecida por PARKER¹⁵, que definió los abusos informáticos como “cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio.

Tratando de superar las definiciones hasta entonces ofrecidas, ROMERO CASABONA¹⁶, considera importante la necesidad de hablar de pluralidad de delitos informáticos, donde su nota común es la vinculación a los ordenadores. Sostiene que no tienen un bien jurídico común ni una forma de comisión común: por un lado, aparece como el instrumento del delito, de naturaleza informática; y por otro, esta es el objeto de la conducta delictiva, por ello el autor se inclina por conceptualizar estos comportamientos –para el orden legal normativo– como “delincuencia informática” y para quien carece de relevancia jurídica si el ordenador es el objeto sobre el que recae la conducta o el medio de cometerla.

No ha resultado fácil concretar un único concepto de delito informático; por ello, en la actualidad se niega por algunos¹⁷ la existencia de este concepto y, con ello, de esta tipología delictiva, prefiriendo utilizar para abarcar todo este conjunto de comporta-

¹² CALLEGARI, L., “Delitos Informáticos y Legislación”. En: *Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana*. Medellín, Colombia, N° 70 julio-agosto-septiembre, 1985, p. 35; DE LA CUADRA, E., “Regulación Jurídica de la Informática Computacional”. En: *Temas De Derecho*. Año II N° 3, 1987. Universidad Gabriela Mistral. Santiago de Chile, 1987, p. 76; TONIATTI, R., “Libertad Informática y Derecho a la Protección de los datos personales: Principios de Legislación Comparada”. En: *Revista Vasca de Administración Pública*. No. 29, enero-abril, 1991, España. 1991, p. 45; TIEDEMANN, K., Poder económico y delito. Introducción al Derecho penal económico y de la empresa. Ariel, Barcelona, 1985, p. 55.

¹³ GONZÁLEZ RUS, J. J., “Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos”. En: *Revista de la Facultad de Derecho de la Universidad Complutense*. Madrid, 2006. p. 32; ROMERO CASABONA, C. M., De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal. Granada, 2006.

¹⁴ BEQUAI, A., *Computer Crime*. Lexington, MA: Lexington Brooks Massachusetts, 1978, p. 3.

¹⁵ VELÁZQUEZ PARKER, R., *Crime by computer*. New York, 1989, p. 12.

¹⁶ ROMERO CASABONA, C. M., Ob. Cit., p. 42.

¹⁷ MORANT VIDAL, J., Protección penal de la intimidad frente a las nuevas tecnologías, Tirant Lo Blanch, Valencia, 2013, p. 42; ORTS BERENGUER, E., ROIG TORRES, M., Delitos informáticos y delitos comunes cometidos a través de la informática, Tirant Lo Blanch, Valencia, 2008, p. 13; ÁLVAREZ VIZCAYA, M., “Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la Red”. En: *Cuadernos del Poder Judicial*, N° 10, Marcial Pons, Madrid, 2001, p. 257.

mientos que tienen que ver con la informática, de uno u otro modo, expresiones como “Delincuencia informática”, “Criminalidad informática” o, “Delitos informáticos, que incluiría en dichos conceptos todos los comportamientos en los que un sistema informático sea el medio para lesionar un bien jurídico, cualquiera, y todos aquéllos en que dicho sistema sea él mismo el propio objeto sobre el que recae la acción delictiva.

No quedan fuera de esta línea de pensamiento, los que se ubican en una tercera posición y alegan que los delitos informáticos han de ser observados y consecuentemente analizados desde una triple visión: como fin en sí mismo, como medio y como objeto de prueba¹⁸.

Otros, como CHOCLÁN MONTALVO¹⁹, definen la “criminalidad informática” como el conjunto de actos antijurídicos según la ley penal vigente, realizados con el empleo de un equipo automático de procesamiento de datos; acepta la heterogeneidad de estas conductas, deja fuera del grupo aquéllas en las que los sistemas informáticos, o la información en ellos contenida, es el objeto sobre el que recae la conducta delictiva.

Existen otros, para los cuales tampoco es necesario que exista un Título en el Código penal sobre los delitos informáticos, encontrándose las distintas conductas vinculadas de una u otra manera con los sistemas informáticos, ya sea por el medio de comisión, ya por el objeto del delito ya incluso por ambos aspectos, dispersas en diferentes títulos del código, en una ubicación en que lo que prima es el bien jurídico afectado²⁰.

En cualquiera de estas corrientes se advierte la posición del legislador en un ambiente de coexistencia pacífica, por la conservación de las buenas relaciones sociales, desde lo micro hasta lo macro mundo y que se sitúan en determinado momento histórico social.

Desde esta perspectiva conceptual el bien jurídico en esencia no desaparece, solo cambia en cuanto al ámbito de protección que lo sujeta. El desarrollo de esta institución jurídica pasa por momentos totalmente distintos ya que los mismos son productos de las necesidades propias del desarrollo de la sociedad y los distintos cambios sometidos a ella, en lo que hay que tener en cuenta que estos no se originan al crear una norma, sino que su existir es previo a la misma.

Lo expuesto significa que, en un primer momento, la protección de un bien de suma importancia para el conjunto social, ya por la selección de estas necesidades

¹⁸ BAÓN RAMÍREZ, R., “Visión general de la informática en el nuevo Código Penal”. En *Cuadernos del Poder Judicial Español*, N° 11. Marcial Pons, Madrid, 1996, p. 77. MONTERDE FERRER, F., “Especial consideración de los atentados por medios informáticos contra la intimidad y privacidad”. En: *Cuadernos del Derecho judicial*, Dialnet, 2011, p. 196; PÉREZ LUÑO, A. E., *Manual de informática y Derecho*. Atelier Libros. Barcelona, p. 75.

¹⁹ CHOCLÁN MONTALVO, J. A., *Infracciones patrimoniales en los procesos de transferencia de datos*, Granadas, 1996, p. 69.

²⁰ MATA y MARTÍN, R. M., *Delincuencia informática y Derecho Penal*. Madrid, 2001, p. 21; GONZÁLEZ DE CHAVES CALAMITA, M., “El llamado delito informático”. En: *Anales de la Facultad de Derecho*. Universidad de Barcelona, 2014, p. 45.

valoradas socialmente y después positivarlas en norma de carácter constitucional o de índole especial e incluso, de orden internacional, será un segundo paso en el ámbito de su construcción jurídica, para una vez terminada la nueva categoría de bienes a protegerse, determinar cuáles son verdaderamente materia de protección penal.

Los bienes jurídicos, en su conformación jurídico penal se justifican como categoría límite al poder punitivo del Estado y se levantan como obstáculo capaz de impedir arbitrariedades, distorsiones o confusiones en la elaboración de la estructura penal; las funciones de garantía son inherentes al bien jurídico penal y se vincula a la relación individuo Estado. Bajo el mecanismo de garantía resulta posible denunciar todos los elementos que amenacen o avasallen a la persona en su relación con el Estado.

Cuestión bien importante en esta lectura sobre bienes jurídicos lo es la función de interpretación de la norma penal, lo que –en todo caso- conducirá siempre al bien jurídico, en cuya sede se pueden establecer criterios esclarecedores o correctivos de los alcances de la protección a fin de evitar distorsiones en la comprensión del contenido de los bienes jurídicos en concreto. Tema bien interesante y complejo y que no se profundizará en este estudio, para no desviar el curso del objeto de investigación.

2.2.Posibles bienes jurídicos generales que exigen tutela

No obstante las discrepancias doctrinales ya comentadas en torno a la construcción teórica misma de un concepto de delito informático y las consideraciones de cómo debería ser ello tratado en el ámbito normativo a los fines de su mejor y más completo encuadre de las conductas que en dicho ámbito puedan suscitarse, cada vez son más las voces que sostienen la necesidad de creación de una nueva categoría jurídico penal que abarque las conductas vinculadas con el comportamiento informático, entendiéndose que se trata sólo –o no en absoluto– de la lesión de bienes jurídicos tradicionales, sino ante la lesión de un nuevo interés que merece ser objeto de atención también por el Derecho penal.

Tal idea, extendida cada vez más, no conlleva, sin embargo, a una unidad de criterio a la hora de entender cómo debe explicarse este interés y cómo debe definirse el bien jurídico penal a que pretende hacerse referencia. En este derrotero encontramos el tratamiento genérico del bien jurídico informático, visto desde posiciones necesitadas de protección o tutela penal, que encierran –conceptualmente- las categorías de bienes jurídicos que apuntan a dicha tutela²¹.

2.2.1. Seguridad informática

El vocablo seguridad sugiere, proteger que pertenecen a un legítimo propietario, de los posibles peligros y ataques ejecutados por terceros extraños no autorizados, que presentan determinado significado o valor; mientras que la seguridad informática se

²¹ ROMERO CASABONA, C. M., Ob. Cit., p. 1.

asegura de proteger los sistemas informáticos, que como un todo se integran por información, servicios, equipamiento y redes.

El objetivo de la seguridad informática es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información que contiene el sistema informático, entendido como el conjunto de elementos hardware, software, datos y personas que permiten el almacenamiento, procesamiento y transmisión de información, siendo vulnerables todos los elementos que lo integran.

Sobre la base de la vulnerabilidad antes expuesta, se han desarrollado estándares o criterios de seguridad, entre los que se destacan el secreto o confidencialidad, la integridad, la accesibilidad o disponibilidad, la autenticidad²².

El secreto o confidencialidad exige que la información debe estar disponible solamente para aquellos usuarios autorizados; la integridad por su parte requiere que la información no se pueda falsear, es decir, que los datos recibidos o recuperados sean los auténticos, los mismos que fueron enviados o almacenados; y la accesibilidad o disponibilidad, debe precisar quién y cuándo puede acceder a la información.

La autenticidad, asegura el origen y el destino de la información y el no repudio significa que la entidad que envía o recibe datos no puede alegar desconocer el hecho. Estos dos últimos criterios revelan determinada importancia en el entorno bancario y de comercio electrónico.

Otros criterios de seguridad en un sistema informático se identifican con la consistencia, el aislamiento, la auditoría, la prevención y la información²³. La consistencia demanda asegurar que el sistema se comporta como se supone que debe hacerlo con los usuarios autorizados.

El aislamiento exige que en sistema impida que personas no autorizadas entren en él; por su parte, la auditoría refiere sobre la capacidad del sistema de determinar qué acciones o procesos se han ejecutado y quién y cuándo las han realizado, mientras que la prevención como criterio de seguridad informático, hace alusión a que los usuarios deben saber que sus actividades quedan registrada en el sistema por un periodo de tiempo que permite la verificación en un momento posterior y el criterio de información viene determinado por la posibilidad que ofrezca el sistema de detectar comportamientos sospechosos y alertar a las posibles víctimas.

Como posible bien jurídico colectivo a tutelar, objeto de ataques vinculadas a la cuestión informática, se erige la seguridad informática. Su protección evita la lesión de bienes jurídicos de carácter individual puestos en peligro y aquellas conductas atentato-

²² ALONSO ROMERO, L., Seguridad Informática. Conceptos generales. Disponible: campus.usal.es/-derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf. Fecha de consulta: 24 de mayo de 2017, p. 3. RIBAGORDA, A., o. et. al., Seguridad y protección de la Información. Centro de Estudios Ramón Areces, 1994, p. 12.

²³ ALONSO ROMERO, L., Ob. Cit, p. 4.

rias a la seguridad de las redes y sistemas informáticos, pero no siempre efectivamente dañados²⁴.

La concepción misma de un bien jurídico de naturaleza colectiva, indisponible, como tal, por el individuo concreto, que no encuentra suficiente protección mediante la salvaguarda en exclusiva de bienes jurídicos de naturaleza individual, pues muchas veces, al margen de otras consideraciones, no existirá la voluntad lesiva de dañarlos de manera efectiva, lo que no impide que pueda entenderse idóneo un adelantamiento de las barreras de protección a la de meras situaciones de peligro para lo cual esta perspectiva puede ser eficaz.

2.2.2. Integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos

En la década de los setenta del pasado siglo, cuando los países más avanzados tecnológicamente comienzan a preocuparse por el impacto que sobre la intimidad presentan las tecnologías de la información se aprueban las primeras leyes que tienen como objeto la tutela del derecho a la autodeterminación informativa o *habeas data*, reconocido en el artículo 12 de la Declaración Universal de los Derechos Humanos de 1948.

La protección de datos personales intenta amparar el derecho de los individuos a determinar cuándo, cómo, a quién, qué y para qué información sobre ellos puede ser cedida a terceros, o como dice el Tribunal Constitucional Español, *“el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado”*²⁵.

La integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos, tiene como punto de partida la consideración de la informatización de todos los datos, tanto de carácter público como privado, y la necesidad de poder confiar en su autenticidad y en su disponibilidad plena como garantía para un desarrollo económico y social acorde a los tiempos actuales²⁶.

Así se constituye en tutela de la incolumidad de los datos, de su libre disposición y de su mantenimiento en los términos en que los ha configurado su titular, bien jurídico también de carácter supraindividual que adelanta la intervención penal en cuanto al mismo tiempo es instrumental respecto de otros bienes jurídicos que pueden verse da-

²⁴ DEL MAR CARRASCO ANDRINO, M., El acceso ilícito a un sistema informático. Tirant Lo Blanch. Valencia, 2009, p. 342.

²⁵ Sentencia del Tribunal Constitucional español, número 292 del año 2000\292, citada por RIBAGORDA GARNACHO, A., La protección de datos personales y la seguridad de la información. Disponible: www.jcyl.es/web/jcyl/binarios/528/955/08-ribagorda.pdf?blobheader.../pdf. Fecha de consulta: 14 de enero de 2020, p. 5.

²⁶ RODRÍGUEZ MORULLO, G., Derecho Penal e Internet. Madrid, 2001, p. 259.

ñados o en peligro con el menoscabo de la accesibilidad, integridad o confidencialidad de determinados datos.

2.2.3. Intimidación informática

Respecto a la consagración normativa del derecho a la intimidad en el plano internacional, el primer antecedente que se tiene de reconocimiento expreso data del año 1948, cuando en el artículo 12 de la Declaración Universal de Derechos Humanos se estableció: *Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*

El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966 en relación con el derecho a la intimidad estableció: 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

El derecho a la intimidad se ha asumido además de manera consecuente con la normativa internacional en los textos constitucionales modernos, lo que implica el reconocimiento de derechos inalienables en el ser humano; derechos que tiene toda persona por el sólo hecho de gozar de la condición de humano y por ello, toda persona se hace titular de ciertos bienes jurídicos, pero no por el otorgamiento del Estado sino en virtud de un título que emana de la juridicidad natural del hombre²⁷.

De esta manera se consagraron los derechos fundamentales, derechos que por provenir directa e inmediatamente de la condición humana, por integrar el núcleo jurídico primario de toda persona en cualquier época y en cualquier lugar, constituyen el fundamento de la comunidad política por servirle de principio y de razón primordial²⁸, y esto implica armonizar en términos de convivencia civilizada, la libertad y el orden; entendiéndose que en un Estado Social de Derecho el anhelo de la paz sólo es legítimo alcanzarlo con el respeto a la dignidad humana.

La dificultad de aproximarse al tema del derecho a la intimidad es reconocida por diversos autores²⁹, debida no sólo a que se trata de un derecho relativamente nuevo, sino también a que nos encontramos ante algo que desde su origen ha estado influido

²⁷ MADRID-MALO GARIZÁBAL, M., *Derechos fundamentales*. Editor Ltda. Santa fe de Bogotá. 1997, p. 8.

²⁸ Ídem, p. 20.

²⁹ MARTÍNEZ DE PISÓN CAVERO, J., “La configuración constitucional del derecho a la intimidad”. En: *Derechos y Libertades. Revista del Instituto Bartolomé de Las Casas*. Madrid, año II, N° 3, mayo-diciembre 1994, p. 323. Disponible: file:///dspace/bitstream/10016/1493/4/DL-1994-II-3-Pison.pdf; Fecha de consulta: 23 de enero de 2020. SUÁREZ, E. M., “Estado de la cuestión sobre el derecho a la intimidad”. En: *Dikaion. Revista de la Facultad de Derecho de la Universidad de La Sabana*. Chía, Volumen 3, 1994, p. 64.

fuertemente por los distintos cambios sociales y culturales, experimentando diversas transformaciones³⁰.

A partir de la década de los 70 debido al avance de las nuevas tecnologías de la información, en especial de las bases de datos computarizadas y los sistemas de vigilancia, se empieza a plantear una nueva defensa de lo privado en relación con lo público, hablándose de la necesidad de expansión del núcleo del derecho fundamental a la intimidad para hacer frente a los nuevos retos que podrían significar, incluso, la pérdida de la vida privada³¹.

El concepto de intimidad es asumido por la mayoría de la doctrina como sinónimo de privacidad o de vida privada³², que abarca los diversos actos, situaciones y circunstancias que por su carácter personalísimo no deben, salvo el consentimiento de la persona afectada o por razones legítimas, estar expuestos a la curiosidad y a la divulgación, sino salvaguardados de la injerencia extraña, al ser uno de los valores que en toda sociedad democrática debe tener el hombre para ser el auténtico dueño de su núcleo jurídico personalísimo³³.

Asimismo, se reconoce que la intimidad como noción es algo básicamente subjetivo, unido a una esfera interior de la vida del hombre y del grupo humano fundamental del cual haga parte, y estrechamente vinculado al hogar, domicilio o espacio físico reservado, que debe ser respetado tanto por las demás personas como por el Estado, debido a que las manifestaciones del ser humano en este ámbito están excluidas del conocimiento público y de cualquier intromisión ajena, salvo el consentimiento de su titular³⁴.

Como derecho, se le ha definido en el sistema anglosajón o del *Common Law*, donde el término empleado es *privacy*, se le vincula con la idea de libertad del individuo, en el sentido de que hay una esfera de acción que no le afecta más que a él mismo y en el que la sociedad no tiene más que un interés indirecto; es decir, se considera que sin un espacio íntimo aislado de la injerencia de la sociedad no hay libertades públicas, y asimismo se configura como un derecho a estar solo, a que a uno lo dejen en paz,

³⁰ SUÁREZ, E. M., Ob. Cit., p. 67. MÁRQUEZ ESCOBAR, Pablo. *El ojo ve, el poder mira: la arquitectura para la vigilancia y el fin de la privacidad*. Pontificia Universidad Javeriana, Bogotá, 2004, p. 64.

³¹ MÁRQUEZ ESCOBAR, P., Ob. Cit., p. 80; SUÁREZ, E. M., Ob. Cit., p.48.

³² No obstante, algunos diferencian estos conceptos dándole un mayor ámbito a la vida privada, distinguiendo varios niveles de intimidad dentro de la privacidad, la cual definen como el retiro temporal de un sujeto que se separa de la sociedad voluntariamente a través de todo tipo de medios psicológicos o físicos y la intimidad como aquella fase de la privacidad en la que el sujeto se encuentra situado en un grupo reducido en el que caben una serie de relaciones como las derivadas de la esfera familiar o conyugal. Cfr. VICENTE Y GUERRERO, G., “El derecho a la privacidad frente al uso justificado de los sistemas de vigilancia”. En: *Derechos y Libertades. Revista del Instituto Bartolomé de las Casas*. Madrid, año III, Nº6, febrero 1998. p. 520.

³³ MADRID-MALO GARIZÁBAL, M., Ob. Cit., p. 200.

³⁴ MOLINA ARRUBLA, C. M., *El secreto en el derecho penal colombiano*. Santa Fe de Bogotá, Editorial Leyer, 1997, p. 120.

mediante el cual el individuo tiene la garantía de protección de su persona frente a cualquier invasión del recinto de su vida privada y doméstica³⁵.

En cuanto al sistema romano-germánico, se suelen distinguir diversos grados de intimidad, como en la doctrina alemana, donde se habla de tres esferas: *Intimphäre* o ámbito de lo secreto de hechos que deben permanecer ignorados e incomunicados para los demás; *Privatsphäre* o ámbito de la vida personal y familiar que se quiere mantener protegido frente a la injerencia o publicidad ajena; e *Individulphäre* o ámbito que atañe a la peculiaridad o individualidad de la persona, como el honor, el nombre o la imagen³⁶.

El derecho a la intimidad normalmente aparece vinculado con la dignidad y la libertad, como bienes que son personalísimos, caracterizado por una esfera privada exenta de intromisiones extrañas sin justa causa, bien sea de particulares o del Estado, en la cual cada uno puede gozar de su soledad o de la tranquilidad en familia.

Aunque el núcleo esencial del derecho fundamental a la intimidad podría definirse como el espacio intangible, inmune a intromisiones externas, del que se deduce un derecho a no ser forzado a escuchar o ver lo que no se desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto³⁷, junto a la tutela de situaciones concretas de la vida humana objetivables, del espacio físico en el que se desarrolla y las relaciones personales que propicia, debido a que la proyección social de la persona conlleva que el núcleo de su intimidad no se contraiga a la dimensión personal, sino que se extienda a la dimensión social más inmediata, como la familiar, la laboral, la económica³⁸.

En los últimos años, a causa de las tecnologías de la información y las comunicaciones y también respecto a los sistemas de vigilancia, se entiende que la intimidad también incorpora y comprende las facultades de control y disposición de la información que afectan al individuo³⁹.

La intimidad informática se plantea como bien jurídico autónomo y diferenciado, de naturaleza estrictamente informática, merecedora y necesitada de protección penal específica. Su contenido central vendría dado por el derecho del individuo a decidir qué información personal se puede difundir sobre él y su familia y cuál pueda ser el destino de esta difusión. Pero, en realidad, se está ante un derecho complementario del que tradicionalmente trata de garantizar la tutela de la intimidad en su sentido más amplio, simplemente vinculado al desarrollo concreto de la informática.

³⁵ SUÁREZ, E. M., *Ob. Cit.*, p. 71.

³⁶ Ídem, p.70.

³⁷ MOLINA ARRUBLA, C. M., *Ob. Cit.*, p. 120.

³⁸ SUBIJANA ZUNZUNEGUI, I. J., "Policía judicial y derecho a la intimidad en el seno de la investigación criminal". En: *Cuaderno del Instituto Vasco de Criminología*. Nº 10, extraordinario, octubre 1997, San Sebastián, p. 124.

³⁹ MARTÍNEZ MARTÍNEZ, R., *Ob. Cit.*, p. 68.

Siguiendo esta posición respecto a este valioso bien jurídico, no se trata sólo de reconocer el derecho de excluir a los demás de un determinado ámbito que el titular considera reservado y que ha de protegerse frente a intromisiones indeseadas, sino de un poder positivo de control sobre la información personal que los demás pueden tener de cada uno y sobre el uso que puedan hacer de la misma. Ello se entiende así, por estimarse que no queda protegido por los tradicionales bienes jurídicos en su diversidad de construcción normativa, tanto de índole individual como de bienes materiales⁴⁰.

La vulneración de estos bienes jurídicos no solo tiene alcance individual y concreto de sus titulares, sino que su comisión también pone en peligro la confianza de la sociedad en el buen funcionamiento de los sistemas informáticos y de las redes de transmisión de datos.

3. Posibles bienes jurídicos particulares que exigen tutela

La dinámica de la previsión legal de los delitos informáticos no solo debe abarcar bienes jurídicos generales, sino también conductas tradicionales que se ejecutan hoy a través de la informática y requieren de su especial protección, como los derechos de propiedad intelectual y la indemnidad sexual.

3.1. Propiedad intelectual

La propiedad intelectual es entendida como toda creación que genera el ser humano como resultado de su intelecto y le proporciona derechos exclusivos de protección sobre la creación misma.

Por medio de los derechos de propiedad intelectual se protegen tanto las obras de derecho de autor, como aquellas provenientes de la propiedad industrial; cuando se habla de derechos de autor, se hace referencia a la protección que gozan todas las producciones en el campo literario, científico y artístico, cualquiera que sea el modo o forma de expresión, (libros, conferencias, obras dramáticas o dramático-musicales; obras coreográficas y pantomimas; las composiciones musicales con o sin letra; las obras de dibujo, pintura, arquitectura, escultura, grabado, obras de artes aplicadas), muchas de las cuales tienen hoy una formulación virtual en la Internet.

Los derechos de propiedad industrial, genera la protección a la búsqueda de soluciones concretas de problemas específicos en el campo de la industria y del comercio, o a la selección de medios diferenciadores de establecimientos, mercancías y servicios, (las invenciones, las marcas y otros signos distintivos, dibujos y modelos industriales, nuevas variedades vegetales, circuitos integrados, etc.), las que de igual modo presentan en la actualidad su visualización en la Internet.

⁴⁰ Ídem.

En la actualidad en virtud de los derechos que genera la propiedad intelectual, se incluyen determinadas acciones vinculadas al uso de las tecnologías de la información y las comunicaciones como distribución y copia ilegales de música, películas, obras de arte, fotos, guiones, así como de programas informáticos, marcas, patentes, etc., todo lo que causa pérdidas de millones de dólares en ingresos a los titulares de los derechos reconocidos.

3.2. La indemnidad sexual

Una de las acciones ilegales vinculadas al Internet que más repudio origina en la actualidad resulta el estado de indefensión que presentan y al cual se ven expuestos a diario los menores de edad, víctimas de actos de pornografía infantil, acoso sexual, etc., lo cual atenta directamente contra el desarrollo de la personalidad de niñas y niños y en tanto requiere de especial protección.

En este punto se muestra recurrente la posición de ROXIN⁴¹, respecto a que las meras inmoralidades no lesionan bienes jurídicos, el que a su vez precisa que la difusión de pornografía, si bien son estimadas inmoralidades cuando este ocurre entre personas adultas conscientemente, no menoscaban derechos individuales ni bienes *“en el sentido de estados vulnerables, protegibles y valiosos. En ellas falta una “real causalidad lesiva”*⁴² y en tanto no lesiona bienes jurídicos, solo deben entenderse como infracciones de conceptos generales como la moral. Criterio que no puede asumirse en el caso de los menores víctimas, por carecer de la capacidad de entendimiento y responsabilidad de sus actos, los que gozan de la protección de su indemnidad, en este caso sexual.

Para la protección de la indemnidad sexual, se debe partir de que la naturaleza del bien jurídico tutelado determina que la posibilidad de conocimiento de las imágenes por parte del público –publicidad- no constituya un presupuesto esencial de esta modalidad delictiva. Aquí no se protege el pudor público, sino el derecho de los menores de edad a un desarrollo de la sexualidad progresivo y libre de injerencias indebidas.

4. Conclusiones

Conforme al Derecho penal, el riesgo de los comportamientos dañosos vinculados al delito informático lo está en los niveles de dependencia de la sociedad de las nuevas tecnologías para el diario quehacer y desarrollo de sus actividades sociales, económicas y personal y los avances de las nuevas tecnologías de la información traen aparejado un cambio en la respuesta punitiva y, desafortunadamente, no necesariamente para bien,

⁴¹ ROXIN C., Ob. Cit., p. 52

⁴² Ídem.

pues los tipos penales se van tornando cada vez más de peligro abstracto y, por ende, no se sabe bien qué es lo que se ataca, ni cómo, ni cuánto.

El grado de tutela al bien jurídico no está claro, como tampoco la exigibilidad de otra conducta. En muchos casos de las afectaciones a bienes jurídicos no son delitos, sino infracciones civiles, administrativas, laborales o comerciales, para los que el cauce procesal de exigibilidad de responsabilidad es bien distinto; pero también eficaz.

Los momentos actuales discurren aún por un proceso de desarrollo tecnológico y de desarrollo de cultura informática no consolidada, por lo que nada impide y –contrario- aconseja, acudir para su tutela legal a otros mecanismos de protección –incluso penales- menos severos, como el de las medidas de prevención. La técnica más conveniente para dar respuesta penal a las necesidades de tutela surgidas del desarrollo de la informática, internet y las redes de transmisión de datos, dado su específico desarrollo, resultan la de incorporar un nuevo bien jurídico bajo el rubro del legal uso de las tecnologías de la información y las comunicaciones.

Comoquiera que la doctrina y legislación no son pacíficas sobre el tema, así como resulta innegable los cambios imprevisibles que en dicho ámbito puede suscitarse y a diario se suscitan, es aconsejable también ante determinadas lagunas de punición, la incorporación de este nuevo bien jurídico.

Con independencia de los distintos criterios que se han seguido en torno a la figura del delito informático, y en particular sobre la existencia de un bien jurídico digno de tutela penal, una cuestión resulta medular de cara a la demostrada crisis del Derecho penal y a su expansionismo, y es lo referido a buscar formas menos invasivas de solucionar los posibles conflictos en torno al uso ilegal de la información y ofrecer mayor protagonismo al Derecho administrativo sancionador, y sobre todo, a desarrollar estrategias de prevención situacional en este sector especializado de la informática y el ciberespacio, al que por razones obvias del desarrollo humano y de las comunicaciones se accede cada día con mayor frecuencia.

Por lo relevante que resultan los comportamientos estimados delictivos vinculados al uso de las tecnologías de la información y las comunicaciones para las personas naturales, para las personas jurídicas, para los Estados y para la sociedad global en su conjunto, de conformidad con el principio de exclusiva protección de bienes jurídicos, se justifica sea objeto de tutela penal: el legal uso las tecnologías de la información y las comunicaciones a través de la creación de un bien jurídico pluriofensivo en concreto.