"*La revolución científica y técnica,... constituye tanto factor de progreso como motivo acuciante de nuevas desigualdades en la sociedad internacional. Aporta todo un arsenal de expectativas que pueden servir tanto para liberar al hombre de sus servidumbre frente a la naturaleza, como para imponerle nuevas y mucho más sofisticadas técnicas de dominación frente a sus semejantes*".

Nieves Sánz Mulas[1]

Aproximación a la criminalidad informática en Colombia

*Ricardo Posada Maya**

Resumen

El continuo avance de la era digital en nuestro medio, y el aumento progresivo de conductas peligrosas contra los intereses de los ciudadanos, hace imperativo el análisis de lo que la doctrina penal moderna ha llamado como 'delincuencia informática'. Concepto no exento de inconvenientes, que aglutina una serie de comportamientos cuya recepción jurídica apenas comienza en Colombia. Ante dicho contexto, es necesario desarrollar una aproximación a esta modalidad delictiva, no sólo con el propósito de ahondar en sus características, sino, también, para verificar la necesidad de crear una legislación especial en la materia.

Abstract

The continuous advance of the digital era in our means, and the progressive increase of dangerous behaviors against the citizen's interests, makes imperative the analysis of what the modern criminal doctrine has called as 'computer delinquency'. Concept doesn't exempt of inconvenient that agglutinates a diverse series of behaviors whose juridical reception hardly begins in Colombia. In this context, it is necessary to develop

* Profesor de Derecho penal y Constitución & Democracia de la Universidad de los Andes. Miembro del GECTI. rposada@uniandes.edu.co

1 Sánz Mulas, Nieves: La validez del sistema penal actual frente a los retos de la nueva sociedad, en: El sistema penal frente a los retos de la nueva sociedad. Coord. María Rosario Diego Díaz-Santos y Eduardo Fabián Caparrós, XV Congreso Universitario de Alumnos de Derecho penal, Madrid, Colex, 2003, pág. 11.

an approach to this criminal modality, no only with the purpose to deepen in their characteristic, but, also, to verify the necessity to create a special legislation in the matter.

KEYWORDS: Penal Law, computer delinquency, white collar crimes, computer illegal access, computer espionage, information, data, computer media, computers. Derecho penal, delincuencia informática, crímenes de cuello blanco, intrusismo informático, espionaje informático, información, datos, medios informáticos, computadoras.

1. Introducción

Es un hecho notorio que la transformación de los medios informáticos, científicos y tecnológicos durante los últimos 30 años, no sólo ha modificado las necesidades vitales de las personas, al fijarles patrones sociales e individuales de comportamiento (*computer dependency*); sino que también ha transformado de manera notable las relaciones jurídicas y sociales en nuestro medio cultural[2]. A tal punto que en la actualidad pocos sujetos se pueden sustraer de realizar actividades por medios informáticos o telemáticos: desde revisar el correo electrónico (vía *e-mail* o *Mailing list*), gestionar la información de la empresa, disfrutar de su ocio visitando '*Web pages*' y desarrollar comunicaciones por Messenger, NetMeeting o I.R.C. (*Internet Relay Chat*); hasta celebrar negocios o pagar por productos y servicios que de modo ordinario se adquirían y desenvolvían en espacios distintos a la Red[3].

2 Cfr. Consejo de Europa: Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, serie de tratados europeos Núm. 185, preámbulo, En: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm; Farjat, Gérard: Nuevas tecnologías y derecho económico, en: El Derecho y las nuevas tecnologías, Contexto económico, social y cultural. AA.VV., Separata de Revista del Derecho industrial, No. 33, Buenos aires, Depalma, 1990, pág. 530, cuando advierte que "en realidad, estamos en presencia de un proceso general de aceleración en la evolución de nuestras sociedades contemporáneas bajo la influencia de una revolución tecnológica permanente". De igual forma, Champaud, Claude: El impacto de las nuevas tecnologías en la empresa, en: El Derecho y las nuevas tecnologías. Contexto económico, social y cultural. AA.VV., separata de Revista del Derecho industrial, No. 33, Buenos aires, Depalma, 1990, pág. 815 y ss.; Gutiérrez Francés, M.a Luz: Fraude informático y estafa (Aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios informáticos), Madrid, Ministerio de Justicia, 1991, págs. 37 a 41; Nochteff, Hugo: El nuevo paradigma tecnológico y la asimetría norte-sur, en: El Derecho y las nuevas tecnologías. Contexto económico, social y cultural. AA.VV., Separata de Revista del Derecho industrial, No. 33, Buenos aires, Depalma, 1990, págs. 592 a 593; Romeo Casabona, Carlos María: Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la información, Madrid, Tudesco, 1987, pág. 19 y ss.; Silva Sánchez, Jesús María: La expansión del derecho penal. Aspectos de la política criminal en las sociedades postindustriales, 2ª ed., Madrid, Civitas, 2001, pág. 28; Tiedemann, Klaus: Criminalidad mediante computadoras, trad. de Amelia Mantilla viuda de Sandoval, en: Nuevo Foro Penal No. 30, octubre-diciembre de 1985, Bogotá, Temis, págs. 481 a 492.

3 El incremento de usuarios de la Internet en el mundo es llamativo. Según las cifras existentes en la Web, a febrero de 2005 el número de usuarios ascendió a la cifra de 817'447.147 millones de personas, es decir, el 12,74% de la población mundial (6412'067.185 ML.). Con lo cual, en los últimos cinco años, el uso de esta clase de tecnología se incrementó en un 126,4 % en el mundo. En Suramérica, el número de usuarios de Internet es de 39'102.074 (de 362'221.900 ML.) y el crecimiento fue del 173,6%. Finalmente, el número de usuarios aproximados de la Internet en Colombia asciende a 2'000.000 de personas (el 5,6% de 45'299.400 ML.) a diferencia del año 2000 en el que el número de usuarios fue de 878.000 personas. Lo que implica un uso e incremento tecnológico del 127,8 %. Consultado el 15.08.2005, en: http://www.exitoexportador.com/stats.htm. Véase, del mismo modo: http://www.itu.int/ITU-D/ict/statistics/index.html y http://www.aui.es/estadi/internacional/ internacional.htm

Desde luego, no sólo los sistemas de comunicación, investigación y finanzas han '*evolucionado*' por la facilidad técnica de acceso, procesamiento y transmisión eficaz de la 'información' o de los datos. También lo han hecho los soportes tecnológicos complementarios de los medios informáticos, desde los niveles más simples hasta los más complejos, la distribución del tiempo y la economía de mercado en el ámbito de la era globalizada[4]. Todo lo cual, condiciona las estructuras espaciales e industriales existentes, quizá en beneficio del bienestar individual y colectivo[5].

Sin embargo, como resultado del mal uso de los avances tecnológicos, informáticos y telemáticos, es evidente el incremento de la probabilidad —*estadística*— de nuevos peligros (amenazas) o de la producción de lesiones graves no enteramente controlables por las '*víctimas*', no sólo frente a la información como derecho y función pública[6], sino, también, frente al desarrollo adecuado de los sectores sociales e industriales más importantes (Vg. *el trasporte, la medicina y la farmacéutica, los sistemas y mercados financieros y bursátiles, los sistemas militares de defensa e inteligencia, los bancos de datos públicos y privados, el medio ambiente, la propiedad económica, intelectual e industrial, la generación de recursos económicos, la industria mediática y la seguridad, etc.*). Sistemas cuyo funcionamiento depende —*con mayor frecuencia*— del procesamiento y transmisión automatizada de datos e información informatizada, y su menoscabo puede producir resultados catastróficos con pérdidas humanas y materiales significativas para los individuos y la colectividad[7].

Riesgos tangibles causados por nuevas formas de conducta comisivas u omisivas, dolosas e imprudentes (CP. arts. 21 y ss., y 25.1), que implican el abuso de sistemas informáticos o telemáticos en el modo de realización de los delitos tradicionales (*computer crimes*); o la comisión u omisión de conductas informáticas idóneas para generar fisuras de seguridad que afectan a los sistemas informáticos, al procesamien-

4 Cfr. Zúñiga Rodríguez, Laura: Política criminal, Madrid, Colex, 2001, pág. 276.

5 En este sentido, cfr. Sánz Mulas: ob. cit., págs. 9 y 13 (48); Rodríguez Gómez, Carmen: Criminalidad y sistemas informáticos, en: El sistema penal frente a los retos de la nueva sociedad, Coord. María Rosario Diego Díaz-Santos y Eduardo Fabián Caparrós, XV Congreso Universitario de Alumnos de Derecho penal, Madrid, Colex, 2003, págs. 139 y 140 (-162); Silva Sánchez: ob. cit., pág. 27; Zúñiga Rodríguez: ob. cit., pág. 252 y ss.

6 Cfr. Corte Constitucional: T-594/1993, C-221/1994, T-596/1994, C-13/1997, T-35/1997, T101/1998, T-153/1998, C-481/1998, SU-641/1998, SU-642/1998, SU-642/1998, SU-337/1999, SU-623/2001, T-1025/2002, T-750/2003, T-808/2003, T-30/2004.

7 Sobre los efectos negativos de la revolución informática vid. Gutiérrez Francés, ob. cit., pág. 42 y ss.; Sánz Mulas: ob. cit., pág. 11; Matellanes Rodríguez, Nuria: Algunas notas sobre las formas de delincuencia informática en el Código penal, en: Hacia un Derecho penal sin fronteras, Coord. María Rosario Diego Díaz-Santos y Virginia Sánchez López, XII Congreso Universitario de Alumnos de Derecho penal, Madrid, Colex, 2000, pág. 129, precisa que "el proceso de la técnica representa un nuevo factor en la interdependencia múltiple entre la criminalidad de los negocios y el estado socioeconómico de la sociedad"; y Ull Pont, Eugenio: Derecho público de la informática, Madrid, UNED, pág. 17. Asimismo, Vid. el IC3-2004 Internet Fraud-crime

to, transmisión o almacenamiento de la información o los datos[8], como objetos y funciones susceptibles de protección jurídico penal, junto a los bienes jurídicos 'tradicionales' (*computer-related crimes*)[9]. Amenazas que entrañan, de forma subsidiaria, la pérdida de credibilidad y confianza —*individual y colectiva*— en la seguridad que las instituciones públicas y privadas están obligadas a proveer en la gestión informática de los productos y servicios que desarrollan. Elementos que se deben garantizar para sostener las condiciones mínimas de interacción normal de los individuos en el moderno sistema social digital[10].

Así las cosas, la fenomenología criminal ha variado como secuela del cambio informático global; pues la primera se ha adaptado al segundo, con el efecto previsible de que los mecanismos institucionalizados de regulación de la vida social han transformado —*no siempre de manera adecuada*— sus propias perspectivas y criterios de imputación[11]. Especialmente el Derecho penal, con el fin de mejorar sus herramientas de prevención, control y sanción. Y ello es así, pues se afirma que las técnicas jurídicas de control tradicionales resultan cada vez menos eficaces —*aunque ello sea discutible*[12]— para prevenir o someter formas de criminalidad masificadas, especializadas[13], continuas, lesivas, muy difíciles de descubrir, rastrear y criminalizar; por oposición a la progresiva vulnerabilidad de las víctimas y de las funciones protegidas.

Características que concurren en el ámbito informático, con la observación adicional de que la mayoría de estas conductas ocurren en contextos de globalización

---

Report. Enero 01/2004 a 12/31 de 2004, del Nacional collar Crimencenter and FBI., 2005, en: http://www.ic3.gov o http://www.ifccfbi.gov, en el que se expone la tasa de criminalidad informática en EE.UU. durante el 2004.

8 Por dato se entiende la unidad básica de información, ello es, cualquier representación de información, conocimiento, hechos, conceptos o instrucciones que pueden ser procesadas u operadas por sistemas automáticos de computadores, y cuya unión con otros datos conforma la información en sentido estricto.

9 Vid. Matellanes Rodríguez: Algunas..., ob. cit., págs. 129-130 (147); Rovira del Canto, Enrique: Delincuencia informática y fraudes informáticos, Estudios de Derecho penal No. 33, (Dir.) Carlos María Romeo Casabona, Comares, Granada, 2002, pág. 69 y ss.

10 Como lo advierte Cadavid Quintero, Alfonso: Introducción a la teoría del delito, especial consideración a los fundamentos del delito imprudente, (Colección Sistema Penal No. 2), Medellín, Diké, 1998, pág. 134, "…esas condiciones de participación han de mirar a la persona como individuo y como miembro de todo el colectivo social".

11 De hecho, estas tendencias han llevado a hablar de la 'crisis de la expansión del Derecho penal' en la post-modernidad económica y social. Sobre el particular, cfr. Silva Sánchez: ob. cit., pág. 25 y ss.; El mismo: Prólogo a la ed. española, en: La insostenible situación del Derecho penal, Estudios de Derecho penal, (Dir. Carlos María Romeo Casabona), Granada, Instituto de ciencias criminales de Frankfurt y Área de Derecho Penal de la Universidad Pompeu Fabra, 2002, pág. XI y ss; Y Zúñiga Rodríguez: ob. cit., pág. 37 —cita 57.

12 Cfr. Díez Ripollés, José Luis: De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado, en: RECPC 07-01 (2005) http://criminet.ugr.es/recpc, pág. 01:3 y ss.

13 Silva Sánchez: ob. cit., pág. 30; cfr. Farjat, Gérard: ob. cit., pág. 524.

comunicativa, favorecidas por la interconexión de computadoras a través de redes internaciones. Dicho lo cual, la criminalidad informática o los delitos tradicionales realizados por tales medios adquieren dimensiones que obligan a reevaluar y homogenizar la reacción jurídica de los diferentes Estados[14]. En cualquier caso, es claro que el problema de la '*criminalidad informática*' no se reduce a los países industrializados, pues a diferencia de otros avances tecnológicos, éste está supeditado a las necesidades y avances del marcado internacional y se cuenta además como un instrumento paradigmático de mercadeo en el ámbito de la '**World Wide Web**'.

No obstante lo anterior, lo cierto es que la protección penal en la materia ni es sencilla ni homogénea a nivel internacional, y en muchos casos, la tipificación de tales conductas informáticas supone privilegiar técnicas de penalización dudosas y problemáticas que desestabilizan el complejo bloque constitucional de garantías asistido por el Derecho penal liberal. He aquí, precisamente el debate jurídico actual en nuestro medio: *¿Cuándo, bajo qué condiciones y frente a cuáles aspectos, se puede considerar adecuado y legítimo proteger los intereses informáticos propiamente dichos en nuestro medio? ¿Qué bien jurídico concreto se protege, cuándo se protege aquéllos de forma independiente? Y ¿Cuáles son los límites de criminalización que se desprenden del principio de intervención mínima del Derecho penal, para este ámbito específico?*

Por supuesto, la criminalización primaria de las conductas peligrosas dirigidas a afectar los intereses informáticos, los intereses de los usuarios y propietarios de los sistemas informáticos, los intereses generales, de terceros y del Estado a través de dichos medios y sus instrumentos, resulta un problema sustancialmente político-criminal[15] que —*como cualquiera otra decisión en este sentido*— implica valorar la utilidad real (*por oposición a la simbólica*) y la correcta legitimidad de la penalización de dichas conductas, desde las diversas perspectivas sociales, económicas y políticas que intervienen en la realidad colombiana, con el propósito de lograr una legislación dinámica en la materia.

De este modo, cuestiones tan complejas como las expuestas no se pueden resolver aceptando —*de forma acrítica*— las amplias demandas de criminalización especializada

14 Cfr. Sobre el carácter internacional de la informática, Bekerman, Jorge M.: Informática: su regulación jurídica internacional "vis-á-vis" la brecha tecnológica, en: El derecho y las nuevas tecnologías. Contexto económico, social y cultural. AA.VV., separata de Revista del Derecho industrial, No. 33, Buenos aires, Depalma, 1990, pág. 747.

15 Cfr. Möhrenschlager, Manfred E.: Tendencias de política jurídica en la lucha contra la delincuencia relacionada con la informática, trad. Francisco Baldó Lavilla y Santiago Mir Puig, en: Delincuencia informática, Barcelona, PPU, 1992, pág. 50, cuando indica: "Al examinar concretamente si la protección jurídico (-penal) debe extenderse al ámbito del proceso de datos se deberán hacer las siguientes reflexiones. ¿Hasta qué punto existe ya una protección fuera del ámbito de las nuevas tecnologías? ¿Son lesionados de forma análoga los intereses allí protegidos en el ámbito del proceso de datos? ¿Existe efectivamente una necesidad de extensión de la protección jurídico-penal? ¿No debe ésta extenderse incluso más allá del ámbito de los ordenadores? En efecto, el peligro de una <<sobre-incriminación>> no puede ser perdido de vista, si bien el legislador puede escapar del mismo por diversos causes".

que muchos sectores técnicos proponen, a través de normas penales '*sui géneris*' o autónomas de peligro, de emprendimiento, en blanco y simbólicas (incluso paralelas a los tipos penales tradicionales), para aumentar la eficacia de la seguridad informática a través del instrumento punitivo. Justamente, porque en dicho análisis operan de forma simultánea criterios normativos que exigen salvaguardar la materialidad de los derechos fundamentales de los asociados, lo que incluye por igual los derechos de las víctimas y de los procesados bajo el paradigma de Estado Social y democrático de Derecho (Const. Pol. Preámbulo y art. 1°) y los principios político criminales que se desprenden del mismo (CP., arts. 1° a 13).

Ello exige, entonces, encontrar un punto de equilibrio adecuado entre una intervención punitiva limitada en la materia y las garantías fundamentales de los ciudadanos. Más aún, cuando todo indica que los parámetros tradicionales para justificar la protección de los bienes jurídicos, no resultan plenamente satisfactorios para justificar —*del mismo modo*— los intereses informáticos; precisamente, atendidas sus características particulares como *el uso masivo, la descentralización, la continuidad, el automatismo y la necesaria remisión a complejas cuestiones técnicas*[16] (que por lo pronto escapan a las consideraciones jurídicas que se presentan en estas páginas), caracterizadas por su inestabilidad y permanente transformación (de lo cual se deduce que la '*la seguridad de la información*' es todavía un interés jurídico en formación y, por ende, difuso).

En fin, lo dicho, acompañado de la incapacidad institucional para responder de forma adecuada ante esta criminalidad, a la par que se modifican las cuestiones tecnológicas y particularmente la Internet sin la apropiada adecuación legislativa[17], hacen del tema de la criminalidad informática un fenómeno complejo, difícilmente prevenible y previsible, simbólico y seriamente inseguro —*desde el punto de vista dogmático, procesal y probatorio*—, donde impera una gran '*cifra negra de criminalidad*'[18].

---

16 Sobre las características de los delitos informáticos, vid. Sanz Mulas: ob. cit., pág. 21; Matellanes: ob. cit., pág. 135; Poullet, Ives: Derecho y nuevas tecnologías de la información: un enfoque comparativo del derecho europeo continental, en: El Derecho y las nuevas tecnologías. Contexto económico, social y cultural. AA.VV, separata de Revista del Derecho industrial, No. 33, Buenos aires, Depalma, 1990, pág. 773; Rovira del Canto: ob. cit., pág. 76 y ss; Sieber, Ulrich: Criminalidad informática: peligro y prevención, trad. de Elena Farré Trepat, en: Criminalidad informática, compendio, Barcelona, PPU., 1992, pág. 29 y ss.

17 Sobre el particular, cfr. Rodríguez Gómez: ob. cit., pág. 141, quien indica que: "sin embargo, Internet crece a tal velocidad, y su desarrollo se está produciendo de forma tan desorganizada, que el ordenamiento jurídico no tiene tiempo de prever, luego de regular las posibles relaciones que se generen en su seno, y con mayor motivo los conflictos que necesariamente se derivan de esas relaciones. Es un hecho incuestionable que la cyberdelincuencia se desarrolla a mayor velocidad a la que los Estados pueden reaccionar, tanto para prevenir como para castigar".

18 Como advierte Matallenes: ob. cit., págs. 134 y 135, ello se explica toda vez que la mayoría de los sujetos pasivos de esta clase de delitos, son personas jurídicas para las cuales "resulta vergonzoso denunciar los hechos, dados los evidentes perjuicios que para su reputación se

Por tal motivo, antes de proyectar al Derecho penal como protector de *prima ratio*, *en primer lugar*, la comunidad jurídica nacional debe alcanzar determinados consensos polticocriminales en la materia, que procuren una racionalización progresiva de las medidas preventivas y punitivas que deba adoptar la legislación en el contexto económico colombiano, desde luego, atendidas las recomendaciones internacionales en la materia. Y, en segundo lugar, es necesario que nuestro medio tome conciencia de la importancia de lograr altos niveles de autorregulación privada en gestión de seguridad informática[19], pues sólo de este modo se podrán identificar y legitimar los espacios de intervención punitiva necesitados de protección penal, de conformidad con las exigencias de subsidiariedad y fragmentariedad, una vez agotadas otras instancias legales de prevención (paradigma de contención).

II. Ámbito de definición de los delitos informáticos

Según la doctrina especializada, la criminalidad informática incluye dos manifestaciones distintas desde la perspectiva de la fenomenología criminal[20]. Tal y como se mencionó antes, la primera de ellas se relaciona con las conductas punibles tradicionales que admiten, al ser tipos abiertos por su estructura, la ejecución de su verbo rector a través de redes de comunicación automatizadas o por sistemas informáticos o telemáticos (utilización de elementos incorporales). Conductas que afectan a bienes jurídicos individuales o supraindividuales de arraigada tradición jurídica, como el patrimonio económico o público, la intimidad personal o la fe pública. Un ejemplo sería la realización de conductas con el propósito de destruir equipos o sistemas informáticos y telemáticos a través de programas dañinos; o cuando en la Web se disponen los mecanismos lógicos necesarios para inducir en error a sujetos, quienes por virtud del mismo realizan actividades que implican su despatrimonialización efectiva en beneficio ilícito de terceros (estafas en la Web), entre otras conductas delictivas[21].

---

derivarían del conocimiento público de su vulnerabilidad y porque consideran que puede ser más ventajoso para ellas mantener al sujeto en su puesto de trabajo (u ofrecérselo) que ponerlo a disposición de las autoridades judiciales"; AA.VV. Penalización de la criminalidad informática, Proyecto académico, Santa Fe de Bogotá, Gustavo Ibáñez, 1998, pág. 63 y ss.; Gutiérrez Francés, ob. cit., pág. 72; Romeo Casabona: Poder informático…, ob. cit., pág. 36 y ss.

19 Ponen de relieve la importancia de dichas medidas en materia de disuasión, prevención, detección, minimización de efectos y cumplimiento de exigencias legales: Gutiérrez Francés: ob. cit., pág. 622; Romeo Casabona: Poder informático…, ob. cit., pág. 40; Sieber: Criminalidad…, ob. cit., págs. 16 y ss. y, 34 y ss.; Sieber: Documentación para una aproximación al delito informático, trad. de Ujala Joshi Jubert, en: Delincuencia informática, Barcelona, PPU, 1992, pág. 83 y ss.; Sneyers, Alfredo: El fraude y otros delitos informáticos, Madrid, Tecnologías de Gerencia y Producción, S.A., 1990, pág. 155.

20 Cfr. Matallenes: ob. cit., pág. 130; Rovira del Canto: ob. cit., pág. 131.

21 Desde luego, esta perspectiva debe ser concretada a los grupos de delitos considerados informáticos desde una perspectiva criminológica, pues de no ser así, casi todos los tipos

A su turno, la segunda manifestación (*delitos informáticos propiamente dichos*) se relaciona con aquellas conductas lesivas no consentidas, cuyos objetos materiales exclusivos son la confiabilidad (*calidad, pureza, idoneidad y corrección*), la integridad y la disponibilidad de datos o información, y de los componentes lógicos de programación de los equipos informáticos que permiten el tratamiento, transmisión o almacenamiento de los mismos (*programas operativos o aplicativos, o software*[22]). Objetos que resultan lesionados o puestos en peligro por conductas que los manipulen con fines ilícitos o de lucro, o también por el uso de programas lesivos creados con tal propósito[23], como, P. Ej.: los virus que se intrusan en los códigos fuente del software (Windows u Office), los

penales previstos por el Código de 2000 se podrían considerar como delitos informáticos, precisamente, porque su estructura modal abierta permitiría su realización a través de medios informáticos.

22 Según la Decisión 351 de 1993 (Comunidad Andina de Naciones) art. 3°, un programa de ordenador es la "expresión de un conjunto de instrucciones mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador, un aparato electrónico o similar capaz de elaborar informaciones, ejecute determinada tarea u obtenga determinado resultado. El programa de ordenador comprende también la documentación técnica y los manuales de uso". El ordenamiento colombiano define lo que queda comprendido por la voz software en el Decreto reglamentario 1360 de 1989, art. 1°, de la siguiente forma: "De conformidad con lo previsto en la Ley 23 de 1982, sobre derechos de autor, el soporte lógico (software) se considera como una creación propia de dominio literario". Y en el art. 2° Ibíd., indica: "El soporte lógico (software) comprende uno o varios de los siguientes elementos: el programa de computador, la descripción del programa y el material auxiliar". En cuanto a su protección, el art. 7° del mencionado decreto advierte que "la protección que otorga el derecho de autor al soporte lógico (software) no excluye otras formas de protección por el derecho común".

23 Por el nombre genérico de virus se engloban varios conceptos distintos, que de forma necesaria deben estar integrados en un archivo con instrucciones propias. / A) Virus. Consiste en un programa de software que, oculto en otro programa, destruye datos o información. No requiere las redes para existir y su hábitat natural es el computador. / Virus de acción directa. En el momento de su ejecución infecta a otros programas. / B) Virus residentes. Al ser ejecutados, se instalan en la memoria del ordenador. Infectan a los demás programas a medida que son ejecutados. / C) Gusano. Este tipo de software no busca principalmente la destrucción de datos, sino su autorreplicación y transmisión para interferir la función informática de otros ordenadores. Su campo de actuación es la Red. / D) Bomba Lógica. Es otro tipo de software que permanece latente hasta que, dada una condición o una fecha determinadas, despierta y se ejecuta, lo que produce la destrucción del ordenador o la Red. / E) Troyanos. No producen destrucción alguna, sino que abren una puerta trasera en el computador para que otro usuario pueda acceder en él, todo ello sin el conocimiento y consentimiento del usuario. / F) Programas Bug. Examinan los códigos fuente o las instrucciones básicas de los programas y determinan aspectos vulnerables de los mismos, que al ser desconocidos por la generalidad de los usuarios, se pueden emplear con propósitos ilícitos.

gusanos, las bombas lógicas, las llaves maestras, los programas Bug y el *'spam'*[24]. Conductas que generalmente comportan, no sólo amenazas contra la propiedad, la integridad, la disponibilidad y la confiabilidad de los datos o la información informatizada, sino también atentados contra la intimidad personal, los derechos de autor o la seguridad.

También puede suceder el caso de conductas que afecten la información o ataquen sistemas informáticos con el propósito de facilitar, consumar o llevar a cabo conductas punibles tradicionales que luego ocurren en la Web o que comienzan en ella; pero terminan por fuera de la misma. O conductas que afecten la información o ataquen sistemas informáticos con la finalidad de ocultar, asegurar el producto o lograr la impunidad de conductas tradicionales que se han realizado en o por fuera de la '*Red*'. En estos casos, se puede hablar de unidades de conducta de naturaleza pluriofensiva (*pues afectan diversos bienes jurídicos tutelados*), que probablemente configurarán una pluralidad de tipicidades entre '*computer crimes*', '*computer-related-crimes*' y conductas punibles tradicionales.

Ahora bien. Uno de los inconvenientes más importantes en esta materia, es que asumir una concepción teórica de la '*delincuencia informática'* estructurada entre el criterio objetivo del ámbito delictivo (*situación típica de riesgo*) y el normativo del bien jurídico protegido, resulta ambivalente de cara a las conductas delictivas tradicionales preexistentes, pues éstas se verifican a veces muy amplias o muy limitadas para proteger el interés jurídico '*seguridad de la información*'. Ambigüedad jurídica que es frecuente, a pesar de que muchas legislaciones consagran normas penales especiales, pues hasta el momento no ha sido posible lograr un acuerdo político criminal que erija una regla clara y confiable que facilite *—de conformidad con un bien jurídico delimitado—* una clasificación 'jurídico-penal' satisfactoria de los comportamientos delictivos informáticos. Clasificación que también justifique *—en concreto—* su posible tratamiento general como tipos penales autónomos. De hecho, por fuera de las recomendaciones internacionales[25], la doctrina penal trabaja con múltiples clasificaciones en la materia, que no siempre resultan compatibles entre sí[26].

---

24 Sobre el particular, cfr. Quintero Marín, Víctor Hugo: El Spam y otros abusos de correo electrónico, en: Revista de Derecho, comunicaciones y Nuevas tecnologías, No. 1 (Abril de 2005), Bogotá, Cijus- Ed. Uniandinas, 2005, págs. 143 a 173.

25 Consejo de Europa: Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, serie de tratados europeos Núm. 185, en: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm

26 Como advierte Campoli, Gabriel Andrés: Pasos hacia la reforma penal en materia de delitos informáticos en México, en: Revista de Derecho Informático: Alfa-redi Derecho y Nuevas Tecnologías, No. 079 - Febrero del 2005, http://www.alfa-redi.org/rdi-articulo.shtml?x=974, "…en verdad las clasificaciones de los técnicos en informática no coinciden con las de los hombres de derecho, ya que unos clasifican por cuestiones técnicas y los otros lo hacemos por las conductas desarrolladas, lo que no coincide al 100%, ya que como sabemos los equipos informáticos no son más que herramientas…".

Por tal motivo, la categoría de '*delitos informáticos o Cibercrímenes*' está llamada por el momento –*en nuestro medio*– a hacer parte de otras clasificaciones materiales de corte criminológico en el ámbito penal –p. Ej.: *los delitos de "cuello blanco*[27] *o white collar crimes y/o High-tech crimes"*–, que abarcan un sinnúmero de comportamientos lesivos contra bienes jurídicos variados, sobre todo en el ámbito de los intereses patrimoniales y socio-económicos. Como lo advierte **MATELLANES**: "*no hay un único <<delito informático>>, sino que la actuación subrepticia en torno a las funciones mencionadas puede generar la comisión de los más diversos tipos delictivos*"[28]. Con tal punto de partida, es necesario asumir una definición relativamente flexible de criminalidad informática (o de datos e información), con el propósito de lograr su adecuado tratamiento criminológico, dogmático, procesal y politicocriminal. Una definición que permita, o bien adaptar –*por equivalencia*– las conductas punibles preexistentes en la legislación jurídico penal; o adicionar de modo excepcional tipos penales nuevos con el fin de garantizar la protección integral de '*la sociedad de la información*'.

Desde luego, vale la pena aclarar que –*en los términos de la clasificación asumida*– por *criminalidad informática en sentido estricto* o, de modo más preciso, por *delito informático propiamente dicho*, se entiende cualquier conducta con fines ilícitos, ello es, no autorizada por el titular del bien jurídico afectado o abusiva de dicho consentimiento, dirigida a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación y ejecución automática de programas de datos o información informatizada reservada o secreta de naturaleza personal, empresarial, comercial o pública. Ello, con independencia de que los resultados o los actos de agotamiento de dicha conducta punible de emprendimiento constituyan una conducta delictiva independiente. Como es apenas

27 Vid. Guerrero Mateus, María Fernanda/ Santos Mera, Jaime Eduardo: Fraude informático en la Banca, Aspectos criminológicos, Santafe de Bogotá, Resma, 1993, pág. 39 y ss.; Matellanes: ob. cit., pág. 134.

28 Ibíd., pág. 130. Sobre el particular, Márquez Escobar, Carlos Pablo: El delito informático, la información y la comunicación en la esfera penal, conforme con el Nuevo Código Penal, Bogotá, Leyer, S.F., pág. 91, indica: "…para nosotros el delito informático no es un nuevo catálogo de hechos punibles sino un conjunto de conductas tipificadas que siendo tradicionales o no, atentan contra distintos objetos jurídicos y cuyo fin material y productivo es la información"; Poullet: ob. cit., pág. 779. Sin embargo, Rovira del Canto: ob. cit., pág. 130, afirma que "es preciso delimitar o reducir tal consideración o calificación de delito informático a aquellos supuestos delictivos que realmente tengan presente en su protección no solo bienes jurídicos tradicionales sino también los incorporados como consecuencia de las nuevas tecnologías de la informática y telecomunicaciones, esto es, directamente la información en sí misma, como bien dotado de valor económico, en cuanto que representación de poder que devienen de su conocimiento y acceso a la misma, o indirectamente a través de la fiabilidad de su representación, los datos informáticos o de la seguridad y fiabilidad de sus causes de procesamiento y transferencia, los sistemas y redes informáticas y de telecomunicaciones, o de los medios que originan el funcionamiento de dichos sistemas, esto es, los programas informáticos o software".

evidente, la definición anterior excluye las conductas punibles tradicionales realizadas sobre objetos informáticos, como, P. Ej: el hurto de una computadora, el abuso de un 'cajero automático' y la destrucción incendiaria o terrorista de centrales informáticas.

Para terminar, no se puede ignorar que un sector muy respetable de la doctrina penal sostiene *—de manera contundente y por oposición a un simple interés jurídico—* la existencia consolidada de un bien jurídico intermedio susceptible de protección penal, que consiste en: '*la seguridad de las funciones informáticas*' referida al almacenamiento, disponibilidad, tratamiento y transmisión de información eficaz y segura con valor para el comercio o la industria. Bien jurídico de naturaleza intermedia que estaría referido al '*orden económico social*', sin perjuicio de afectar también *—de manera colateral—* el patrimonio económico, entre otros bienes personales o colectivos.

Con tal punto de partida, los delitos informáticos constituirán figuras delictivas autónomas (*delicta sui generis*), de peligro y en blanco, aplicables de forma preferente cuando se vulneren las funciones informáticas referidas a la información (*entendida como bien inmaterial público y nuevo paradigma económico*), frente a otras conductas que vulneren bienes jurídicos personales o personalísimos de forma incidental[29]. Dicho lo cual, el problema jurídico se traslada, no solo a la cuestión de la legitimidad de las modalidades típicas necesarias para proteger dicho interés social como bien jurídico, sino también al tratamiento que se debe dar, conforme a las reglas que rigen la unidad o pluralidad de tipicidades, a las conductas que trascienden la afectación de la información y vulneren *—al tiempo—* otros bienes jurídicos como la intimidad personal[30].

---

29 En este sentido, cfr. Reyna, Luis: El bien jurídico en el delito informático, en: http://www.alfa-redi.org7revista/data/34-14.asp. Sobre el tema, vid. Castro Ospina, Sandra Jeannette: Delitos Informáticos: La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano, Madrid, DelitosInformaticos.com, 15.07.2002. http://www.delitosinformaticos.com/delitos/colombia.shtml; Rovira del Canto: ob. cit., págs. 67 y 69 y ss. También en: Castro Ospina, Sandra Jeannette: Delitos Informáticos: La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano, en: XXIII Jornadas Internacionales de Derecho penal, Memorias, Bogotá, Universidad Externado de Colombia, Departamento de Derecho penal, págs. 127-162.

30 En este sentido, se comparte plenamente la opinión de Cadavid Quintero, ob. cit. , pág. 134, cuando advierte que "No se repudia entonces, de ninguna manera, la posible protección de bienes jurídicos colectivos; pero se exige que ella se dé solo en la medida en que el respeto a los mismos se constituya en condición para la creación de un medio más adecuado para la realización individual de los ciudadanos. La protección penal de bienes jurídicos colectivos carentes de esa relación instrumental o funcional con la garantía de mejores condiciones de vida para los ciudadanos, que en consecuencia se configure como protección del sistema social visto formalmente, es decir, como mera estructura vacía de tal función, no es aceptable".

III. Diversas hipótesis de delitos informáticos en sentido criminológico

Visto en términos generales el contexto de la criminalidad informática, a continuación se verifican de manera sucinta algunas conductas que, al ser realizadas en el ámbito informático[31], se incluyen en los bloques de '*cibercrímenes*' en sentido criminológico como computer related crimes o delitos informáticos en sentido estricto (*–intrusismo, espionaje, daños, fraude, falsedad, responsabilidad por contenidos y violación a los derechos de autor*); se determina brevemente su tratamiento en el estatuto punitivo colombiano[32] y se plantean las observaciones jurídicas pertinentes; para terminar con algunas consideraciones a modo de conclusión.

A. El intrusismo informático. Por esta modalidad delictiva *–en sentido general–* se puede entender la conducta de arrogarse ilegalmente *–de forma no autorizada–* el derecho o la jurisdicción de intrusarse o '*ingresar*' en un sistema informático o red de comunicación electrónica de datos, con la consecuente trasgresión de las seguridades dispuestas por el '*Webmaster*' o prestador del servicio[33] al '*Webhosting*' u '*Owner*', con el fin de proteger los servicios de transmisión, almacenamiento y procesamiento de datos que ofrece frente a posibles abusos de terceros (*ingreso en cuentas de e-mail ajenas*). Así como también la utilización o interferencia indebidos de dichos equipos o sistemas informáticos o telemáticos, o la permanencia contumaz en los mismos por fuera de la autorización o del consentimiento válidamente emitido por el titular del derecho (art. 32, num. 2) o de la ley. La doctrina compara usualmente esta conducta con el delito de violación de domicilio (CP. art. 189 y ss.). No obstante, ello sería plausible si la actividad de intrusión, la permanencia contumaz o el uso ilegal se hubieren realizado de forma engañosa, clandestina o arbitraria desactivando las medidas electrónicas existentes, teniendo en cuenta que los medios a los que se accede son completamente distintos.

---

31 Sobre el tema, véase Rodríguez Gómez: ob. cit., pág. 142 y ss.; Schwarzenegger, Christian: Computer crimes in Cyberspace. A comparative analysis of criminal law in Germany, Switzerland and northern Europe, en: http://www.weblaw.ch/jusletter/artikel.jsp?articleNr=1957.ok.2002. Jusletter 14. Oktober 2002, www.jusletter.ch. Sobre las diferentes propuestas internacionales cfr. Convention on cybercrime (ETS. No. 185), en : http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm

32 Como lo advierte Rovira del Canto: ob. cit., pág. 1: «el principal problema es el de verificar si tales conductas… pueden ser subsumidas por los tipos penales existentes. Y de ser así, si la punibilidad de los mismos es o no adecuada de cara al principio de legalidad".

33 La Convención de Budapest del 23.22.2001, ob. cit., art. 1°, lit. c, indica que: "Proveedor de Servicios" significa: I) Cualquier entidad pública o privada que suministra a los usuarios de su servicio la capacidad de comunicarse por medio de un sistema de computador, y II) Cualquier otra entidad que procesa o almacena datos del computador a favor de dicho servicio de comunicación o de los usuarios de éstos servicios.

En realidad, el fundamento material de la incriminación punitiva de dicha conducta consiste en ingresar dolosamente *—con violación de las condiciones de privacidad—* al sistema informático o red de comunicación electrónica de datos, y tener la finalidad y la posibilidad fáctica *—al menos un instante—* de obtener servicios o de disponer de la información existente y retirarla del mismo; con lo cual, se crea un peligro verificable y concreto para el titular de los bienes jurídicos. Actividades para las que no se ha concedido al intruso la clave de seguridad personal o la correspondiente autorización que, precisamente, es lo que permite la conexión normal al medio informático y lucrarse de manera lícita (aun cuando sea el mismo prestador del servicio sin legitimidad, arguyendo razones de verificación).

Justamente, el CP. de 2000 sanciona en el art. 195[34], mediante una fórmula genérica, la figura del ***acceso abusivo a un sistema informático***[35] ***protegido con medida de seguridad,*** a la cual se le asigna *—por ese sólo hecho—* la condigna sanción de multa en la modalidad progresiva de unidad multa que, según el patrimonio y los ingresos económicos del sujeto, podría ascender hasta 1000 salarios mínimos mensuales legales vigentes (art. 39 num. 2). Conducta punible que pretende proteger la intimidad, la reserva y el derecho a la no interceptación de comunicaciones privadas[36], desde la perspectiva del bien jurídico más general de la libertad individual (Capítulo séptimo del Título III, Libro II del CP. Y Const. Pol., art. 15).

---

34 Art. 195: "El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa". Dicha conducta tiene referente en el CP. español, art. 197.2, apt. 2°, cuando indica que se impondrán las penas previstas en el art. 197.1, "…a quien, sin estar autorizado, acceda por cualquier medio a los mismos…", es decir, cuando se acceda sin autorización en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado que contenga datos reservados de carácter personal o familiar. De otro lado, el CP. Federal de México regula los delitos de acceso ilegal a los sistemas informáticos en los arts. 211 Bis 1 al 211 bis 7 y en la Ley 2002-67 de Comercio electrónico, firmas electrónicas y mensajes de datos (Registro Oficial 557-S, 17-IV-2002), arts. 58 a 64; La ley 19223 de 1993 de Chile, art. 2°, consagra como delito el acceso, con ánimo de usar o conocer de forma indebida la información contenida en un sistema de tratamiento de información (con lo cual congloba las posibles afectaciones generales a la intimidad o confidencialidad de la información oficial); el CP. Suizo castiga dicha conducta en el art. 146bis.; el CP. francés, mod. Ley 92-683 de 1994, la sanciona en el art. 323-1; el StGB. alemán en el § 202a; el CP italiano en el art. 615-. tercero. De otro lado, dicha conducta tiene referente en la Convención de Budapest del 23.22.2001, ob. cit., Cáp. II, Sección 1, art. 2° "Acceso ilegal" que, entre otras cosas, demanda el propósito (elemento subjetivo especial distinto del dolo) de obtener datos del computador o realizar cualquier otro intento deshonesto.

35 En general, los sistemas informáticos contienen, entre otras cosas, sistemas operativos, es decir, programas o conjuntos de programas que realizan la gestión de los procesos básicos del sistema y que permiten la normal ejecución de las operaciones relativas al tratamiento automático de la información.

36 Sobre el derecho fundamental a la intimidad, cfr. sentencias T-414/1992, T-611/1992, T-259/1994, T-696/1996, T-729/2002, entre otras.

Así las cosas, el tipo penal bajo análisis prevé —*desde un punto de vista estructural*— dos conductas de naturaleza alternativa que, desafortunadamente, no exigen al agente realizar la conducta con alguna finalidad ilícita concreta o alcanzar algún grado de disponibilidad sobre datos o informaciones para realizar actividades delictivas posteriores. De este modo, en primer lugar, se prevé la conducta de acceso directo, no autorizado y doloso (*abusivo u oculto*) a un sistema informático protegido con medida de seguridad. Descripción comportamental que demanda, no sólo que la acción intrusiva comporte la infracción al deber de confianza (que en el punto resulta necesaria pero insuficiente por sí misma), sino, también, que la conducta conlleve la realización de manipulaciones dolosas orientadas a quebrantar o a superar las medidas de seguridad informáticas dispuestas para limitar el 'ingreso' o acceso libre al sistema, programa, módulo informático o base de datos. Acciones que requieren —*generalmente*— el empleo de conocimientos medianamente avanzados o de instrumentos, programas (estilo «*Daemon Tools*») o la utilización aparatos electrónicos adicionales que faciliten dicha actividad[37].

En este sentido, será atípico el ingreso voluntario a una página Web o a un sistema informático público o de libre acceso; así como también —*en principio*— el acceso a un sistema en el que sólo se han dispuesto advertencias referidas a la prohibición genérica de acceder sin la observancia de ciertas condiciones como, por ejemplo, si no se cumple con cierta edad o si no se está en un determinado lugar o país. Y ello es así, pues tales advertencias, aunque expresan determinada voluntad de *prevenir* el acceso al sistema informático, en realidad no constituyen medidas de seguridad que *limiten* el acceso de terceros a los datos o la información, en el sentido requerido por la descripción típica vertida en el art. 195 del Código penal.

Así mismo, desde una perspectiva material, también resulta necesario que dichas medidas de seguridad sean idóneas, adecuadas, explícitas y equivalentes —*como mínimo*— a aquellas medidas sugeridas como consecuencia de la aplicación de los estándares de gestión de seguridad informática; o a aquellas medidas o programas de seguridad empleados en el tráfico informático ordinario por los técnicos expertos en la materia[38] . Y ello es así, pues se requiere la existencia de medidas de seguridad que efectivamente

37 Precisamente, el CP. español sanciona en el art. 264.2, apt. 3°, las conductas de fabricar, importar, poner en circulación o tener cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador, entre otros objetos protegidos.

38 En este sentido, Castro Ospina: Ob. cit., en: http:/www.delitosinformáticos.com/delitos/colombia3.shtml, afirma que "las medidas de seguridad de un sistema no se limitan a las claves o login para accesos autorizados; tiempo de uso; y áreas restringidas de acceso para usuarios"; Sieber: documentos…, ob. cit., pág. 84 y ss., y Sieber: Criminalidad…, ob. cit., pág. 34 y ss. Actualmente existen varias normativas técnicas que precisan los estándares básicos en materia de gestión técnica, legal y administrativa en el manejo de la seguridad de la información, como por ejemplo: el ISO 14001:1996, el ISO 9001:2000 y de manera más reciente, el UNE/ISO/IEC

provean seguridad con eficacia, de conformidad con la importancia y la clase de sistema informático, red de comunicación electrónica de datos o base de datos de que se trate (medidas que serán simples si se trata de un ordenador personal, y complejas si se trata de la base de datos de una entidad bancaria). De no ser así, no se podría hablar con rigor de una conducta de acceso abusivo a un sistema informático '*protegido*', sino, más bien, de acceso abusivo a un sistema informático '*desprotegido*' por contar con medidas de seguridad ineficaces.

De otro lado, esta exigencia es fundamental, pues, si bien es posible que la existencia de un sistema de seguridad informático 'ineficaz' probablemente no elimine la consideración de que la conducta intrusiva representa un riesgo abstracto para el bien jurídico 'seguridad de la información'; sí implica debatir —según la clase de datos o información vulnerada y de sistema violado— si la conducta de intrusión queda cobijada plenamente por el ámbito de protección de la norma penal; pues es precisamente la omisión del titular del sistema informático —*al no adoptar las normas técnicas requeridas en la materia para la clase de sistema que ostenta*— lo que permite exponer la integridad, confidencialidad o disponibilidad de los datos o la información de naturaleza reservada al riesgo de intrusión (suicidio informático). En efecto, mientras más sensible sea la información, mayores deben ser las medidas de seguridad dispuestas para su 'protección' real, cuando se esté obligado a ello.

Es más, incluso si al intruso le es imputable la conducta de acceso abusivo, no cabría desechar la posibilidad de atribuir algún tipo de responsabilidad jurídica al titular del sistema informático, red de comunicación electrónica de datos o bases de datos (si bien no penal en nuestro medio por virtud del principio de legalidad, sí de otra índole), por ejemplo, en aquellos casos en los que se desarrollan actividades de almacenamiento, procesamiento o transmisión de datos sensibles de terceros sin salvaguardas adecuadas. Precisamente, porque en la sociedad del riesgo y de la informa-

17799 (BS. 7799-2:2002 o código de buenas prácticas) y UNE 71502, que tienen como sustrato la planeación, verificación, manutención y disposición de medidas correctivas y preventivas para proteger la información en el ámbito de los mercados internacionales. En realidad, dichos sistemas buscan mejorar los siguientes aspectos: a) Establecimiento de los límites de la revisión. b) Identificación de activos de información. c) Evolución de los activos informáticos y determinación de su importancia. d) Evaluación de riesgos y amenazas. e) Evaluación de las vulnerabilidades de la empresa y control de accesos.Vulnerabilidades de orden organizacional, tecnológico, comunicativo, operativo físico, administrativo, procedimientos de seguridad, etc. f) Evaluación, planeación, selección y mejoramiento de medidas de seguridad (salvaguardas). g) Políticas y organización de seguridad; y h) Políticas de mantenimiento y desarrollo de los sistemas. Sobre el particular, cfr. www.baquia.com/noticias.php?id=9402 http://centrum.pucp.edu.pe/excelencia/ensayos/Gestion_manejo_seg_inf_bs7799.pdf www.bsiglobal.com/NSB/Governance/index.xalter www.s21sec.com/s21sec/ser_iso.jsp http://andercheran.upv.es/~toni/personal/campusti.pdf; i) Por todos, Cfr. Posada Maya, Ricardo: ¿Es intagral la protección juridicopenal por intrución informática para titulares de información reservada?, en: Revista Sistemas, No. 96 (Abril-junio 2006), Bogotá,Asociación Colombiana de Ingenieros de Sistemas, págs. 56-63, www.acis.org.co.

ción, quien adelanta este tipo de actividades adquiere la responsabilidad jurídica de proteger dichos objetos intangibles de manera eficaz e integral.

Es más, es posible sostener que la sola tenencia legítima de datos o de información de terceros (bancos de datos financieros, contables, etc.) constituye una modalidad de '*actividad peligrosa*'[39], pues dichos objetos, al encontrarse por fuera del ámbito de custodia material y directa de su titular, representan para éste una fuente de riesgos que escapa a su control y responsabilidad. En este orden de ideas, no es descabellado pensar en la posibilidad jurídica de estructurar —*en el futuro*— tipos penales de peligro concreto, bien por la omisión del control debido en la gestión de seguridad informática referida a las actividades de almacenamiento, procesamiento o transmisión de datos o información de naturaleza sensible de terceros; o por la adopción de medidas de seguridad y sistemas de salvaguarda irrisorios o inapropiados para proteger la seguridad, integridad, confiabilidad y disponibilidad de datos o informaciones sensibles de regulación controlada legalmente.

En fin, desde una perspectiva politicocriminal no parece adecuado librar de responsabilidad al titular del sistema informático, en aquellos casos en que, o bien de manera insegura o con simples advertencias expone al público contenidos legalmente regulados que requieren controles de acceso y de seguridad para cierta población protegida (pornografía), o cuando los datos o información de terceros sean manipulados o conocidos por intrusos debido a la omisión de controles previos en el ámbito de dominio específico de los titulares de sistemas informáticos.

En segundo lugar, el tipo penal consagra la conducta de permanencia abusiva dolosa en sistemas informáticos 'protegidos', contra la voluntad concurrente de quien tiene derecho a excluirlo —*por la violación de las condiciones de privacidad*—. Ello, sin importar si el sujeto ingresó al sistema por la violación arbitraria o clandestina de las medidas de seguridad dispuestas por el 'Owner'; o porque accedió por una violación no intencional o incidental de las medidas de seguridad, pero se mantuvo voluntariamente en el 'medio' con conciencia de que su permanencia constituye un abuso informático (al menos con dolo eventual)[40].

En este sentido, se puede afirmar que la expresión '...se mantenga *contra la voluntad de quien tiene derecho a excluirlo'* es innecesaria en algunos casos; pues basta conque el sujeto activo (intruso) hubiere advertido de forma inequívoca la restricción de ingreso

39 En sentido similar, cfr. AA. VV. Penalización…, ob. cit., pág. 34, cuando advierten que: "La actividad informática calificada por la doctrina como una actividad peligrosa, donde la información es un instrumento de poder y fuente potencial de peligrosidad, tiene indiscutiblemente unos riesgos que comprometen a los operadores que en dicha actividad intervienen".

40 Respecto del dolo y su prueba, vid. Díaz Pita, María del Mar: El dolo eventual, Valencia: Tirant lo blanch, 1994; Laurenzo Copello, Patricia: Dolo y conocimiento, Valencia: Tirant lo blanch, 1999 y Ragués I Vallès, Ramón: El dolo y su prueba en el proceso penal. Barcelona, José María Bosch, 1999.

al sistema y haya superado las medidas de seguridad de forma fraudulenta (intrusión dolosa directa o por aprovechamiento doloso de error ajeno), para deducir que su permanencia posterior en el mismo resulta contraria a la voluntad y al consentimiento del titular. Desde luego, esta interpretación debe ser matizada cuando el ingreso al 'medio' informático es *incidental, indirecto o bajo error* y la permanencia sea voluntaria, pues en estos casos lo que constituye la calificación de la intención como dolo de permanencia ilícita sería la 'contumacia' del sujeto activo, que se configura cuando el sujeto pasivo o el sujeto titular efectúa *—al menos—* una advertencia, señal o alarma directa que exprese su voluntad de excluir al intruso[41]. Ello, con independencia de las dificultades para determinar si alguno de los sujetos '*on-line*' representa una amenaza a los intereses del sujeto pasivo.

De otro modo, resultaría problemática la justificación politicocriminal del castigo penal al intruso incidental o por error que permanece en el sistema (error de tipo), y ello, pues se presumiría '*iure et de iure*' que su actuar voluntario de permanencia en el sistema es doloso y delictivo, en razón del mero peligro que su comportamiento probablemente pueda representar en abstracto para los intereses del sujeto pasivo, incluso bajo error.

Adicionalmente, todo indica que el tipo penal descrito en el art. 195 constituye una cláusula general, pues, como se advirtió, paradójicamente el legislador no exige que el *'intruso'* actúe bajo el influjo de elementos subjetivos especiales orientados a obtener datos informáticos, dañar, lucrarse o interferir el sistema al que se ha conectado. Con lo cual se promueve jurídicamente, en principio, la sanción penal de una serie de comportamientos de intrusismo directo *inofensivo* que normalmente no deberían castigarse por la vía penal *—pero sí administrativa—*; como sucede con el denominado "*hacking blanco o Joyriding*"[42], en el cual el intruso carece de intención de lesionar, lucrarse o causar daño en provecho propio o de terceros, dado que despliega la conducta con el fin de ocupar la red por curiosidad o desafío intelectual, a la par que señala la insuficiencia de las medidas de seguridad que posee el sistema. Ello, con independencia de la responsabilidad que se pueda derivar de los hechos, como consecuencia de los daños causados al hacer obsoletas las medidas de seguridad previamente dispuestas por el titular del sistema, al bloquear los sistemas o generar borrados accidentales en los datos o información informatizada contenida en los medios.

No obstante, parte de la doctrina moderna[43] justifica dicha penalización extensiva *—y la consecuente restricción de derechos fundamentales—*, al argumentar que el sólo

41 En la misma línea, vid. Castro Ospina: ob. cit., http:/www.delitosinformáticos.com/delitos/colombia3.shtml.

42 Sobre el particular, Matellanes: ob. cit., pág. 133, indica el perfil criminológico de dichos personajes.

43 Vid. Rovira del Canto: ob. cit., pág. 196 y ss., quien indica que dicha conducta entraña la producción de un perjuicio de peligro de los intereses económico-patrimoniales contenidos en los programas o en los datos a los que tiene acceso o la pérdida de esfuerzo o costo que la

ingreso al sistema informático constituye, por sí mismo, un grave peligro potencial que amenaza la seguridad del sistema y la fiabilidad de la información contenida en el mismo. Según afirman, el 'intruso' directo o blanco sí obtiene una ventaja personal, al adquirir los conocimientos necesarios para perfeccionar su técnica intrusiva. Plus de conocimiento que probablemente será empleado para realizar actos posteriores de '*craking malicioso*' (prognosis de peligrosidad contraria al principio de culpabilidad).

En realidad, la legitimidad del castigo penal a dichas conductas alternativas es una cuestión polémica en la doctrina, al menos, tal y como se han estructurado en la legislación vigente. Y ello es así, porque lo que se castiga finalmente –*anticipación de la barrera de intervención penal*– son verdaderas actividades preparatorias o preeliminares de infracción a la seguridad y el control, de una conducta posterior que se presume como '*cracking malicioso*', la que también se presume dirigida a causar un peligro[44] a la intimidad individual, la reserva y la garantía de no interceptación de comunicaciones privadas. Penalidad que sólo encuentra justificación en la protección del interés autónomo de la gestión de seguridad colectiva o individual de datos e informaciones; interés jurídico muy distinto al bien jurídico personalísimo tutelado en concreto, que legitima y fundamenta el correspondiente tipo penal[45] (libertad-intimidad).

No otra cosa se deduce de esta modalidad de tipificación de delitos de peligro en abstracto[46]. Categoría por virtud de la cual el legislador pretende una construcción

---

ha supuesto al titular establecer medidas de seguridad. Sin embargo, es menester recordar que no toda interpretación admisible se traduce en mecanismos de tipificación adecuados desde el punto de vista de las garantías constitucionales. Con lo cual deben ser analizados cuidadosamente los límites de constitucionalización del Derecho penal, por lo que respecta a la protección de los bienes jurídicos y su fundamento material como elementos que también pueden constituir bienes jurídicos.

44 Sobre el concepto más general de peligro, cfr. Quintero Olivares, Gonzalo/Morales Prats, Fermín/Prats Canut, José Miguel: Manual de Derecho penal, Parte general, 3ª ed., Navarra, Aranzadi, 2002, pág. 333, indica:"la noción más extendida llama peligro, en lo jurídico-penal, a la posibilidad relevante de que un resultado se produzca como consecuencia normal de un determinado acto o situación". De igual manera, Cfr. Cuello Contreras, Joaquín: El derecho penal español, Parte general, 3ª ed., Madrid, Dykinson, 2002, pág. 527 y ss.

45 Sobre el tema de la legitimidad cfr. Gómez Martín,Víctor: El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (Art. 270, Párr. 3° CP.), en: RECPC 04-16.pdf. (2002), Pág. 16: 24 pdf. Y ss. En: http://criminet.ugr.es/recpc/recpc04-16.pdf; También, Díez Ripollés: ob. cit., pág. 01: 24 pdf.

46 Sobre el concepto específico de delito de peligro en abstracto cfr. Berdugo Gómez de La Torre, Ignacio/ Arroyo Zapatero, Luis/ García Rivas, Nicolás/ Ferré Olivé, Juan Carlos/ Serrano Piedecasas, José Ramón: Lecciones de Derecho penal, Parte general, 2ª ed., Sl.: La Ley, 1999, pág. 156; Luzón Peña, Diego Manuel: Curso de Derecho penal, Parte general I, Madrid, Universitas, 1999, pág. 314; Zugaldía Espinar, José M. (Dir.) AA.VV.: Derecho penal, Parte general, Valencia,

menos formalizada, estricta y ligera de las infracciones penales, al no imponerles una específica "*forma de ser normativa*"[47] que impida limitar —*en sentido extrasistemático*— el ejercicio del *ius puniendi* del Estado, a través de los principios generales de proporcionalidad, ultima ratio y mínima intervención punitiva.

Según lo dicho, se trata de conductas preparatorias que —*difícilmente*— satisfacen los requerimientos del principio constitucional de lesividad (CP. art. 11[48]); precisamente, porque éste postulado fundamental demanda un comportamiento que genere de forma positiva —*mas que un simple estado de peligro presunto*— un estado de peligro efectivo para el bien jurídico[49], entendido como un contenido típico material más preciso (*real y próximo de necesaria verificación*) desde la perspectiva del *desvalor de resultado*; o al menos la posibilidad de admitir como prueba de inocencia la inexistencia de un peligro en el caso concreto[50]. Resultado en sentido jurídico contra la intimi-

---

Tirant Lo Blanch, 2002, pág. 398 y ss.; Muñoz Conde, Francisco Y García Arán, Mercedes: Derecho penal, Parte general, 5ª ed., Valencia, Tirant lo blanch, 2002, pág. 305 y ss.; Jescheck, Hans-Heinrich Y Weigend, Thomas: Tratado de Derecho penal, Parte general, Trad. de Miguel Olmedo Cardenete, 5ª ed., Granada, Comares, 2002, pág. 283 y Cuello Contreras: ob. cit., pág. 522, al advertir que: "aquí el peligro aparece sólo como el motivo que lleva al legislador a prohibir un comportamiento, si bien la tipicidad se cumple plenamente con la realización de la acción prohibida, no habiendo necesidad de constatar peligro alguno para el bien jurídico como resultado de tal actividad (prohibida en sí misma)".

47 Cfr. Quintero/Morales/Prats: ob. cit., pág. 334, cuando indican que: "los delitos de peligro concreto tienen expresamente establecida en el tipo la necesidad de que se haya provocado una situación de peligro (resultado de peligro)…".

48 Sobre la vulneración del principio de lesividad a través de los delitos de peligro en abstracto, cfr. Gracia Martín, Luis: Prolegómenos para la lucha por la modernización y expansión del Derecho penal y para la crítica del discurso de resistencia, Valencia, Tirant lo Blanch, 2003, pág. 137, cuando examina la crítica a la expansión penal, que por supuesto no comparte: "Ciertamente, los tipos de peligro abstracto se orientan a la protección de la seguridad de los bienes jurídicos individuales. Sin embargo, la capacidad abstracta-general de afectar a la seguridad y, con ello, a remotos bienes jurídicos fundamentales, puede ser afirmada de cualquier conducta, por muy inocua que sea en el caso concreto. El tipo de peligro abstracto será entonces uno carente de límites, pues podrá estimarse comprendida en él cualquier conducta con tal que muestre elementos de contrariedad al vago y abierto concepto de la "seguridad" o al "interés general" de protección de bienes jurídicos". De opinión contraria, Rodríguez Gómez: ob. cit., pág. 143. Dicho art. 11 indica: "para que una conducta típica sea punible (sic.) se requiere que lesione o ponga efectivamente en peligro, sin justa causa, el bien jurídicamente tutelado por la ley penal".

49 En relación con la función del bien jurídico y los principios de proporcionalidad y última ratio frente a bienes jurídicos colectivos, véase a Hirsch, Hans Joachim: Acerca del estado actual de la discusión sobre el concepto de bien jurídico, Trad. de Daniel Pastor, en: modernas tendencias en la ciencia del Derecho penal y en la Criminología, Actas y congresos, Madrid, UNED, 2001, págs. 378 -379.

50 Vid. Zugaldía Espinar Y AA.VV.: ob. cit., pág. 400. Más adelante indica en la pág. 482, que "en el fondo, como todo el problema reside en la presunción iuris et de iure de la peligrosidad de la acción, la objeción podría superarse sencillamente si se admitiera la prueba en contrario del

dad, que no parece satisfecho –*plenamente*– con el simple acceso del *intruso,* sin que dicha conducta esté acompañada de otras actuaciones y finalidades ilícitas que indiquen –*objetivamente– el peligro en la órbita que cada persona se ha reservado'*; como se ha dicho, más allá de la simple motivación de superar –*por superar*– las medidas de seguridad electrónicas dispuestas.

Como ejemplo de dichas intromisiones lesivas se pueden mencionar el "*sacavenging*", "*trashing*" o "*diving*", ello es, escarbar basura electrónica con el propósito de buscar y obtener información confidencial de los usuarios que sea de utilidad para sí o para un tercero, como: *passwords*, números de tarjetas de crédito y debito, e información personal, etc. En la misma línea se encuentra la conducta de '*data didlig*' aunque ella supone modificar programas de ordenador para sustraer la información; así como la instalación de *troyanos*[51] *o* usar "*desencriptadores de claves*"; programas de grabación o de clonación para un acceso posterior con la finalidad de adulterar contenidos o identidades personales (*falsedad en documentos, falsedad personal, apropiación de identidades, etc.*); entre otras conductas, como el '*Zapping*' o '*Superzapping*'.

Desde luego, se debe reconocer la dificultad para demostrar –*con certeza*– que el sujeto ha accedido al sistema con ánimo de lucro o de causar daños en el medio; lo que explica –*aunque no legitima ni justifica todavía desde la perspectiva político-criminal*– la anticipación de la intervención punitiva a la mera protección de la seguridad de un sistema de almacenamiento, procesamiento o transmisión de datos o información automatizada, restringiendo la libertad, el patrimonio económico u otros derechos de libertad[52]. Dicho lo cual, en este delito se advierte una exigencia progresiva de objetivización de los elementos subjetivos del tipo, situación que dificulta la protección de categorías

---

peligro representado por la acción (que la acción típica es una acción peligrosa constituiría una prueba iuris tantum, no iuris et de iure. De esta forma podría excluirse la tipicidad en los casos en los que la acción no hubiese representado en modo alguno un peligro para el bien jurídico protegido, esto es, en los casos en los que falte, sin más, la acción peligrosa misma. Esta es una vía para "desformalizar" los delitos de peligro abstracto y otorgarles un contenido material…".

51 Explica este dispositivo Gómez Martín: ob. cit., pág. 35, al indicar que: "existe un programa informático, denominado comúnmente "Caballo de Troya", cuya única finalidad consiste en conseguir facilitar la información que se encuentra asociada a un determinado sistema informático, por ejemplo, la relativa al "login" y al "password" del usuario. El funcionamiento del "Caballo de Troya" es el siguiente: el "cracker" deja el programa en el sistema informático preparado para ser ejecutado cuando alguien acceda a él, ejecutándose en lugar del proceso de "login" e imitando la pantalla verdadera. El usuario, que no advierte nada extraño, teclea como siempre el "login" y el "password", pero estos no son comprobados, sino que se guardan en un archivo de texto y se simula un "password incorrecto". En este momento, el "Caballo de Troya" llama al proceso de "login" y "password" real y el usuario, al creer haber marcado incorrectamente el "login" y el "password", vuelva a intentarlo, consiguiendo en esta ocasión acceder al sistema y no dando la menor importancia a lo ocurrido. Como consecuencia de todo ello, el "login" y el "password" habrán pasado a un archivo de texto propiedad del "cracker".

52 Cfr. Poullet: ob. cit., pág. 782.

garantistas al momento de su aplicación. Por supuesto, no se olvide que se podrían desplegar medidas alternativas de naturaleza administrativa para esta clase de comportamientos, de acuerdo con el carácter de *última ratio* del Derecho penal[53].

En síntesis, todo indica que estas modalidades delictivas de intrusión o permanencia ilícita, precisamente por la estructura de peligro que poseen y por el adelantamiento de la barrera de protección que comportan, no encuadran cabalmente en la protección del bien jurídico libertad personal, sino más bien en la protección del interés jurídico autónomo '*seguridad colectiva o pública de la información*'; sin perjuicio de que dichos comportamientos vulneren de forma accesoria a la intimidad personal, a la reserva e interceptación de comunicaciones privadas *(y con ello a la libertad, la dignidad y el libre desarrollo de la personalidad*), cuando efectivamente representen un peligro concreto o próximo para los sujetos pasivos.

B. El espionaje informático. Por tal modalidad criminal deben entenderse aquellas actividades dirigidas a obtener, captar y desarrollar sin autorización datos, comunicaciones, programas, licencias, imágenes y sonidos almacenados en ficheros o bases de datos públicos o privados, donde se acumula y procesa información confidencial, exclusiva y valiosa protegida. Sobre el particular, los supuestos se deben diferenciar por virtud de la protección penal que se otorga a los distintos bienes jurídicos involucrados: *la intimidad, el orden económico social y la seguridad del Estado*.

1. En este orden de ideas, si la obtención abusiva o la divulgación de comunicaciones, documentos electrónicos, ficheros médicos, psiquiátricos o profesionales, e-mails, fotografías, información en bases de datos, etc., conlleva una intromisión en la esfera privada del sujeto que vulnera el bien jurídico intimidad personal, mediante el uso de medios informáticos o telemáticos; entonces, tales conductas serán castigadas mediante los tipos penales dispuestos para proteger la intimidad, garantizar la no interceptación de comunicaciones y la divulgación de secretos. Ello, con independencia de que dicha conducta constituya al tiempo un delito de acceso abusivo a un sistema informático protegido con medida de seguridad.

De este modo, el Código Penal colombiano (Ley 599/2000) protege en los arts. 192 y ss., la intimidad personal, la inviolabilidad de las comunicaciones y los datos reservados. **a)** Precisamente, el art. 192, inc. 1°, mod. L.890/2004, art. 14, sanciona la interceptación ilícita de comunicaciones en las modalidades de sustracción ('*Dowling*'), interceptación, control ilícito y conocimiento indebido doloso de comunicaciones

53 Vid. Silva Sánchez: ob. cit., pág. 20; Gracia Martín: ob. cit., pág. 141, sobre la posición que critica la expansión penal indica: "A la vista, pues, de la ausencia total de elementos de lesividad, e incluso de peligrosidad general, en los hechos individuales aislados, no es admisible, ni legítimo, extender a los mismos la amenaza de una sanción penal. Estos hechos debieran ser monopolio del Derecho administrativo sancionador en virtud de la diferencia cualitativa, y no simplemente cuantitativa, que es preciso reconocer entre lo ilícito penal y lo ilícito administrativo. Su criminalización implicaría, pues, una administrativización del Derecho penal".

privadas dirigidas a otra persona, sea del caso vía Web (*correo electrónico o de otra forma*) o por la conducta de '*Wiretapping*' (interceptación de líneas telefónicas o telemáticas), con una pena de prisión de uno a tres años, *siempre que la conducta no sea sancionada con pena mayor*[54]. El artículo es en realidad insuficiente con relación al tema que se trata, pues carece de las distinciones legales necesarias para graduar de manera adecuada el injusto de la conducta y con ello la pena imponible. Por lo demás, el tipo referido no contempla la conducta de procurarse datos[55] para sí o para un tercero que, además de no ser perceptibles, son reservados y protegidos contra accesos indebidos. No se puede olvidar que el art. 195 ha adelantado la barrera de protección penal al mero acceso abusivo al sistema.

De otro lado, en primer lugar, dicho tipo penal no distingue la punibilidad entre los sujetos comunes (outsider) y los sujetos responsables (*insider*) del procesamiento, integridad, reserva y transmisión de dichas comunicaciones. Como es evidente, la segunda categoría de sujetos debería responder con una pena superior que la pena imponible a los primeros, atendida su responsabilidad funcional y la confianza depositada por el titular en ellos. Adicionalmente, no se considera que los sujetos que interceptan las comunicaciones pueden ostentar la calidad de servidores públicos (*con ocasión de un proceso judicial*[56]*, o de actividades de inteligencia militar o judicial, etc.*),

54 Art. 192, inc. 1°: "El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido. Incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya otro delito sancionado con pena mayor. (Ley 890/2004, art. 14). Por su parte, el CP. español, como ya se dijo, castiga dichas modalidades de conducta en el art. 197.1, 2, 4 (agravante si el sujeto es insider), 5 (agravante por afectar datos personalísimos —especialmente protegidos por la Constitución española, art. 18.4- como la religión, la salud, la vida sexual, etc. o si se afectan menores de edad o incapaces), y 6 (agravante por ánimo de lucro), 198, 199, 200 y 201, desplegando toda una casuística que abarca los distintos escenarios posibles en la materia. Así mismo, será un tipo modificado (art. 197.6, apt. 2), si se realiza con ánimo de lucro o se afectan menores de edad o incapaces. Por su parte, el StGB. Alemán en el § 202a, considera como delito el espionaje de datos protegidos; el CP. italiano, arts. 616 y 617 (cuarto y quinto), prevé respectivamente los delitos de violación de la correspondencia electrónica e interceptación abusiva de comunicaciones. De otro lado, dicha conducta tiene referente internacional en la Convención de Budapest del 23.22.2001, ob. cit., Cap. II, Sección 1, art. 3°: "Interceptación ilegal", y también en la ley 19223 de 1993 de Chile, art. 2, que consagra como delito la interceptación o interferencia, con ánimo de usar o conocer de forma indebida la información contenida en un sistema de tratamiento de información.

55 Cfr. Márquez Escobar, Carlos Pablo: El delito informático, la información y la comunicación en la esfera penal, conforme con el nuevo código penal, Bogotá, Leyer, S. F., pág. 22, indica que: "De esta manera pues, el proceso de comunicación contiene el proceso de información, pero se diferencia de aquél en que hay una transmisión de respuesta a la información enviada, de modo que se da un proceso de alimentación externa de los datos enviados".

56 En este sentido, el CP. español contempla dicha posibilidad en el art. 536, cuando una autoridad, funcionario público o agente que intercepte telecomunicaciones privadas, imágenes

empleados laborales y profesionales al servicio del sujeto afectado (*sea este persona natural o jurídica*), lo que debería agravar también la conducta referida.

En segundo lugar, el tipo penal resulta genérico, pues no sólo no desagrega los distintos tipos de servicios prestados por plataformas informáticas o telemáticas susceptibles de ser interceptados (correos electrónicos, comunicaciones vía Messenger, comunicaciones telefónicas comunes, etc.), con lo cual se comprende cualquier clasificación posible; sino que tampoco especifica los espacios para realizar la interceptación, sustracción o destrucción de la información, lo que permite incluir los medios informáticos en los que normalmente se desarrollan este tipo de actividades intrusivas, es decir: los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros donde se encuentren almacenadas dichas comunicaciones.

b) A su turno, el art. 192, inc. 2°, castiga las conductas de revelación o divulgación del contenido de las comunicaciones interceptadas —*por la red o por cualquier otra vía informática o telemática; o de comunicaciones almacenadas en sistemas de tratamiento de información*—; y el empleo en provecho propio o ajeno de la información confidencial contenida en las comunicaciones con perjuicio de terceros, con una pena de dos a cuatro años de prisión (L. 890/2004, art. 14)[57]. Desde luego, también ignora el empleo en provecho propio de datos en sentido estricto.

---

o cualquier señal de comunicación, o utilice artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, en sede de un proceso judicial y con violación de las garantías constitucionales. Conducta sancionada con una pena de inhabilitación especial de dos a seis años. A su turno, será aplicable el art. 198, cuando la obtención de documentos (imágenes, correo electrónico, documentos electrónicos, etc.) y/o su revelación son realizadas en la Web o en bases de datos informáticas por servidores públicos que se prevalen de su cargo, sin que medie causa judicial.

57 El CP. español consagra dicha conducta en el art. 197.3, cuando sea realizada por un sujeto 'outsider', así: "se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores", es decir, los numerales 1 y 2 del art. 197 referidos a documentos en sentido lato y a datos reservados de naturaleza personal o familiar registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo o registro público o privado. Conducta que será agravada por el numeral (4) si la conducta es realizada por un sujeto 'insider', (5) si se afectan datos de carácter personal que revelen la ideología, la religión, creencias, salud, origen racial o vida sexual—especialmente protegidos por la Constitución española, art. 18.4- o si se afectan menores de edad o incapaces, y (6) cuando la conducta se realice con ánimo de lucro. Así mismo, será un tipo modificado (art. 197.6, apt. 2), si con ánimo de lucro se afectan menores de edad o incapaces. Asimismo, el CP. español, art. 536, apt. 2°, agrava la conducta de interceptación de comunicaciones realizadas por un servidor público, con ocasión de un proceso judicial y violación de las garantías constitucionales. Por su parte, la Ley 19223 de 1993 de Chile, art. 4°, consagra como delito la revelación o difusión maliciosa de datos contenidos en un sistema de información. Conducta que será agravada si se trata de un sujeto 'insider'.

c) Ahora bien, si se trata de la divulgación o empleo en la Web o medios de comunicación asimilados, con ánimo de lucro personal o para un tercero, de información contenida en documentos (*incluyendo los e-mail, cartas digitalizadas, fotografías, documentos personales o de trabajo, etc.*) reservados (art. 194, mod. L. 890/2004, art. 14), se impondrá una pena de multa progresiva en su modalidad de unidad multa (CP. col., art. 37), siempre y cuando la conducta no sea sancionada como un delito con pena mayor *(subsidiaridad expresa)*. Por lo demás, la divulgación y el empleo de documentos reservados suponen —*de manera usual*— la realización de una conducta punible previa, consistente en la sustracción y el apoderamiento de los documentos reservados que, como es evidente, no resulta incluida por el art. 192.

En cualquier caso, el tipo no logra satisfacer la necesidades político-criminales sobre la protección de la intimidad privada, no solo por la levedad de la sanción finalmente imponible al autor (multa progresiva en sus diversos grados -art. 39 CP.) bajo el verdadero contexto de la gravedad de la infracción y atendidas las posibles consecuencias para el titular del bien jurídico en todos los órdenes; sino porque asimila de forma inadecuada la importancia de los contenidos de los documentos que '*deben permanecer en reserva*'. Y ello es así, pues no todos se referirán de modo expreso a datos comunes secretos, sino que muchos tendrán la naturaleza de documentos —*en sentido lato*— de carácter personalísimo sobre la ideología, la religión, las creencias, la salud, el origen racial o la vida sexual de un sujeto determinado. Contenidos que —*sin duda alguna*— deben ser protegidos con mayor rigor desde el punto de vista jurídico penal (Const. Pol., art. 15).

Del mismo modo, el tipo analizado asimila —*de manera inadecuada*— el tratamiento jurídico de los sujetos protegidos. En efecto, no es lo mismo revelar o divulgar información sobre un sujeto mayor de edad que información relativa a un menor de edad o un incapaz que se encuentre en situación de indefensión frente a dichas actividades. Por lo que concierne al sujeto activo, el tipo penal puede ser realizado por un sujeto común ('el que'), con lo cual no se distingue punitivamente la conducta de un particular y la conducta de divulgación o revelación cuando sea realizada por un servidor público que abusa de su cargo o sus funciones.

2. De otro lado, si la obtención de datos reservados o confidenciales almacenados o tratados en sistemas informáticos concierne a *secretos o descubrimientos industriales*[58],

58 Indica Matellanes: ob. cit., pág. 143, que por secreto industrial se entiende: "toda información relativa a la industria o empresa que conocen un número reducido de personas y que por su importancia económica el titular desea mantener oculta. Dentro del mismo se incluyen tanto los relativos a los aspectos industriales (procedimientos de fabricación, mantenimiento, suministros, proveedores, costos, etc.), como comerciales (listas de clientes, tarifas, descuentos, publicidad, proyectos de expansión, etc.) y en general, los relativos a la organización interna de la empresa, cuyo conocimiento pueda afectar a su capacidad de competir". Vid. Decisión 486 de 2000 (Comunidad Andina de Naciones) y Ley 75 de 1990, art. 45, sobre información privilegiada.

comerciales o científicos, procesos o aplicaciones de una empresa pública o privada, o información privilegiada de movimientos de bolsa que confieran al *intruso* una posición de privilegio en las relaciones de tráfico económico (insider information), se aplicará el art. 308 (L. 890/2004, art. 14), que regula especialmente la *Violación de reserva industrial o comercial* (insider trading), del siguiente modo:

a) El que emplee o divulgue —*vía Web o de cualquier otra manera*— información científica, proceso o aplicación industrial, llegados a su conocimiento por razón de su cargo (*insider*), oficio o profesión y que deban permanecer en reserva, será sancionado con una pena de prisión de dos a cinco años y multa de veinte a dos mil salarios mínimos mensuales legales (L. 890/2004, art. 14).

b) Será castigado con la misma pena el que de forma indebida conozca, copie u obtenga secreto relacionado con descubrimiento, invención científica, proceso o aplicación industrial o comercial, haciendo uso de recursos informáticos, como sucedería cuando se propician las fugas de datos (*Data Leakage*) o se generan puertas falsas (*Trap Doors*) para obtener accesos no previstos en las funciones básicas de los programas y así obtener la información confidencial. Hipótesis que no comprenden el apoderamiento de 'objetos originarios' en los que se materializa el secreto, pues ésta será una hipótesis ordinaria de hurto.

c) Si los sujetos outsider o insider obtienen provecho propio o para terceros, la pena será de tres a siete años de prisión y multa de cien a tres mil salarios[59] (ajustada L. 890/2004, art. 14). Como es de suponer, para considerar la información como un secreto industrial, esta deberá constar en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros elementos similares.

Lo anterior, sin perjuicio de la tipificación de otras infracciones a los derechos que la ley reconoce al autor de una obra (*copyright*), como por ejemplo: la violación a los derechos morales de autor (art. 270), la defraudación a los derechos patrimoniales de autor (art. 271) y la violación a los mecanismos de protección de los derechos patrimoniales de autor.

59 El CP. español, en el art. 278.1 relativo a los delitos contra el mercado y los consumidores, sanciona el apoderamiento de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos con el propósito de descubrir secretos de empresa por medio de la Red o haciendo uso de instrumentos informáticos, con una pena de prisión de dos a cuatro años. b) Si para los mismos efectos se utilizan los mecanismos señalados en el art. 197.1, el agente será sancionado con una pena igual. c) Si se difunden, revelan o ceden los secretos descubiertos por el hacker (art. 278.2), la pena será de tres a cinco años y multa de veinticuatro meses. d) El art. 279.2 agrava la pena en su mitad superior, tanto si la información se utiliza en provecho económico propio, como cuando se utiliza información privilegiada de bolsa para adquirir acciones a título personal.

3. Finalmente, si con dicha conducta punible se obtiene y/o revela información o datos que puedan afectar *la seguridad nacional, la justicia o la inteligencia nacional*, se aplicarán las siguientes disposiciones[60]:

a) El art. 196 mod. L. 890/2004, art. 14, sanciona la conducta de violación ilícita de comunicaciones o correspondencia de carácter oficial, en el sentido de sustraer, ocultar, extraviar, interceptar, controlar o impedir de modo ilícito las comunicaciones o correspondencias de carácter oficial, sea del caso por medios informáticos. La conducta será agravada (inc. 2°) si las comunicaciones o la correspondencia está destinada o remitida a la rama judicial, a los organismos de control o de seguridad del Estado. Cuando el sujeto insider (servidor público) sólo revele documentos (electrónicos) reservados o secretos se aplicará el art. 418. Si el servidor público utiliza en provecho propio o ajeno descubrimiento científico, u otra información o datos secretos o reservados llegados a su conocimiento por razón de sus funciones, se aplicará el art. 419.

b) Si el intruso *obtiene de modo indebido información*, por medio de instrumentos informáticos o por virtud del acceso ilegal a sistemas informáticos nacionales, o *emplea o revela* en la Web secreto político, económico o militar relacionado con la seguridad del Estado colombiano, se aplicará en sentido estricto el delito de *espionaje* consagrado en el art. 463 mod. L. 890/2004, art. 14. Tipo penal que protege el bien jurídico '*Seguridad del Estado*'[61].

Ello, sin perjuicio de aplicar otras infracciones dirigidas a menoscabar la libertad o la autonomía personal, como, por ejemplo: el constreñimiento ilegal (art. 182), cuando, para obtener información sensible para la víctima o información de terceros, se constriñe a su titular o tenedor legítimo.

---

60 Desde luego, algunos autores afirman que el bien jurídico 'seguridad de las funciones informáticas' es un interés de la comunidad, que no incluye los intereses del Estado. Cfr. Castro Ospina: ob. cit., http:/ www.delitosinformáticos.com/delitos/colombia2.shtml.

61 El CP. español consagra las siguientes disposiciones: a) El que se procure información legalmente calificada como reservada o secreta, relacionada con la seguridad nacional o la defensa nacional, o relativa a los medios técnicos o sistemas empleados por las fuerzas armadas o las industrias de interés militar, será castigado con pena de prisión de uno a cuatro años (art. 598). Pena que se agravará en su mitad superior (art. 599.1°), si quien realiza la conducta (insider) fuera depositario o tuviere conocimiento del secreto por razón y con ocasión de su cargo o destino. O si el secreto (referido a la seguridad nacional) se publica en un medio de comunicación social asegurando la difusión del mismo (art. 599.2°). b) Si se reprodujeren vía Web planos o documentos relacionados con zonas, instalaciones o materiales militares de acceso restringido o calificados como información reservada (art. 600.1), el sujeto activo será sancionado con una pena de seis meses a tres años. c) Si se tratare de información o correspondencia reservada o secreta, relacionada con la energía nuclear (art. 602), dicha conducta se sancionará con pena de prisión de seis meses a tres años; salvo que el hecho no sea sancionado con otra pena diferente (más grave).

C. El sabotaje informático o 'Mischief'. Esta modalidad delictiva abarca las conductas dirigidas a interferir, obstaculizar, dañar, inutilizar, alterar o suprimir el servicio de: i) los sistemas informáticos o de redes de comunicación pública de datos, o equipos informáticos o telemáticos; ii) bases de datos, datos específicos, informaciones necesarias, comunicaciones o documentos electrónicos que tengan valor económico; iii) las funciones de procesamiento, tratamiento y transmisión; siempre que dichos elementos sean necesarios para el adecuado funcionamiento de sistemas como, por ejemplo: el comercio electrónico, terminales aéreas, sistemas bancarios o industriales, etc. Conductas que pueden ser realizadas no solo por medio de borrados tradicionales (crash programs), sino también mediante software especializado como virus, Cancer routines, bombas lógicas, '*electronic-mail bombing*' o '*spam*' etc.[62].

Es necesario advertir que el ordenamiento colombiano carece de una fórmula especial que incluya las distintas hipótesis de sabotaje informático en 'sentido estricto', de tal suerte que su tipificación dependerá, en cada caso concreto, de la conducta efectivamente realizada y del objeto sobre el cual recae la acción:

a) Así las cosas, si se trata de daño, perturbación, inutilización o destrucción material o funcional del *Hardware* utilizando medios informáticos, telemáticos o programas como bombas lógicas; o de otros elementos que puedan ser considerados bienes muebles informáticos (en todo caso distintos a aquellos objetos lógicos como

62 El CP. español castiga el daño informático en el art. 264.2 (Delitos patrimoniales relativos al delito de daños en bien ajeno (Capítulo IX, «De los Daños», del Título XIII «Delitos contra el patrimonio y contra el orden socioeconómico» del Libro II). De tal suerte que se impone una pena de prisión de uno a tres años y multa al sujeto que "por cualquier medio destruya, altere, inutilice, o de cualquier otro modo dañe los datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informático" (Negativa o degradación de servicio). Mientras que la destrucción o inutilización de los equipos materiales tangibles quedaría cobijada por la modalidad básica de daño prevista en los arts. 263 y 264.1, a condición de que dicho daño no esté previsto en otros títulos del CP. español. Tipo penal que es susceptible de varias críticas. Primero. El verbo rector alterar implica sancionar como daño algunas conductas que -en sentido estricto- carecen de dicha significación. Con lo cual se castigan hechos que no se compadecen con la ratio de protección del supuesto de hecho penal. Segundo. cuando se 'dañan, inutilizan, destruyen o alteran' documentos electrónicos se dañan datos, dicho lo cual, los objetos sobre los cuales podría recaer la acción delictiva se repiten. Tercero. Según lo dicho, en sentido estricto las redes no contienen datos electrónicos, como quiera que son las vías electrónicas idóneas para transmitirlos. Por supuesto, la anterior disposición se aplica (subsidiariedad expresa) sin perjuicio de la preferencia por especialidad de otras normas frente a supuestos de sabotaje político o terrorismo en los que se destruya información del Estado, como ocurre en las hipótesis vertidas en el art. 603, que castiga con una pena de tres a seis años de prisión, la destrucción e inutilización de la correspondencia o documentación (también electrónica o telemática) reservada o secreta, relacionada con la defensa nacional española. Cfr. Corcoy Bidasolo, Mirentxu: Protección penal del sabotaje informático. Especial consideración de los delitos de daños, en: Delincuencia informática, compendio, IURA-7, Barcelona, PPU, 1992, pág. 154 y ss.; Möhrenschlager: El Nuevo Derecho penal…, ob. cit., pág. 139 y ss.; Romeo Casabona: Poder informático…, ob. cit., pág. 175 y ss.

datos, *documentos electrónicos o software* protegidos de forma especial por los delitos contra la propiedad intelectual o industrial, los delitos contra la intimidad o tipos especiales que se llegaran a crear), dicha conducta quedará cubierta por el tipo penal vertido en el art. 265[63] mod. L. 890/2004, art. 14. A su turno, dicha conducta será agravada por el art. 266, num. 4 mod. L. 890/2004, art. 14, cuando el daño recaiga sobre bienes u objetos materiales (informáticos) que revistan interés científico, histórico, asistencial, educativo, cultural, artístico, de uso público, de utilidad social o sobre bienes que conforman el patrimonio cultural de la nación. Desde luego, estos comportamientos no constituyen delitos informáticos en sentido estricto, sino conductas asociadas con la informática.

En general, la doctrina ha criticado esta disposición normativa, pues en materia informática las distintas modalidades de conducta alternativa consagradas como verbos rectores del delito de daño en bien ajeno, pueden comportar —*en concreto*— conductas que entrañen desde la irreparabilidad del objeto material sobre el cual recae la acción —*y con ello la vulneración o el peligro para el bien jurídico patrimonio económico*—, hasta conductas que impliquen daños aparentes o insignificantes que pueden ser solucionados con base en conocimientos básicos de programación. De este modo, según la expresión genérica: '*de cualquier otro modo dañe*: una simple variación dolosa de la configuración de los equipos o programas que componen el sistema informático podría —*de cara al sujeto pasivo*— comportar la inutilidad transitoria de la unidad informática (computador), atendidos los servicios útiles dispuestos por su poseedor. En consecuencia, todo indica que los diversos verbos rectores comportan distintos grados de desvalor de acción, de resultado y de necesidad de pena, que no resultan equivalentes en la individualización de la sanción, no empero contar con la misma incidencia estructural en la configuración del tipo penal analizado[64].

63 Art. 265. Daño en bien ajeno. El que destruya, inutilice, haga desaparecer o de cualquier otro modo dañe bien ajeno, mueble o inmueble incurrirá en prisión de uno (01) a cinco (05) años y multa de cinco (05) a veinticinco (25) salarios mínimos mensuales legales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor.| La pena será de uno (01) a dos (02) años de prisión y multa hasta de (10) salarios mínimos legales mensuales vigentes, cuando el monto del daño no exceda de diez (10) salarios mínimos legales mensuales vigentes. Sobre el particular, cfr. Márquez Escobar: El delito informático…, ob. cit., pág. 202 y ss.

64 En efecto, de cara al principio de lesividad (art. 11 CP.) no resulta lo mismo destruir un sistema informático que inutilizarlo. Por lo que concierne al desvalor de acción, tampoco parece adecuado afirmar —a priori— una mayor gravedad del delito cuando el daño (destrucción, inutilización, desaparecimiento o daño de cualquier otro modo) sea realizado por medio de la fuerza física que por la violencia informática; entre otras cosas, porque no es cierto que la segunda modalidad (la informática) constituya un forma menos peligrosa de lesionar o colocar en peligro el bien jurídico tutelado en comparación con la primera, y porque el criterio para graduar el desvalor de acción no depende exclusivamente de la mayor o menor cantidad de movimientos corporales naturalísticos que realice el agente con dolo de dañar los bienes protegidos. De este modo, con un simple 'click' se puede realizar una conducta más lesiva de

De igual modo, la doctrina es consecuente al afirmar que no todas las conductas constitutivas de 'sabotaje informático', pueden ser tipificadas en la descripción del delito de daño en bien ajeno. Y ello es así, pues los objetos lógicos no son bienes muebles o inmuebles en sentido estricto. De ello se desprende que el daño de bienes inmateriales, o requiere una reformulación del tipo referido, atendida la prohibición de la analogía derivada del principio de legalidad (C.P., art. 6°), o debe ser regulado de forma independiente —*incluso de forma agravada cuando se trate de sistemas, programas o datos de naturaleza oficial*—, siempre que dicha conducta no sea sancionada por las disposiciones relativas a los derechos de autor (CP., art. 270 y ss) u otras normas penales complementarias. Un buen ejemplo de normativa especial en la materia son los arts. 1° y 3° de la Ley 19223 de 1993 de Chile, que consagran como delito la destrucción o inutilización maliciosa de un sistema de tratamiento de información, sus partes o componentes; y (3°) el allanamiento, daño o destrucción de los datos contenidos en un sistema de tratamiento de información[65]. Un argumento igual puede ser utilizado para negar la tipicidad del hurto (art. 239 y ss.), por lo que concierne al apoderamiento por interceptación de elementos lógicos que no se puedan asimilar a cosas muebles o a documentos con valor económico intrínseco[66].

b) Si se trata de la destrucción de comunicaciones privadas dirigidas a otra persona, como un correo electrónico, se aplicará en algunas de sus modalidades, como ya se dijo, el art. 192 mod. L. 980/2004, art. 14. Si la correspondencia o comunicación anterior fuere oficial, o dirigida o remitida a la Rama Judicial, los órganos de control o de seguridad del Estado se aplicará el art. 196 mod. L. 980/2004, art. 14. Lo anterior, a condición de que dicha destrucción de documentos electrónicos sólo afecte la intimidad y la libertad; porque si afecta a la fe pública, en el sentido de que dicho documento privado electrónico sirve de prueba, también serán aplicables los arts. 292

inutilización que aquella producida por actividades de naturaleza física). Ello demuestra la necesidad de distinguir los diversos grados de desvalor de acción y resultado que tales verbos rectores sobrellevan, o precisar un criterio de individualización de la pena más preciso respecto de los delitos de daño en bien ajeno, sobre todo cuando su desarrollo implique utilizar medios informáticos que afecten los equipos físicos. Cfr. Möhrenschlager: El nuevo derecho penal informático en Alemania, trad. Jesús María Silva Sánchez, en: Delincuencia informática, Barcelona, PPU, 1992, pág. 107. Por el contrario, Castro Ospina: ob. cit., en: http://www.delitos informáticos.com/delitos/Colombia2.shtml, afirma que dichas conductas quedan abarcadas por el delito de daño en bien ajeno.

65 Sobre el particular, cfr. el StGB., §§ 303a, 303b, regula las conductas de alteración, borrado, supresión, inutilización o alteración de datos. De forma adicional, cfr. §§ 202ª (II), 269 y 274(I) 2. Igualmente, vid. CP. Suizo, § 144 bis (1), que sanciona la conducta de daños sobre datos informáticos; y el CP. francés, mod. Ley 92-683 de 1994, art. 323, que sanciona la conducta de suprimir o modificar fraudulentamente los datos que componen un sistema de tratamiento automatizado, entre otras conductas. A su turno, el CP italiano, art. 420, sanciona los atentados contra sistemas informáticos o telemáticos de utilidad pública.

66 Sobre dicha polémica vid. Gutiérrez Francés: ob. cit., pág. 592.

(destrucción, supresión u ocultamiento de documento público -electrónico) y 293 mods. L. 980/2004, art. 14 (destrucción, supresión u ocultamiento de documento privado -electrónico), según el caso.

c) Finalmente, el art. 199 mod. L. 980/2004, art. 14, consagra el tipo penal de ***Sabotaje* (en sentido estricto)**. Figura por virtud de la cual se castiga la conducta del '*Cracker*' que, destinada a suspender o paralizar el trabajo, destruya, inutilice, haga desaparecer o de cualquier otro modo dañe bases de datos, soportes lógicos, instalaciones o equipos sistematizados para el tratamiento automatizado de datos *—para el caso utilizando medios informáticos o telemáticos—*, entre otros objetos de valor para la actividad empresarial (conducta que no solo atenta contra la libertad de trabajo, sino que también vulnera el ejercicio empresarial y el patrimonio económico de las compañías). Como es evidente, el sabotaje puede resultar en el daño del contenido de los sistemas informáticos y asimilados, o en el daño de los equipos informáticos en sí mismos considerados; pero por vía electrónica utilizando programas dañinos u otros recursos[67].

De otro lado, dicha conducta punible debería ser agravada en aquellos casos en que se destruya información necesaria, de la cual dependa la ausencia de interferencias en los procesamientos electrónicos de datos para realizar las operaciones diarias de la compañía. Desde luego, previa advertencia de que la sola introducción de un 'virus' en el sistema, con el propósito de realizar cualquiera de los verbos rectores del tipo, implicará su amplificación a través de la figura de la tentativa (art. 27). En este sentido, usualmente carece de importancia que el sistema cuente con un filtro lógico estándar (antivirus o firewell), pues en la mayoría de los casos éstos programas resultan muy limitados al requerir la actualización constante de las listas de virus maliciosos conocidos.

Lo dicho, sin perjuicio de aplicar otros tipos penales bajo esta modalidad criminológica, como sucede, entre otros, con el delito de pánico económico (art. 302), cuando la divulgación o reproducción de información falsa o inexacta tenga lugar por medio de la Web (como sistema de información público) o cuando se manipule información almacenada. Información que pueda afectar la confianza de clientes, usuarios, inversionistas o accionistas de una institución vigilada o controlada por la Superintendencia financiera, o de un fondo de valores o en cualquier sistema de inversión colectivo legalmente constituido. De igual forma, dicha conducta será castigada si la información suministrada por medios informáticos tiene como finalidad provocar o estimular el retiro de capitales nacionales o extranjeros de Co-

67 Cfr. StGB. § 303b, consagra de manera específica la conducta de sabotaje, cuando se interfiera en el procesamiento de datos de vital importancia para los negocios, la empresa o una autoridad pública. En este sentido, la legislación alemana sanciona —en sentido concreto- la imposibilidad de disponer de los datos de forma adecuada. El CP. francés, mod. Ley 92-683 de 1994, castiga en el art. 323-2, el sabotaje de un sistema de tratamiento automatizado de datos.

lombia. En ambos casos, la pena será agravada si, como consecuencia del 'sabotaje informático en sentido lato', se produjere alguno de los resultados previstos por el sujeto al momento de realizar la conducta.

D. El fraude informático. Esta modalidad delictiva, también conocida como "*Fraud by computer manipulation*", se puede desarrollar a través de manipulaciones a los usuarios de la Internet, a los programas de funcionamiento de sistemas informáticos y telemáticos o a los contenidos de bases de datos, afectando de este modo el almacenamiento, procesamiento o transferencia de datos o información informatizada[68], el patrimonio económico o la administración pública. Buenos ejemplos de lo anterior son: el '*financial institución fraud*', que consiste en inducir a una persona en error con el propósito de realizar negocios de crédito o capital en la Web (esquemas de pirámides), o de realizar una actividad de crédito mediante fraudes de banca electrónica; el '*gamming fraud*', en el cual se solicitan dinero o valores a un sujeto, creando una falsa expectativa de ganancias que luego se incumple (apuestas y casinos on-line); el '*advance fee fraud*', los '*phony scrow services*' y las compras y ventas fraudulentas (los fraudes de boletos de avión), en los cuales el sujeto pasivo es instado a pagar abonos en dinero significativos, para recibir servicios, más dinero o mercancías que no se envían o se incumplen; los fraudes a compañías de seguros y a la hacienda pública, fraudes a la confianza que terminan en pérdidas financieras; el '*spoofing/phisching*' en los que el defraudador personifica una identidad ajena (en la Web o vía e-mail) para obtener beneficios ilícitos u obtener información confidencial de los usuarios; las conexiones a líneas con costes inflados no declarados; las manipulaciones en el pago de sueldos, facturas, subsidios; y esquemas de compañías extranjeras inversoras, etc.[69].

En realidad, desde el punto de vista dogmático, nuestro ordenamiento sólo prevé aquellos supuestos de delincuencia informática vinculados con delitos patrimoniales tradicionales, como el hurto de soportes informáticos (art. 239 y ss.), el abuso de confianza sobre objetos muebles informáticos (art. 249 y 250), o eventos ordinarios de estafa (art. 246) en los cuales se recrea la clásica "*mise in scene*" en la Web o se hace uso de artificios semejantes por correo electrónico, con el propósito de inducir en error al sujeto o mantener el ya existente en los usuarios, y obtener así un provecho

68 Cfr. Gutiérrez Francés: ob. cit., pág. 87 y ss.; Romeo Casabona: Poder informático…, ob. cit., pág. 48 y ss.; Sieber: Criminalidad…, ob. cit., pág. 16, indica que: el autor puede en un principio introducir datos falsos en el ordenador (manipulaciones del input), puede alterar el orden del proceso (manipulaciones del programa y de la consola), o bien puede posteriormente falsificar el resultado, inicialmente correcto, obtenido del ordenador (manipulaciones del output)"; Sieber, Ulrich: Documentación…, ob. cit., pág. 67 y ss.

69 Sobre el tema, vid. Cfr. Rodríguez Gómez: ob. cit., pág. 147; Javato Martín, Antonio Ma.: La tutela penal de consumidor en el comercio electrónico en el Derecho Suizo, en: RECPC 07-r2 (2005)- http://criminet.ugr.es/recpc, págs. r2: 1-6 pdf. Igualmente, cfr. http://www.obs-internet.com: los diez delitos, engaños y fraudes más frecuentes en Internet.

efectivo económico ilícito. En consecuencia, si el sujeto activo obtiene un provecho ilícito —*para sí o para un tercero*— en perjuicio ajeno, mediante la inducción o mantenimiento en error del sujeto pasivo a través de *artificios* o engaños de naturaleza informática (vía Web, correo electrónico, etc.) incurrirá en un delito de estafa tradicional. A su turno, si se tratare de rifa, juego o lotería dispuesta y manipulada de forma ilegal en la Web, o si el sujeto activo manipula alguna dispuesta legalmente en la red mediante dispositivos o programas informáticos, se aplicará la variante típica consagrada en el inc. 2° del mencionado artículo, que adicionalmente resulta una modalidad de delito masa de estafa (art. 31, parágrafo).

Sin embargo, debe recordarse que los delitos informáticos en sentido estricto implican hipótesis especiales de apoderamiento o sustracción de datos o información con ánimo de lucro genérico (hurto de tiempo informático o de servicios que impliquen erogaciones importantes para la empresa o su titular[70]) o de defraudación informática en las que no existe inducción o manteniemiento en error de una persona, sino más bien la manipulación, introducción, alteración, borrado o supresión de datos, sistemas, redes, programas, bases de datos o de los resultados del procesamiento de datos con *ánimo de lucro o de beneficio*, que conllevan una defraudación potencial no consentida a los intereses económicos de las víctimas, en provecho de los defraudadores o terceros[71]. Situaciones que no quedan cubiertas por los tipos tradicionales. La diferencia entre ambas modalidades criminales es evidente: los tipos económicos tradicionales generalmente vinculan la acción de despatrimonialización a objetos de naturaleza material, mientras que los delitos informáticos en sentido estricto vinculan la conducta con objetos de naturaleza inmaterial con repercusiones indirectas en el ámbito patrimonial[72]. Quebrar dicha diferencia para castigar como hurto, por

70 Es evidente que esta modalidad de agresión 'informática' no es susceptible de incriminación en nuestro Derecho vigente, pues el hurto de uso con ánimo de lucro, como tipo modificado atenuado (CP., art. 242.1), sólo es posible cuando el apoderamiento recae sobre 'cosas', a condición de que se restituyan en término no mayor de 24 horas. Y el tiempo informático difícilmente puede calificarse como cosa de naturaleza corporal.

71 Así el CP. español, art. 248.2 del CP, considera reos de estafa a quienes, con ánimo de lucro, y valiéndose de alguna manipulación informática o de un artificio semejante, consigan la transferencia de cualquier activo patrimonial, sin el consentimiento del sujeto pasivo y con perjuicio del mismo o de un tercero; el StGB alemán, § 236a y el CP. italiano art. 640-tercero; Gutiérrez Francés, ob. cit., pág. 114; Márquez Escobar: El delito informático…, ob. cit., pág. 185; Möhrenschlager: Tendencias…, ob. cit., pág. 53 y ss.; Romeo Casabona: Poder informático…, ob. cit., pág. 47 y ss., 64 y ss.; Sieber: Criminalidad…, ob. cit., págs. 27 y 28.

72 Así, AA.VV. Penalización…, ob. cit., pág. 26; Márquez Escobar: El delito informático…, ob. cit., pág, 176 y ss., Romeo Casabona: Poder informático…, ob. cit., pág. 53 y ss. y 147; Montano, Pedro J.: Responsabilidad penal e informática, en: www.unifr.ch/derechopenal/artículos/pdf/ montano1.pdf, pág. 5 y ss.; Rovira del Canto: ob. cit., pág. 82, caracteriza estas modalidades especiales de fraude informático, como aquellas en las cuales "la cuantía del perjuicio económico ni debe afectar la consumación delictual, ni tampoco a la existencia del delito en sí;

ejemplo, el apoderamiento de datos o información, implicaría desconocer la prohibición de construir tipos de forma analógica.

Precisamente, no se puede dejar de lado la modalidad delictiva conocida en el mundo informático como "*salami*" o "*slicing*" y en nuestro medio como "*jaleteo*", consistente en una forma de realización continuada del tipo penal, a través de la cual, el agente (*insider o outsider*) —*haciendo uso de un software especial que introduce datos u órdenes falsas o efectúa alteraciones en los programas que gestionan automáticamente transferencias bancarias o reconocimientos de créditos a favor del agente*[73]— mantiene en error operativo a la entidad, y se apropia de pequeñas cantidades de dinero, que son sustraídas automáticamente del redondeo de cifras mayores en la liquidación de cuentas o de sus respectivos intereses. Sobre el particular, **Rodríguez Gómez** explica que "*si de cada uno de los cálculos efectuados sustraemos el último decimal, nos encontraremos con una suma de ínfimas cantidades cuyo resultado puede ser una ingente cantidad de dinero.*"[74]. Modalidad de conducta que ha sido olvidada en la regulación positiva vigente, pero que podría quedar cubierta por el tipo penal de *estafa*[75], en su modalidad de transferencia de activos patrimoniales no consentidos *mediante artificios* en perjuicio de terceros. En estos casos, lo discutible sería verificar la inducción o el mantenimiento del error operativo en el sujeto pasivo afectado que causa la transferencia económica, cuestión bastante compleja[76].

De otro lado, el CP. prevé como delito en el art. 300 mod. L. 890/2004, art. 14, referido a las infracciones contra el orden económico social, la conducta de ***Ofrecimiento engañoso de productos y servicios***, de la siguiente forma: "*El produc-*

---

por lo que ni debe fundamentarse en ello el grado de ejecución delictual, valorando el hecho como tentativa o consumación, ni deben atenderse a un límite mínimo del mismo como base de su aminoración penal". Ello desde luego, pues dichos tipos penales se dirigen a proteger en primera instancia el bien jurídico seguridad de la información y no el patrimonio económico, y porque resultan tipos de mera actividad, de peligro y generalmente en blanco, de tal suerte que su resultado jurídico puede afectar el sistema o su funcionamiento, el equipo o el titular del derecho; Sieber: Criminalidad…, ob. cit., pág. 39.

73 Sobre el particular, cfr. Matellanes: ob. cit., pág. 139.

74 Cfr. Rodríguez Gómez: ob. cit., pág. 147.

75 Sobre el particular, Matellenes: ob. cit., pág.139-140, indica que: "por lo demás, los elementos del delito son básicamente los mismos: se requiere ánimo de lucro; la manipulación informática o el artificio semejante equivalen al engaño bastante y al error; la transferencia no consentida es el acto de disposición que provoca el perjuicio para tercero, elemento que también se requiere. Debe tenerse en cuenta que lo común será que la transferencia se haga directamente por el sistema informático que recibe la orden fraudulenta, por lo que la referencia a "no consentida" no puede entenderse como exigencia de un acto concreto de voluntad contrario a la transferencia, sino como orden de cargo hecha en activos ajenos sin derecho a ello". En contra de que la manipulación informática sea tenida como error, cfr. Möhrenschlager: El Nuevo Derecho penal…, ob. cit., pág. 110.

76 Cfr. Gutiérrez Francés: ob. cit., pág. 588.

tor, distribuidor, proveedor, comerciante, importador, expendedor o intermediario que ofrezca al público bienes o servicios en forma masiva, sin que los mismos correspondan a la calidad, cantidad, componente, peso, volumen, medida e idoneidad anunciada en marcas, leyendas, propaganda, registro, licencia o en la disposición que haya oficializado la norma técnica correspondiente, incurrirá en multa". En realidad, se trata de un tipo de mera actividad doloso, que además puede constituir un delito masa de estafa en la Web sobre bienes y servicios de primera necesidad.

Otra modalidad de defraudación en la Internet utilizando medios informáticos, que atenta no sólo contra el orden económico social (propiedad industrial), sino también contra el patrimonio económico, es la conducta prevista por el art. 306 mod. L. 890/2004, art. 14, relativa al uso fraudulento del nombre comercial que designa a un determinado empresario, de las enseñas o signos que utilizan las empresas para identificar sus establecimientos y páginas Web, de las marcas o signos perceptibles capaces de distinguir en el mercado los productos y servicios producidos frente a otros similares de otro empresario (incluyendo sus lemas, frases o leyendas complementarias), patentes de invención, modelos de utilidad o diseños industriales protegidos legalmente, o el uso de algunos similarmente confundibles con los primeros en el mismo ámbito industrial. O la venta o comercialización vía Web de bienes producidos o distribuidos con violación a los derechos industriales de otro[77].

Para terminar, subsisten otras modalidades de delitos tradicionales que pueden ser realizados vía informática como la extorsión[78] (art. 244 y ss. mod. L. 890/2004, art. 14), el lavado de activos (art. 323 mod. L. 747/2002, art. 8° y L. 890/2004, art. 14) y la omisión de control (art. 325 mod. L. 890/2004, art. 14); conductas especiales de hurto como el '*cardig*', que suponen el apoderamiento de cantidades de dinero mediante la obtención fraudulenta de la información financiera de las víctimas (claves o passwords) o por la 'falsificación' monetaria que supone la introducción de datos falsos en las bandas magnéticas de las tarjetas de crédito o debito, en perjuicio de sus titulares[79]. Así como el abuso de cajeros electrónicos, lo que permite el retiro de dinero en efectivo utilizando llaves falsas, sustraídas o cualquier otro instrumento similar; o superando las seguridades electrónicas dispuestas por las entidades bancarias (arts. 239 y 240, num. 4)[80].

77 Sobre los elementos normativos contenidos en el art. 306, véase la decisión 486 de 2000 (Comunidad Andina de Naciones) —acuerdo de Cartagena. De otro lado, cfr. CP. español, art. 274.

78 Cfr. Márquez Escobar: El delito informático…, ob. cit., págs. 181 y 182.

79 Vid. Jaén Vallejo, Manuel: Falsificación de tarjetas de crédito o débito: La alteración de los datos contenidos en la banda magnética constituye falsificación de moneda (Art. 386). Nota sobre el Acuerdo del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo de 28 de junio de 2002, en: RECPC 04-j10 (2002), Pág. j10:1- 3. En: http://criminet.ugr.es/recpc/recpc 04-j10.pdf.

80 Cfr. CP. español, art. 239.2. Romeo Casabona: Poder informático…, ob. cit., pág. 121 y ss.

E. La falsedad informática. Otra modalidad delictiva usual consiste en el uso, adulteración, modificación, creación por imitación total o parcial, destrucción u ocultamiento temporal o definitivo de documentos electrónicos públicos o privados por medios informáticos, a condición de que los mismos puedan servir de prueba[81]. Conductas que están dirigidas a simular su veracidad, legitimidad, oponibilidad y autenticidad en el tráfico documental, en el marco de una clara violación a la fe pública (identidad probatoria de los datos o informaciones). Esta modalidad de conducta informática *—al menos en nuestro medio—* se sanciona de forma parcial a través de los tipos ordinarios de falsedad en documentos[82].

En la doctrina penal también se consideran como falsedad informática *—en sentido estricto—*, aquellas acciones preparatorias dirigidas i) a introducir o almacenar datos incorrectos e incompletos, o la adulteración de los almacenados en un sistema informático[83]; y ii) la manipulación o el uso malicioso de los resultados de un proceso de elaboración o transmisión de datos almacenados, mediante la configuración de los programas o del software; conductas que generen información falsa a fin de practicar engaños en el tráfico jurídico mediante documentos. Sin embargo, tales modalidades no resultan claramente cubiertas desde el punto de vista típico en Colombia, pues la sola falsificación de datos almacenados en soportes lógicos destinados a ser usados o el resultado de su procesamiento, no se puede asimilar completamente a la falsedad de documentos electrónicos (Ley 527 de 1999, art. 45) o a la adulteración de de soportes materiales. Ello demuestra la insuficiencia de los tipos penales vigentes en la materia.

---

81 Vid. Möhrenschlager: El Nuevo Derecho penal…, ob. cit., pág. 120, indica sobre el carácter probatorio lo siguiente: "datos que, por ley, uso o convención de los intervinientes están determinados y son apropiados, más allá de su mera existencia, para constituir expresión de la declaración de pensamiento del autor y para proporcionar prueba de determinadas relaciones jurídicas [de modo inmediato o a través de nuevo tratamiento] y permiten conocer a su otorgante, el declarante [al reproducirlos o para el caso de nuevo tratamiento mecánico]"; cfr. Ley 527 de 1999 y Sent. Corte Const. C-662 de 2000, Decreto 266 de 2000.

82 Vid. CP. español, arts. 395 y 400. En el primer caso, se castiga con pena de prisión de seis meses a dos años, la falsedad de documento privado (art. 390. 1, 2 y 3) por alteración de sus elementos o requisitos esenciales, por la simulación de todo o parte del documento que permita inducir en error sobre su autenticidad, y por la suposición de intervención de terceras personas en el documento, que no han tenido parte alguna en su expedición, o sobre las cuales se han consignado declaraciones o manifestaciones que no han tenido lugar o que han expresado de forma distinta. Por su parte, el art. 400 castiga la tenencia de programas de ordenador para la falsificación de dichos documentos, sancionado al agente, en cada caso, con la pena prevista para el autor según la clase de falsedad. Cfr. igualmente el CP. francés, mod. Ley 92-683 de 1994, art. 441-1; el StGB. alemán, § 269 complementado por los §§ 270 a 274 y 348; y el CP. italiano, art. 617, sexto (falsedad informática). Dicha conducta también tiene referente internacional en la Convención de Budapest del 23.22.2001, ob. cit., Cap. II, Sección 1, art. 7°: "Adulteración relacionada con computadores".

83 Vid. Möhrenschlager: El Nuevo Derecho penal…, ob. cit., pág. 121; Romeo Casabona: Poder informático…, ob. cit., pág. 75 y ss.

Desde luego, el ordenamiento penal colombiano prevé diversas hipótesis de falsedad documental que, aunque no castigan la conducta preparatoria de generar datos falsos, si sancionan diversos comportamientos referidos a los documentos espurios que soportan los datos falsos obtenidos como resultado de la manipulación de procesos automatizados; de la siguiente forma: a) La conducta de *falsedad material de documento*[84] *público* (*electrónico*) *que pueda servir de prueba*, se encuentra prevista en el art. 286, mod. L. 890/2004, art. 14. El art. 289 mod. L. 890/2004, art. 14, consagra el delito de falsedad en documento privado (electrónico) que pueda servir de prueba y su uso en el tráfico jurídico; y el art. 291 mod. L. 890/2004, art. 14 cobijaría los casos de uso de documento público (electrónico) cuando no se ha concurrido en la falsificación informática. b) A su turno, el art. 293 mod. L. 890/2004, art. 14 prevé la hipótesis de *destrucción, supresión u ocultamiento, total o parcial, de documento privado (electrónico) que pueda servir de prueba* y el art. 292 mod. L. 890/2004, art. 14 la *destrucción, supresión u ocultamiento, total o parcial, de documento público (electrónico) que pueda servir de prueba, y que se agravará si la conducta es realizada por un servidor público en ejercicio de sus funciones y/o se tratare de documento constitutivo de pieza procesal de carácter judicial*. c) Finalmente, el Código Penal colombiano contempla en el art. 296, la conducta de *falsedad personal,* con una pena de multa que se impondrá siempre y cuando la conducta no constituya otro delito. Desde luego, el tema no es claro frente a las facultades documentales sobre documentos privados electrónicos.

Descripción comportamental que cobija algunas hipótesis del llamado '***enmascaramiento***' **(IP spoofing)**, en las cuales un agente, con el propósito de obtener provecho para sí o para otro, o causar daño, sustituye o suplanta a un usuario de la Internet, o se atribuye nombre, edad, estado civil, o calidad que pueda tener efectos jurídicos en el uso y disfrute de los servicios que se prestan por dicho medio, siempre y cuando dicha conducta no constituya un supuesto de fraude informático cubierto por los tipos penales patrimoniales existentes. En realidad, en algunos casos el agente no se contenta con la simple actividad de '*suplantar*', sino que el agente configura su computador o los programas de sus sistema ordenador (identificación de destino, identificación del remitente, nombre de dominio o datos) con

84 En general, sobre documento electrónico, vid. Bacigalupo Zapater, Enrique: Documentos electrónicos y delitos de falsedad documental, en: http://criminet.ugr.es/recpc, RECPC 04-12 (2002), págs. 1- 17. Precisamente, el art. 294 del CP. Colombiano indica:"para los efectos de la ley penal es documento toda expresión de persona conocida o conocible recogida por escrito o por cualquier medio mecánico o técnicamente impreso, soporte material que exprese o incorpore datos o hechos que tenga calidad probatoria". A su turno, el CP. español, art. 26, indica que a "a los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica". Por todos, véase Corte Constitucional, sent. C-662 del 08.06.2002. El tema es polémico, pues la Ley 527 de 1999, que regula el tema de los documentos públicos electrónicos, es anterior a las normas del Código penal de 2000.

elementos que corresponden a otro equipo informático de un usuario que cuenta con la autorización de naturaleza legal o contractual para acceder *—de forma legítima—* a un servicio o a un sistema informático determinado. De este modo, el agente logra la conexión deseada y obtiene la información, los datos o los servicios a los que normalmente no tendría acceso.

F. La responsabilidad por contenidos expuestos en la Web. Esta categoría de conductas punibles, que perfectamente pueden ser realizadas en la Internet, se pueden clasificar, a su turno, en tres modalidades distintas, de la siguiente manera:

1. Delitos de contenido sexual. Usualmente, los diferentes ordenamientos penales consideran delictiva la conducta de pornografía infantil, bien sea desarrollada por cualquier medio impreso o en la Web[85]. En este sentido, el CP. colombiano, en el art. 218 mod. L. 890/2004, art. 14, sanciona las conductas alternativas *—entre otras—* de venta, compra, exhibición (de películas o fotografías) o la comercialización de material pornográfico en el que participen *—de manera explícita o implícita—* menores de 18 años vía Web. Como es usual, se olvida agravar dicho comportamiento cuando los menores sufran algún tipo de trastorno mental, inmadurez psicológica o diversidad sociocultural, situaciones que pueden incrementar la posibilidad de amenazar o lesionar su formación sexual. Aunque dicha conducta si resulta agravada de una tercera parte a la mitad, cuando el sujeto activo del delito sea integrante de la familia de la víctima[86].

No obstante, dicha conducta no cobija otras conductas lesivas como la distribución, poner a disposición, transmitir o distribuir pornografía de forma directa o indirecta a menores de edad, a través de un sistema informático, o la posesión de pornografía en la que participen menores destinada igualmente a menores de edad. De otro lado, el CP. prevé en el art. 219 (L. 679/ 2001, art. 34, mod. L. 890/2004, art. 14), el empleo de medios de comunicación o sistemas informáticos para obtener, promover u ofrecer contactos sexuales con menores de edad (publicidad de

85 El CP. español castiga diversas conductas relacionadas con menores: a) El art. 186 castiga con una pena de seis a doce meses, al que por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre menores de edad o incapaces. b) Por su parte, el art. 189 consagra un amplio catálogo de conductas que van desde la utilización de menores para elaborar material pornográfico, hasta la venta, difusión o exhibición de dicho material, incluso si el material ha sido elaborado en el extranjero o su origen fuere desconocido. Asimismo, el mencionado artículo castiga con pena atenuada en el grado inferior, la mera posesión en el sistema informático de material pornográfico, para realizar cualquiera de las conductas punibles previstas. También tiene referente en la Convención de Budapest del 23.22.2001, ob. cit., Cap. II, Sección I, art. 9° "Delitos relacionados con Pornografía para los niños".

86 Sobre el tema de los filtros de contenidos en la Internet, vid. Rodríguez Turriago, Omar y Rodríguez Turriago, María Mercedes: Control de contenidos en el Internet: Una realidad que puede ser vista como una amenaza, en: Revista de Derecho, comunicaciones y nuevas tecnologías, No. 1 (abril de 2005), Bogotá, Cijus- Ed. Uniandinas, 2005, Págs. 17 — 51.

contactos ilícitos o uso de medios informáticos para establecer contactos de prostitución infantil[87]).

2. Delitos que impliquen apología al genocidio o propaganda xenófoba o racista. Sobre el particular, el ordenamiento penal colombiano prevé algunas normas para sancionar *—con pena privativa de la libertad—* la difusión pública *—incluyendo la Internet—* de ideas o doctrinas que propicien o justifiquen conductas constitutivas de genocidio, desplazamiento ilegal, discriminación a grupos raciales, sexuales, religiosos, políticos, nacionales o con minusvalías físicas o mentales; o ideas o doctrinas que pretendan la rehabilitación de regímenes o instituciones que amparen prácticas generadoras de genocidio (cfr. CP., art. 102 mod. L. 890/2004, art. 14 y la agravante genérica prevista por el art. 58, num. 3).

Y, **3. Delitos contra el honor**. Finalmente, es necesario señalar las conductas que lesionan el honor, la honra y el decoro por medio de la difusión o realización directa de los delitos de injuria y calumnia utilizando el correo electrónico o la publicación de las mismas en la Web. En este sentido, el CP. Colombiano prevé los delitos contra la integridad moral en los arts. 220 "*injuria*", 221 "*calumnia*" y 222 "*Injuria y calumnia indirectas*", que resultan agravadas por el art. 223, cuando dichas conductas se cometan utilizando cualquier medio de comunicación u otro de divulgación colectiva (en este caso la Web), con penas de prisión que oscilan entre uno y cuatro años aumentadas de una tercera parte a la mitad, más la agravante genérica que prevé el art. 14 de la L. 890 del 2004[88].

G. Otras disposiciones. Para terminar este aparte, es importante señalar la existencia de otras normas penales que protegen la propiedad moral o intelectual, frente a los abusos que puedan tener ocasión en la Web u otros medios informáticos o telemáticos, por ejemplo, en materia de copia *(piratería informática)* o reproducción no autorizadas de música, películas, textos y archivos gráficos protegidos por la ley con ánimo de lucro, o su venta en Internet.

Precisamente, los arts. 270 y ss. del CP. colombiano consagran los delitos contra los derechos de autor, de la siguiente forma: a) El art. 270, mod. L. 890/2004, art. 14, prevé la conducta de "***violación a los derechos morales de autor***", que castiga: Num. 1 la publicación (*también vía Web*) sin autorización previa del titular del derecho de obras inéditas de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, y *programas de ordenador o soportes lógicos* (datos e información). Num. 3. Compendiar, mutilar o transformar sin autorización y por cualquier medio, obras literarias, artísticas, cinematográficas o científicas, fonogramas,

87 Sobre el tema, vid. Lotierzo, Rocco: Le attività di contrasto alla pedofila in Rete, (A.A. 2002, 2003) en: www.penale.it/document/lotierzo_01.pdf.; Márquez Escobar: El delito informático…, ob. cit., pág.165 y ss. Asimismo, cfr. CP. Español, arts. 18, 510 y 607.

88 Cfr. CP. español, arts. 205 y ss."calumnias" y 208 y ss."injurias" por medio de la imprenta.

videogramas, soportes lógicos y programas de ordenador. A su turno, el art. 271, mod. L. 890/2004, art. 14, consagra una serie de conductas punibles consistentes en ***defraudar los derechos patrimoniales del autor***, mediante la reproducción (salvo las copias de seguridad y las excepciones vertidas en la decisión 351 de 1993 de la Comunidad Andina de Naciones arts. 23 y ss., y en la ley 23 de 1982), representación, alquiler, comunicación, ejecución, exhibición, comercialización, difusión, distribución y retrasmisión –*por cualquier medio*–, de las obras protegidas antes mencionadas, sin autorización expresa y previa de su titular[89].

IV. CONSIDERACIONES FINALES

Ahora bien, luego de plantear de forma sucinta las diversas modalidades de conducta que la doctrina penal considera como delitos informáticos en sentido criminológico (amplio y estricto), y algunos de sus referentes positivos en la legislación penal vigente, es necesario efectuar varias precisiones.

En primer lugar. Aunque se pueda afirmar que el Código penal colombiano ha cubierto gran parte de las conductas tradicionales que atentan contra los bienes jurídicos individuales (*intimidad personal o patrimonio económico*) y colectivos tutelados por la vía informática (*'la seguridad informática' y el orden económico social*), bien a través de los 'tipos penales tradicionales' o de figuras típicas especiales, lo cierto del caso es que dicha normativa cuenta con serias deficiencias, como las siguientes:

1. Por una parte, no todas las modalidades delictivas informáticas (en sentido estricto) son castigadas penalmente, como sucede con ciertas hipótesis de daños (sabotaje), falsedad, manipulación y sustracción o uso de los elementos lógicos (inmateriales) de un sistema; o con aquellas conductas orientadas a la producción, distribución o a permitir el acceso de programas dañosos para los sistemas informáticos (*virus, bombas lógicas, caballos de troya, etc.*). Lo que implica serios problemas de impunidad, consideradas las restricciones fácticas de los tipos penales 'tradicionales' en la materia, además de la imposibilidad de ampliar su ámbito de cobertura por entrañar ello una trasgresión a la prohibición de la analogía 'in malam partem'. Sólo por colocar un ejemplo, los tipos patrimoniales prevén objetos de protección que no resultan equivalentes a los objetos requeridos por los delitos informáticos en sentido estricto (*objetos lógicos e inmateriales no equiparables a cosas muebles; o si por ejemplo: el concepto de documento abarca los documentos privados electrónicos).*

89 Vid. CP. español, arts. 270, 298 y ss. y Ley 34 de 2002, art. 96 y ss (Ley de propiedad industrial). Conductas punibles tienen referente en la Convención de Budapest del 23.22.2001, ob. cit., Cap. II, Sección I, art. 10°: "Delitos Relacionados con la violación de los derechos a la propiedad intelectual y de los derechos afines". Cfr. Márquez Escobar: El delito informático…, ob. cit., pág. 204 y ss.

Así mismo, tal y como funciona la legislación vigente, la aplicación actual de un determinado tipo penal dependerá de la naturaleza o las propiedades del objeto sobre el cual recae la conducta. A título de ejemplo, la destrucción dolosa de un documento (electrónico) implicará: la posible aplicación del art. 192, inc. 1° si contiene una comunicación privada dirigida a otra persona; del art. 196 si la comunicación es de carácter oficial; del art. 198 si se encuentra en una base de datos y su destrucción tiene como fin suspender o paralizar el trabajo; del art. 292 si el documento electrónico que sirve de prueba es público, o del art. 293 si el documento (electrónico) que sirve de prueba es privado (en caso de admitir que dicha conducta es posible). Ello demuestra la necesidad de que la legislación penal colombiana asuma una reforma ponderada y estructurada, con el propósito de proteger mejor la información como condición necesaria para la participación normal de los individuos en el sistema social digital.

2. Si bien el legislador colombiano ha considerado el problema de la delincuencia informática desde la perspectiva del '*intruso*', ello es insuficiente, pues ha olvidado la responsabilidad penal imputable a los titulares de sistemas informáticos o telemáticos, redes de comunicaciones o bases de datos. Por ejemplo: cuando de forma dolosa y contraria a las normas técnicas habiliten medidas de seguridad informática inútiles, defectuosas o inconvenientes que expongan la disponibilidad, integridad y confiabilidad de datos o de información informatizada de naturaleza sensible de terceros. Asimismo, tampoco se ha afrontado la responsabilidad de los titulares de sistemas informáticos que divulgan información de contenido regulado *de manera inadecuada*, lo cual facilita a cierta población protegida acceder a la misma sin mayores dificultades técnicas. Como ya se dijo, *desde una perspectiva político criminal,* no resulta satisfactorio que quienes manejan fuentes de riesgo informático (contenidos regulados como pornografía) se sustraigan de responsabilidad, cuando utilicen simples advertencias y condiciones de ingreso a los sistemas, trasladando así la responsabilidad del acceso a la población protegida. No se puede olvidar que en muchos casos la población protegida resulta ser inimputable (art. 33).

3. Desde luego, la ausencia de normas adecuadas se explica porque en nuestro medio subsiste una deficiente gestión en materia de seguridad informática, por lo que concierne a las distintas modalidades de servicios ofrecidos en plataformas computacionales o telemáticas, susceptibles de protección jurídico penal. De hecho, una deficiente gestión de seguridad informática se traduce en dos consecuencias negativas adicionales: por una parte, impide al legislador asumir conceptos, principios y parámetros técnicos puntuales y precisos al momento de estructurar los preceptos penales orientados a proteger '*la información*', con la consecuente imposibilidad de considerar en concreto las diversas conductas que afectan la confidencialidad, la integridad y la disponibilidad de datos o de información

informatizada en la práctica[90]. Y, por otra, dificultan estructurar tipos penales con vocación de permanencia y con la capacidad de abarcar los cambios tecnológicos futuros.

Deficiencia que promueve, a su turno, la tendencia de crear tipos penales informáticos abiertos, en blanco, con cláusulas generales y ánimos de lucro genéricos), tal y como lo exige algún sector de la doctrina penal moderna. De todas formas, no se puede olvidar que dichos mecanismos de tipificación, antes que solucionar la capacidad de conducción de la delincuencia informática a través del ordenamiento jurídico penal, desvirtúan los límites de contención del Derecho penal fundamentado en la protección de bienes jurídicos e instauran un Derecho penal autoritario de la 'seguridad'.

4. De igual manera, las normas vigentes no disponen penas adecuadas para las diversas modalidades delictivas informáticas, según los elementos típicos que varían en concreto la lesividad del comportamiento. Dicho lo cual, se requieren normas que consideren, por ejemplo: que los tipos han sido realizados por sujetos activos comunes 'outsider' o calificados 'insider'; la naturaleza de la información afectada en cada caso concreto (privada, oficial, comercial, financiera, de seguridad nacional, secretos industriales, etc.), los elementos subjetivos que motiven la realización de dichos comportamientos (p. Ej.: ánimo de lucro, fines ilícitos de revelación, utilización, destrucción, provecho, etc.), y la vulnerabilidad de la víctima por lo que atañe a su capacidad de defensa o comprensión de la afectación de sus bienes jurídicos, entre otras circunstancias complementarias que precisen la individualización judicial de la pena (art. 61), tal y como se requiere en el delito de daño en bien ajeno.

Por supuesto, lo dicho no significa que esté plenamente legitimada la construcción indiscriminada de tipos especiales o autónomos (*salvo, tal vez, el caso especial de apropiación y daños sobre objetos lógicos, servicios y tiempo de Internet; y las conductas relativas a producir, importar, vender, distribuir y ofrecer programas lógicos destructivos o 'Tampering'[91], o dar información para su creación o su aplicación*), arguyendo la protección de bienes jurídicos intermedios como 'la confianza y seguridad en la información o los datos informáticos'[92]; pero sí justifica una mayor labor de precisión de los

90 En este sentido, cfr. AA.VV. Penalización…, ob. cit., pág. 20, cuando se advierte que "las conductas reprochables resultan en la mayoría de los casos impunes debido a la inidoneidad de las figuras tradicionales. ...no se castigan dichos comportamientos ilícitos, porque no se tiene claridad sobre la naturaleza jurídica de los bienes objeto material de los delitos ni del interés jurídico".

91 Así, el CP. Suizo, § 144 bis (2), castiga la producción o distribución de virus de computadoras, y el CP. italiano, art. 615-quinto, sanciona la tenencia o difusión de programas dirigidos a producir daños o a interrumpir un sistema informático o telemático.

92 Precisamente, Romeo Casabona, Carlos María: prólogo al texto de Rovira del Canto: ob. cit., pág. XVI, afirma que la descripción de hechos informáticos puede implicar, a la par que se eliminan las lagunas legales en materia de delincuencia informática, i) desdibujar la vinculación

tipos penales tradicionales (principio de taxatividad, art. 10°) que implique la incorporación de elementos que especifiquen o complementen los verbos rectores y los objetos sobre los cuales recae la acción; atendidos los bienes jurídicos protegidos en concreto, los bienes jurídicos específicos susceptibles de protección adicional (la información) y las diversas variantes delictivas que presenta la práctica (*desde conductas propias de intrusión por cualquier medio informático con peligro para la intimidad o las comunicaciones en sistemas protegidos, hasta diversas modalidades de manipulación, destrucción fraudulenta o maliciosa, modificación, pérdida, copia abusiva, conocimiento, cesión, publicación, transferencia o utilización indebidos de información o datos confidenciales sin consentimiento del titular, violación de claves secretas o 'encriptadas' y de medidas de seguridad*).

5. Precisamente, la evolución de la técnica legislativa informática ha demostrado que no son satisfactorias: ni la simple complementación de los tipos existentes, ni la creación de legislaciones especiales 'ad hoc'. Por el contrario, resulta más adecuada la creación de tipos penales nuevos que refundan las conductas tradicionales, sin olvidar las nuevas esferas de protección jurídico penal en el ámbito de la criminalidad informática[93].

La ventaja de tal forma de proceder, sería la disminución de los complejos inconvenientes dogmáticos y sistemáticos que acarrearía (en el ámbito general de la teoría de la parte especial del Derecho penal y en particular de la teoría de la unidad y pluralidad de tipicidades) la existencia de una doble tipificación en el ordenamiento jurídico, bajo la cual, si bien la normativa informática sería de aplicación preferente por virtud del principio de especialidad, ésta no alcanzaría a desvalorar de manera integral el desvalor total de dichas conductas frente a otros bienes jurídicos lesionados o puestos en peligro. Ello implicaría sostener en muchos casos la existencia de concursos efectivos de tipicidades que, sin embargo, probablemente involucrarían transgresiones al principio constitucional de '*ne bis in idem*' (del mismo hecho derivar varios efectos jurídicos), perjudicarían seriamente la seguridad jurídico penal y complicarían la labor jurisdiccional sin necesidad, al momento de proteger los bienes jurídicos (*personalísimos, personales, intermedios o colectivos*) lesionados o puestos en peligro.

Así mismo, de cara a la posibilidad de crear normativas especiales, no se puede perder de vista que los tipos 'tradicionales', aunque directamente protegen otros bienes jurídicos como la 'fe pública', el 'orden económico social' o 'la intimidad', también consideran el valor, la integridad, la disponibilidad y la seguridad de la informa-

---

de dichos comportamientos a un bien jurídico identificado (como sucede en nuestro medio con el tipo penal de acceso abusivo a sistema informático protegido con medida de seguridad); ii) disminuyen la sujeción al principio de taxatividad; y iii) sobredimensionan la incriminación no calculada de conductas no sostenibles desde la perspectiva del Derecho penal, aunque sí desde la óptica del derecho administrativo.

93 Cfr. Gutiérrez Francés: ob. cit., pág.603 y ss.

ción (precisamente porque la 'información' como bien jurídico intermedio se encuentra en relación medial con aquellos). Así, en los delitos de revelación de secretos o de interceptación de comunicaciones, la información confidencial (secreta) representa el objeto material sobre el cual recae la acción de espionaje, y ello mismo es lo que permite calificar dicha acción como lesiva frente al bien jurídico intimidad. Otro tanto puede afirmarse con relación a los delitos de falsedad, en los cuales, lo que realmente puede servir de prueba es la información contenida en los documentos adulterados, información que comúnmente se entiende ligada al concepto de documento. No es, pues, cierto, que cuando se protegen los demás bienes jurídicos, a la par no se esté protegiendo la información como un interés intermedio. Desde luego, sin desconocer la necesidad de proteger la información —en casos excepcionales— *como bien público* digno de protección autónoma, aunque de forma instrumental o subsidiaria frente a los derechos y bienes jurídicos individuales preexistentes. Ello, al menos, hasta que la evolución dogmática permita consolidar de manera definitiva el bien jurídico protegido por estas hipótesis delictivas.

7. Para terminar, vale la pena insistir en la necesidad de verificar y evaluar —*con sumo cuidado*— las formas de tipificación que generalmente utilizan las distintas legislaciones en materia informática, así como también las técnicas que se proyectan utilizar en el ordenamiento jurídico penal colombiano. En otras palabras, se debe determinar la necesidad de tipificar dichas conductas utilizando la técnica de '*amenaza o peligro*' (*Gefärhrdungsdelikte*)[94] abstracto, tal y como se ha definido antes, pues no siempre es conveniente de cara a los caracteres del Derecho penal (fragmentariedad, subsidiariedad y ultima ratio; y a los principios de taxatividad, ofensividad material y culpabilidad). Es más, la doctrina proclive a esta forma de tipificación deberá aún dar buena cuenta de la necesidad de adecuar dichas conductas como tipos de peligro en abstracto, para obtener soluciones preventivas '*idóneas*', sobre la base de bienes jurídicos en formación. Desde luego, será necesario evitar cualquier clase de adelantamiento de las barreras de protección del Derecho penal que supongan intervenciones penales autoritarias, desde la perspectiva de los principios de necesidad de intervención penal y de ofensividad material, una vez considerados los distintos bienes jurídicos susceptibles de afectación en concreto.

En segundo lugar, se debe anotar que en el ámbito de la criminalidad informática todavía existen lagunas difícilmente accesibles desde la perspectiva jurídica, en temas como la jurisdicción y la competencia nacional o internacional, el tiempo y el lugar de la comisión del delito transnacional. Ello, a pesar del aparente consenso logrado en las convenciones internacionales para unificar las diversas legislaciones internas con relación a los tipos delictivos y su condigna penalidad, la unificación de los procedimientos probatorios admisibles desde la perspectiva constitucional y los me-

94 A favor de dicha técnica de tipificación en materia de delincuencia informática, vid. Rovira del Canto: ob. cit., págs. 13, 73 y 117.

canismos de cooperación judicial internacionales aplicables (extradición: sobre todo cuando algunos países no cuentan con modalidades delictivas especiales), entre otros aspectos[95].

En fin, el debate político-criminal en esta materia no es sencillo, y en realidad apenas comienza en Colombia. Lo que en realidad importa es que en el futuro la doctrina y la jurisprudencia se ocupen de una mejor configuración del bien jurídico tutelado (seguridad de la información, datos equipos y programas informáticos) y de la congruencia de los tipos existentes, antes de plantear construcciones especiales en el ámbito penal, desde el prisma de principios tan importantes como la mínima intervención penal y el principio de subsidiariedad. De no hacerlo, esta clasificación pasaría, como tantas otras en Derecho penal, a sumar la larga lista de expansión irrazonable de la intervención punitiva del Estado, en materias que —*en principio*— pueden ser reguladas por las otras ramas del ordenamiento jurídico.

V. Bibliografía

AA.VV. Penalización de la criminalidad informática, Proyecto académico, Santa Fe de Bogotá, Gustavo Ibáñez, 1998.

Bacigalupo Zapater, Enrique: Documentos electrónicos y delitos de falsedad documental, en: http://criminet.ugr.es/recpc, RECPC 04-12 (2002), págs. 1- 17.

Bekerman, Jorge M.: Informática: su regulación jurídica internacional "vis-á-vis" la brecha tecnológica, en: El derecho y las nuevas tecnologías. Contexto económico, social y cultural. AA.VV., separata, Separata de Revista del Derecho industrial, No. 33, Buenos aires, Depalma, 1990.

Berdugo Gómez de La Torre, Ignacio/ **Arroyo Zapatero**, Luis/ **García Rivas**, Nicolás/ **Ferré Olivé**, Juan Carlos/ **Serrano Piedecasas**, José Ramón: Lecciones de Derecho penal, Parte general, 2ª ed., Sl.: La Ley, 1999.

Cadavid Quintero, Alfonso. Introducción a la teoría del delito: especial consideración a los fundamentos del delito imprudente, (Colección Sistema Penal, No. 2), Medellín, Dike, 1998.

Campoli, Gabriel Andrés: Delitos Informáticos y Terrorismo Internacional, en: Revista de Derecho Informático: Alfa-redi Derecho y Nuevas Tecnologías, No. 077 - Diciembre del 2004, http://www.alfa-redi.org/rdi-articulo.shtml?x=1025.

95 cfr. Convention on Cybercrimen (ETS. No. 185, en: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

El mismo: Pasos hacia la reforma penal en materia de delitos informáticos en México, en: Revista de Derecho Informático: Alfa-redi Derecho y Nuevas Tecnologías, No. 079 - Febrero del 2005, http://www.alfa-redi.org/rdi-articulo.shtml?x=974

Castro Ospina, Sandra Jeannette: Delitos Informáticos: La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano, Madrid, DelitosInformaticos.com,15.07.2002.
http://www.delitosinformaticos.com/delitos/colombia.shtml.

———. *La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano*, en: XXIII Jornadas Internacionales de Derecho penal, Memorias, Bogotá, Universidad Externado de Colombia, Departamento de Derecho penal, págs. 127-162.

Champaud, Claude: El impacto de las nuevas tecnologías en la empresa, en. En: El Derecho y las nuevas tecnologías. Contexto económico, social y cultural. AA.VV., separata, Separata de Revista del Derecho industrial, No. 33, Buenos aires, Depalma, 1990, pág. 815 y ss.

Chiaravalloti, Alicia; **Levene**, Ricardo. *Introducción a los delitos informáticos, tipos y legislación (Publicado en el VI Congreso Latinoamericano en 1998, en Colonia, Uruguay. Publicado en La Ley, Nros. 202 del 23 de Octubre de 1998 y 215 del 11 de Noviembre de 1998, Argentina.) (En línea)* Madrid, DelitosInformaticos.com, 02.12.2002. http://delitosinformaticos.com/delitos/delitosinformaticos.shtml

Consejo de Europa: Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, serie de tratados europeos Núm. 185, preámbulo, En: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

Cuello Contreras, Joaquín: El derecho penal español, Parte general, 3ª ed., Madrid, Dykinson, 2002.

Díez Ripollés, José Luis: De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado, en: RECPC 07-01 (2005) http://criminet.ugr.es/recpc.

Estrada Garavilla, Miguel: Delitos informáticos, en: www.unifr.ch/derechopenal/artículos/pdf/delitos.pdf

Farjat, Gérard: Nuevas tecnologías y derecho económico, en. En: El Derecho y las nuevas tecnologías, Contexto económico, social y cultural. AA.VV., Separata de Revista del Derecho industrial, No. 33, Buenos aires, Depalma, 1990 pág. 530 y ss.

Guerrero Mateus, María Fernanda/ **Santos Mera**, Jaime Eduardo: Fraude informático en la Banca, Aspectos criminológicos, Santafe de Bogotá, Resma, 1993.

Gómez Martín, Víctor: El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (Art. 270, Párr. 3º CP.), en: RECPC 04-16.pdf. (2002) http://criminet.ugr.es/recpc/recpc04-16.pdf.

González Rus, Juan José. Protección penal de sistemas, elementos, datos, documentos y programas informáticos (Revista Electrónica de Ciencia Penal y Criminología RECPC, 01-14- 1999) (en línea). Granada, CRIMINET, Web de Derecho Penal y Criminología, 2004. http://criminet.ugr.es/recpc/recpc_01-14.html.

Gracia Martín, Luis: Prolegómenos para la lucha por la modernización y expansión del Derecho penal y para la crítica del discurso de resistencia, Valencia, Tirant lo Blanch, 2003.

Gutiérrez Francés, M.ª Luz: Fraude informático y estafa (Aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios informáticos), Madrid, Ministerio de Justicia, 1991.

Hirsch, Hans Joachim: Acerca del estado actual de la discusión sobre el concepto de bien jurídico, Trad. de Daniel Pastor, en: modernas tendencias en la ciencia del Derecho penal y en la Criminología, Actas y congresos, Madrid, UNED, 2001.

http://criminet.ugr.es/recpc.

http://ccweb.in2p3.fr/secur/legal/l88-19-home.html

http://www.exitoexportador.com/stats.htm.

http://www.derecho-internet.org/virus

http://delitosinformaticos.net.

http://www.fraud.org

http://www.itu.int/ITU-D/ict/statistics/index.html

http://www.aui.es/estadi/internacional/ internacional.htm

http://www.obs-internet.com: los diez delitos, engaños y fraudes más frecuentes en Internet.

Jaén Vallejo, Manuel: Falsificación de tarjetas de crédito o débito: La alteración de los datos contenidos en la banda magnética constituye falsificación de moneda (Art. 386). Nota sobre el Acuerdo del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo de 28 de junio de 2002, en: RECPC 04-j10 (2002), http://www.criminet.ugr.es/recpc/recpc 04-j10.pdf.

Javato Martín, Antonio Ma.: La tutela penal de consumidor en el comercio electrónico en el Derecho Suizo, en: RECPC 07-r2 (2005)- http://criminet.ugr.es/recpc.

Jescheck, Hans-Heinrich Y **Weigend**, Thomas: Tratado de Derecho penal, Parte general, Trad. de Miguel Olmedo Cardenete, 5ª ed., Granada, Comares, 2002.

Lotierzo, Rocco: Le attività di contrasto alla pedofila in Rete (A.A. 2002, 2003) en: www.penale.it/document/lotierzo_01.pdf.

Luzón Peña, Diego Manuel: Curso de Derecho penal, Parte general I, Madrid, Universitas, 1999.

Márquez Escobar, Carlos Pablo: El delito informático, la información y la comunicación en la esfera penal, conforme con el Nuevo Código Penal, Bogotá, Leyer, S.F.

Matellanes Rodríguez, Nuria: Algunas notas sobre las formas de delincuencia informática en el Código penal, en: Hacia un Derecho penal sin fronteras, Coord. María Rosario Diego Díaz-Santos y Virginia Sánchez López, XII Congreso Universitario de Alumnos de Derecho penal, Madrid, Colex, 2000, Págs. 129-147.

Mir Puig, Santiago/**Sieber**, Ulrich/**Möhrenschlager**, Manfred E./**Corcoy Bidasolo**, Mirentxu: Delincuencia informática, compendio, IURA-7, Barcelona, PPU, 1992.

Montano, Pedro J.: Responsabilidad penal e informática, en: www.unifr.ch/derechopenal/artículos/pdf/ montano1.pdf

Möhrenschlager, Manfred E.: Tendencias de política jurídica en la lucha contra la delincuencia relacionada con la informática, trad. Francisco Baldó Lavilla y Rantiago Mir Puig, en: Delincuencia informática, Barcelona, PPV, 1992.

Muñoz Conde, Francisco y **García Arán**, Mercedes: Derecho penal, Parte general, 5ª ed., Valencia, Tirant lo blanch, 2002.

National collar Crimencenter and FBI. C3-2004 Internet Fraud-crime Report. Enero 01/2004 a 12/31 de 2004, 2005, en: http://www.ic3.gov y http://www.ifccfbi.gov.

Nochteff, Hugo: El nuevo paradigma tecnológico y la asimetría norte-sur, en. En: El Derecho y las nuevas tecnologías. Contexto económico, social y cultural. AA.VV., separata, Separata de Revista del Derecho industrial, No. 33, Buenos aires, Depalma, 1990, pág. 592 - 593.

Orta Martínez, Raymond: CiberTerrorismo, en: Revista de Derecho Informático: Alfa-redi Derecho y Nuevas Tecnologías, No. 082 - Mayo del 2005, http://www.alfa-redi.org/rdi-articulo.shtml?x=949.

Portaley Nuevas Tecnologías Sl. *La Legislación Española frente a los Delitos Informáticos, (en línea).* Madrid, DelitosInformaticos.com, 9.02.2004.

http://delitosinformaticos.com/legislacion/legisvsdelitos.shtml.

Poullet, Ives: Derecho y nuevas tecnologías de la información: un enfoque comparativo del derecho europeo continental, en: El Derecho y las nuevas tecnologías. Contexto económico, social y cultural. AA.VV, separata de Revista del Derecho industrial, No. 33, Buenos aires, Depalma, 1990.

Quintero Olivares, Gonzalo/**Morales Prats**, Fermín/**Prats Canut**, José Miguel: Manual de Derecho penal, Parte general, 3ª ed., Navarra, Aranzadi, 2002.

Quintero Marín, Víctor Hugo. El Spam y otros abusos de correo electrónico, En: Revista de Derecho, comunicaciones y Nuevas tecnologías, No. 1 (Abril de 2005), Bogotá, Cijus- Ed. Uniandinas, 2005, págs.143-173.

Reyna Alfaro, Luis Miguel: El bien jurídico en el delito informático, en: http://www.alfa-redi.org7revista/data/34-14.asp. También en: Revista Jurídica del Perú, Lima, Perú, Año LI, Nº 21, Abril 2001, pp. 181-190.

Rodríguez Gómez, Carmen: Criminalidad y sistemas informáticos, en: El sistema penal frente a los retos de la nueva sociedad, Coord. María Rosario Diego Díaz-Santos y Eduardo Fabián Caparrós, XV Congreso Universitario de Alumnos de Derecho penal, Madrid, Colex, 2003, págs. 139-162.

Rodríguez Turriago, Omar y **Rodríguez Turriago**, María Mercedes: Control de contenidos en el Internet: Una realidad que puede ser vista como una amenaza, en: Revista de Derecho, comunicaciones y nuevas tecnologías, No. 1 (abril de 2005), Bogotá, Cijus- Ed. Uniandinas, 2005, págs. 17-51.

Romeo Casabona, Carlos María: Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la información, Madrid, Tudesco, 1987.

Rovira del Canto, Enrique: Delincuencia informática y fraudes informáticos, Estudios de Derecho penal No. 33, (Dir.) Carlos María Romeo Casabona, Comares, Granada, 2002.

Sánz Mulas, Nieves: La validez del sistema penal actual frente a los retos de la nueva sociedad, en: El sistema penal frente a los retos de la nueva sociedad. Coord. María Rosario Diego Díaz-Santos y Eduardo Fabián Caparrós, XV Congreso Universitario de Alumnos de Derecho penal, Madrid, Colex, 2003, pág. 9-28.

Schwarzenegger, Christian: Computer crimes in Cyberspace. A comparative análisis of criminal law in Germany, Switzerland and northern Europe, en: http://www.weblaw.ch/jusletter/artikel.jsp?articleNr =1957.ok.2002. Jusletter 14. Oktober 2002, www.jusletter.ch.

Posada Maya, Ricardo: ¿Es integrada la protección jurídico-penal por intrusión informática para titulares de información reservada?. en: Revista Sistemas, No. 96 (Abril-junio, 2006), Bogotá, Asociación Colombiana de Ingenieros de Sistemas, 2006, págs. 56 a 63, www.acis.org.co.

Sieber, Ulrich: Criminalidad informática: peligro y prevención, trad. de Elena Farré Trepat, en: Criminalidad informática, compendio, Barcelona, PPU., 1992, pág. 29 y ss.

El mismo: Documentación para una aproximación al delito informático, trad. de Ujala Joshi Jubert, en: Delincuencia informática, Barcelona, PPU, 1992, pág. 67 y ss.

Silva Sánchez, Jesús María: La expansión del derecho penal. Aspectos de la política criminal en las sociedades postindustriales, 2ª ed., Madrid, Civitas, 2001.

El mismo: Prólogo a la ed. española, en: La insostenible situación del Derecho penal, Estudios de Derecho penal, (Dir. Carlos María Romeo Casabona), Granada, Instituto de ciencias criminales de Frankfurt y Área de Derecho Penal de la Universidad Pompeu Fabra, 2002, pág. XI y ss.

Sneyers, Alfredo: El fraude y otros delitos informáticos, Madrid, Tecnologías de Gerencia y Producción, S.A., 1990

Téllez Valdés, Julio. Derecho informático. 3ª ed., México, McGraw Hill/ Interamericana Editores, 2004.

Tiedemann, Klaus: Criminalidad mediante computadoras, trad. de Amelia Mantilla viuda de Sandoval, en: Nuevo Foro Penal No. 30, octubre - diciembre de 1985, Bogotá, Temis, págs. 481-492.

Toniatti, Roberto. *Libertad informática y Derecho a la protección de los datos personales*, Principios de Legislación Comparada, Revista Vasca de Administración Pública. No. 29, Enero-Abril, 1991, págs. 139 -162.

Ull Pont, Eugenio: Derecho público de la informática, Madrid, UNED, pág. 17.

Zugaldía Espinar, José M. (Dir.) AA.VV.: Derecho penal, Parte general, Valencia, Tirant Lo Blanch, 2002.

Zúñiga Rodríguez, Laura: Política criminal, Madrid, Colex, 2001.