

ENSAYO JURÍDICO DE DERECHO INFORMATICO

DERECHOS FUNDAMENTALES, INFORMATICA Y NORMAS PENALES

LA VISION IUSINFORMATICA DE LA INTIMIDAD Y LOS DELITOS RELATIVOS A LOS DATOS PERSONALES INFORMATIZADOS.

Por:
Libardo Orlando Riascos Gómez
Doctor en Derecho
lrascos@alumni.unav.es
2008

ABSTRACT

El objeto principal de la presente investigación bibliográfica es analizar, estudiar y cuestionar de la visión ius informática del derecho fundamental a la intimidad, conocido como derecho de "habeas Data" o derecho de autodeterminación informativa en el derecho español y alemán. Una de las instituciones jurídicas relacionadas con esta visión ius informática del derecho es el llamado "*delito informático*". El Delito informático se analiza en el derecho comparado norteamericano, europeo, australiano y colombiano. En el ámbito penal se estudia: El bien jurídico tutelado, los diferentes tipos penales y los medios comisivos del delito o medios electrónicos, telemáticos o informáticos.

Palabras Claves: Derechos, Intimidad, visión ius informática, delito, medios electrónicos o telemáticos, Constitución, legislación.

ABSTRACT

The main object of the present bibliographical investigation is to analyze, to study and to question of the vision computer ius from the fundamental right to the intimacy, well-known as right of "habeas Data" or right of informative self-determination in the Spanish and German right. One of the juridical institutions related with this vision ius informatic of the right is the call "*computer crime*." The computer Crime is analyzed in the North American, European, Australian and Colombian compared right. In the penal environment it is studied: The property juridical protégé, the different penal types and the commisive means of the crime or electronic, telematic or computer means.

Key words: Rights, Intimacy, vision ius computer, crime, electronic or telematic means, Constitution, legislation.

CONTENIDO

PARTE PRIMERA

LA VISION IUS-INFORMATICA DE LA INTIMIDAD EN LA LEGISLACIÓN FORÁNEA Y COLOMBIANA II

- 4.2. [En Colombia: No existe el delito informático en la legislación, pero sí tipos delictivos en los que está presente la informática](#)
- 4.2.1. [Tesis negativa: nullum crimen sine lege previa penale.](#)
- 4.2.2. [Tesis ecléctica:](#) las nuevas tecnologías de la información, imponen una tutela penal efectiva.
- 4.2.3. [Tesis positiva:](#) el delito informático como producto concomitante de las nuevas tecnologías de la información y la comunicación. Técnica penal asimiladora de tipos.
- 4.2.4. [Tipos delictivos](#) en los que está presente actualmente el fenómeno ius-informático: El bien jurídico: El Habeas Data.

DESARROLLO

- 4.2. En Colombia. No existe el delito informático en la legislación, pero sí tipos delictivos en los que está presente la informática.

4.2.1. Tesis Negativa: *nullum crimen sine lege previa penale*

Actualmente no existe el delito informático como tal, ni en el Código Penal, ni en la legislación especial, básicamente por las mismas razones dadas en el derecho penal español y por otras particulares expuestas por la doctrina colombiana.

En efecto, abundando en la tesis negativa a la existencia del delito informático *Rivera Llano* ^[44], considera que al no estar tipificados la legislación vigente, éstos no existen. Lo que sí existe --dice-- son conductas no éticas y antijurídicas cuyos medios de ejecución se verifican con medios modernos o tecnológicos y, por tanto, la valoración de los mismos es nula ya que las conductas son asimilables o están tipificadas en los actuales Códigos Penales. Claro está que estas argumentaciones se quedan sin demostración, pues no se analiza cuáles, cómo y de qué forma se asimilarían los tipos penales actuales al denominado delito informático, a fin de que no sea necesaria su estructuración típica y autónoma.

4.2.2. Tesis Ecléctica: Las nuevas tecnologías de la información imponen una tutela penal.

Rivera Llano ^[45], a pesar de negar la existencia del delito informático, reconoce que los avances de las tecnologías de la información, han ocasionado una especie de *segunda revolución: la informática*, y como tal, los Estados deben afrontar esta situación tutelando penalmente las agresiones que se cometan contra la información. *La era de la información*, está marcada por el desarrollo constante de la industria y la tecnología de la telecomunicación, la miniaturización de los *chips*, la globalización del uso de computadores para toda clase de servicios desde los empresariales hasta los meramente familiares y personales. “*Esta marcha triunfal de las aplicaciones de la informática no solo tiene un lado ventajoso sino plantea también problemas de importancia crucial para el funcionamiento y la seguridad de los sistemas informáticos en el mundo de los negocios, la administración y la sociedad en general*”; y por ello, para paliar algunos de estos problemas debe erigirse el delito informático (*computer crime*) para proteger los atentados de la *criminalidad informática* que cada día crece en el mundo, teniendo como bien jurídico protegible el de la información.

El autor citado, siguiendo en términos muy generales la clasificación de *Ulrich Sieber*, en cuanto a la información creada, procesada o recuperada por medios computacionales, informáticos o telemáticos y luego de aceptar doctrinalmente la existencia de los delitos informáticos, expone que en éstos lo principal no son los medios tecnológicos empleados en la comisión del delito sino el objeto material contra el que van dirigidos, es decir, la información (en su *creación, destrucción o uso*) procesada por la tecnología.

En tal virtud, clasifica a los delitos informáticos, a saber: a) Delitos contra la información por creación, b) Delitos contra la información destrucción total o parcial, c) Delitos contra la información por uso indebido, inapropiado o no autorizado, d) Delitos contra la información por medio de sustracción, que se puede concretar por la simple obtención en “*pantalla*” o por copia de programas o archivos.

En esta concepción y clasificación del delito informático predomina como característica la de considerar a la *información*, en general (electromagnética, computacional o telemática) como bien jurídico tutelable por el Estado. En dicho bien se subsumen derechos no patrimoniales y patrimoniales que otras legislaciones como la española identifican autónomamente, como antes se analizó.

4.2.3. Tesis positiva: El delito informático como producto concomitante de las nuevas tecnologías de la información y comunicación. Técnica Penal similitaria de tipos.

Por su parte, el Criminólogo *Molina Arrubla* ^[46], al hablar de las diversas formas de la criminalidad actual, las clasifica así: a) Por la Estadística, b) Por sus Agentes, c) Por su ámbito; y d) Por su Desarrollo. Dentro de éste último grupo, incluye: a) La *Criminalidad Retrógrada*, es decir, la referida al pasado, ubicando entre ellos los *delitos de Sangre*; b) La *Criminalidad Anterógrada*, es decir, la criminalidad que tiende a generalizarse hacia el futuro, como son las delincuencias en el campo internacional y transnacional; y c) La *Criminalidad evolutiva*, es decir, aquella que nace

concomitantemente con los avances tecnológicos, mercantiles, industriales y con métodos sofisticados y perfeccionistas utilizados en la comisión de los ilícitos. La comisión y ejecución de estos hechos se hace por regla general, a través de labores de inteligencia, como sucede en los fraudes y quiebras simuladas. En otras ocasiones dan origen a una nueva vertiente de la criminología que se conjuga en el llamado *Delito Económico*, o en su caso, por el avance de las nuevas tecnologías de la información y comunicación.

En consecuencia, los “*delitos de informática*”, son producto de la criminalidad evolutiva, la cual nace concomitantemente con las nuevas tecnologías informáticas y telemáticas y el *delito informático* es aquél se comete con el empleo de computadores o equipos electromagnéticos que transmiten datos o *informaciones*.

Los delitos informáticos, según *Tiedemann*,

alude (n) a todos los actos, antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de datos. Por una parte, dicho concepto abarca pues el problema de la amenaza, asociación y divulgación de datos obtenidos por computadores..., y por otra parte, el concepto aludido se refiere a los daños patrimoniales producidos por el abuso de datos procesados automáticamente... ^[47] .

Esta definición contempla el concepto de delito informático con base en los problemas sobrevenidos en el proceso de tratamiento automatizado o computacional de la información personal o los datos de carácter personal, desde aquellos en los que se utiliza como medio comisivo a los equipos electromagnéticos para procesar información hasta aquellos en los que la recolección, utilización, recuperación y abusos de la información constituyen el objeto material del ilícito e igualmente la información con bien jurídico protegible.

Molina A., siguiendo a *Tiedemann* ^[48] , profesor del Instituto de Criminología y Derecho Penal de Friburgo (Alemania), clasifica a los delitos informáticos así: a) Las Manipulaciones que una persona realice en las actividades de entrada y salida de información o de datos computarizados; b) El Espionaje económico, teniendo en cuenta que la información se almacena en soportes electromagnéticos, la transferencia de datos de un lugar a otro por cualquier medio sistematizado es lo más usual actualmente. Este espionaje económico se utiliza por empresas rivales, así como con finalidades políticas por Estados Extranjeros; c) Sabotaje. Se produce daño, destrucción, inutilización en el procesamiento de datos o información automatizada, en programas o software total o parcialmente; y, d) Hurto de tiempo. Tiene cabida en la indebida utilización, sin autorización de equipos computacionales o salas informáticas. Se penaliza el uso indebido y el tiempo de procesamiento de información o de datos perdido por el propietario con las inapropiadas actividades.

El autor citado, al aplicar esta clasificación del delito informático alemana al caso colombiano, comienza diciendo que el bien jurídico tutelado en estos casos prioritariamente es el *Patrimonio Económico* (Título XIV del Código Penal Colombiano de 1980), con lo cual no descarta otros bienes tutelables, ya que considera que la mayoría de las conductas delictivas que se cometen con computadores oscilan entre el hurto, la estafa, el fraude, el abuso de confianza y el daño. Esta técnica asimiladora es una postura tradicional que no aporta mucho a la tesis positiva del delito informático, sino al contrario trata de desvirtuarlo, pues se estima que no hay necesidad de darle autonomía jurídica, ya que basta con estudiar el fenómeno de las nuevas tecnologías de la información y comunicación a la luz de los tipos actualmente existentes en el Código Penal y adecuarlos normativamente, si fuere del caso, o adicionarlo a los tipos existentes como causales de agravación punitiva. Sin embargo, al encasillar los actuales tipos penales previstos en el Código Penal Colombiano, en la clasificación alemana está reconociendo la existencia del delito informático, no sólo en la doctrina sino en la legislación penal vigente, y por ende, la necesidad de tipificarlo y darle autonomía propia y un bien jurídico tutelable. Quizá sólo por ello, la técnica que llamamos asimiladora de tipos penales es el primer gran paso a la autonomía del tipo penal informático en el derecho colombiano.

Al tratar de encuadrar el *Hurto de Software y espionaje*, el citado autor no tuvo en cuenta la abundante legislación existente sobre el tema, aparte de la que fue objeto de su estudio (Código Penal: *Delitos contra la propiedad*, Tit. XIV y *Delitos contra el orden económico social*, Tit. VII). En

efecto, se dejó de lado toda las normas penales especiales previstas en la regulación sobre propiedad intelectual y a la protección de los programas computacionales o *software*, como una de sus especies (Ley 23 de 1982 y 44 de 1994), la prevista en la Ley 296 de 1996, sobre Libertad de competencia económica e infracciones a la misma y las Decisiones 351/93 y 344/94 del Parlamento Andino, sobre propiedad intelectual e industrial, respectivamente.

En las anteriores leyes se prevén tipos penales y contravencionales específicos que protegen la propiedad intelectual, y en especial, el software contra atentados de copia, procesamiento, apropiación, uso indebido, etc., pues el software es un trabajo intelectual de “*pensamiento-resultado*”^[49], “*la expresión de un conjunto organizado de instrucciones, en lenguaje natural o codificado, independiente del medio en que se encuentre almacenado, cuyo fin es el de hacer que máquina capaz de procesar información, indique, realice u obtenga una función, una tarea o un resultado específico*” (artículo 3, lit., a Dec.1360/89), que justifica la protección jurisdiccional.

4.2.4. Tipos delictivos en los que está presente actualmente el fenómeno informático. Bien jurídico: “*Habeas Data*”.

Hemos sostenido antes que la informática y/o la telemática puede afectar a bienes jurídicos patrimoniales y no patrimoniales, como también, a derechos fundamentales y libertades constitucionales, como la intimidad y el *habeas data*. Los diferentes tipos están previstos en los Códigos Penal y Nacional de Policía, y en los estatutos penales especiales v.gr. los que regulan *la propiedad intelectual*^[50] y *la propiedad industrial*. Las normas extrapenales (códigos civil, mercantil y administrativa, principalmente), brindan una protección jurisdiccional preventiva, interpretativa y hermenéutica a la punitiva, pero prioritariamente a la propiedad intelectual e industrial.

En estos estatutos penales principales, especiales y complementarios encontramos hechos punibles que la doctrina universal califica de informáticos, ya sea por que en su comisión se utilizan medios u objetos electromagnéticos: informáticos y/o telemáticos, o porque el derecho de acceso a la información o *habeas data*, constituye un bien jurídico tutelable por el Estado. Algunos de estos tipos punitivos (delitos y contravenciones) se han relacionado antes^[51]. En éste aparte relacionaremos otros más.

Un aspecto capital a destacar de las diversas posturas doctrinales mencionadas es el planteamiento del bien jurídico del derecho fundamental de “*Habeas Data*” cuya tutela o garantía estatal puede válidamente sostenerse en el derecho penal colombiano, entre otras razones, por las siguientes:

En Colombia, se ha constitucionalizado el derecho de *habeas data*, o sea, derecho que tiene toda persona a acceder a la información relevante que le compete, así como a conocerla y solicitar, si fuere del caso, la actualización y la rectificación de la misma (artículo 15, constitucional), tanto de la información obtenida o procesada mecánicamente (oral, escriturario o impresa), como la que ha sido objeto de procedimientos automatizados por equipos computacionales, informáticos o telemáticos y se ha almacenado en dispositivos electromagnéticos (discos fijos, removibles, CD-ROM y RAM o DVD o Disco Digital de Video)^[52], en bancos de datos de carácter público o privado. Este derecho de acceso a la información se extiende también al derecho que tiene toda persona a demandar de cualquier autoridad estatal el “acceso a los documentos públicos salvo los casos que establezca la ley” (artículo 74, constitucional), es decir, el Código Contencioso Administrativo, la Ley 57 de 1985, el Decreto Ley 2150 de 1995 y Ley 226 de 2000, principalmente.

Igualmente para interpretar el ámbito, alcance y limitaciones del derecho de acceso a la información se deberá estudiar la vertientes que tiene el derecho a la información (artículo 20) como derecho fundamental de toda persona en los términos que la legislación universal lo ha instituido (Artículo 19 de la Declaración universal de Derechos Humanos de 1948) y que la Constitución de 1991, ha elevado a rango constitucional el derecho de toda persona a “*informar y recibir información veraz e imparcial*” (artículos. 20), como derecho genérico y la libertad de expresión o “*prensa*” (artículo 73) y el derecho de toda persona de acceder a los documentos públicos, salvo las excepciones de ley (artículo 74), como derechos igualmente fundamentales específicos. En efecto, en el derecho constitucional colombiano, el derecho a la información no sólo se extiende a la vieja libertad clásica e individualista de la *libertad de prensa* vista de un aspecto simplemente activo, es decir, desde el emisor o productor de la información sino también del receptor o consumidor de la información.

La Constitución colombiana, al igual que lo hiciera la Brasileña de 1988 y mucho antes la Portuguesa de 1976, constitucionalizaron el llamado “*Habeas Data*”, con diferente técnica y efectos, pero las tres elevan a rango constitucional lo que se ha conocido como *informática*, el derecho fundamental de *habeas Data*, y en forma particular, la Constitución Colombiana, constitucionaliza las fases del tratamiento automatizado de datos y los límites y autolímites que debe observar con respecto a los demás derechos y libertades constitucionales. En consecuencia, el artículo 15 de la Constitución Colombiana, siguiendo los pasos de la Constitución Portuguesa (artículo 35) y Brasileña, incorporó el *Habeas Data* en el texto constitucional, no como un derecho autónomo como en aquéllas Cartas, sino como un derecho contenido en otro gran derecho continente que tutela “*la intimidad personal y familiar y el buen nombre*”. Técnica esta última que se presta a muchas interpretaciones, entre otras, como la seguida en el derecho constitucional español cuando la doctrina ha escindido de un mismo texto constitucional, otros derechos autónomos o “derechos constitucionales nuevos”, con igual rango del que nació, tal como se viene sosteniendo tras el planteamiento del ius-filósofo Pérez Luño,^[53] con la llamada “*Libertad informática*”, escindida del artículo 18.4 CE., que regula la informática como límite al ejercicio los derechos fundamentales, como la intimidad, honor, imagen, etc., ampliamente criticada en el escrito electrónico de ésta página WEB, intitulada: **LA VISION IUS-INFORMATICA DEL DERECHO A LA INTIMIDAD, NO ES UN NUEVO DERECHO FUNDAMENTAL** En: <http://akane.udenar.edu.co/derechopublico>.

Otra interpretación diferente es la que se dio por parte del constituyente colombiano en la Constitución de 1991, al incorporar anti-técnicamente en un mismo artículo tanto el derecho constitucional de *habeas data* como los derecho el fundamental de la intimidad (que subsume el llamado del “buen nombre” o de la “propia imagen”), pero el primero (*habeas data*) en forma expresa y demasiado amplia que más parece un texto de rango legislativo que constitucional. En efecto, se define el *habeas data*, el procedimiento de recolección y tratamiento de la información mecánica y/o informática, las excepciones en la comunicación privada, las interceptaciones judiciales a la comunicación, así como la extensión a documentos específicos, como los tributarios, por ejemplo. Allí mismo iniciando el artículo se constitucionaliza el derecho a la intimidad personal y familiar, como derecho fundamental objeto de protección especial por parte del estado. Los dos derechos están completamente individualizados, pero el constituyente los fusionó como si se tratara de un mismo fenómeno jurídico, o en consideración media, como si se tratase de derechos complementarios e inseparables y esto no es del todo así. Esta técnica del Constituyente colombiano ha sido objeto de crítica en el escrito electrónico de esta página denominado : LA VISION IUS-INFORMATICA DEL DERECHO A LA INTIMIDAD, NO ES UN NUEVO DERECHO FUNDAMENTAL.

La Corte Constitucional Colombiana, paulatinamente va desentrañando la autonomía del derecho de *habeas data* y la intimidad, como hemos visto en el trabajo electrónico referido anteriormente,^[54] basados en lo que les da identidad y separabilidad: por un lado, los valores constitucionales como la dignidad y el respeto de la persona humana, y la conexión con el derecho de autonomía personal; y por otro, los límites a las demás libertades y derechos fundamentales, como el derecho a la información, el acceso a los documentos públicos o privados, entre otros. Y es, precisamente en la teoría de los límites y autolímites a los derechos constitucionales donde aflora la separabilidad de uno y otro derechos, pues se ha encontrado que una de las mayores vertientes a los “abusos de la información” han dado origen a “un nuevo derecho denominado *habeas data*”^[55] en el derecho constitucional colombiano.

Concordantemente, hemos sostenido que con la manipulación de la información mecánica (impresa) o automatizada (informática), no sólo se vulnera derechos patrimoniales y no patrimoniales sino también derechos de tratamiento jurídico *sui generis*, como el de la propiedad intelectual o la industrial. En tal virtud, no podemos simplemente supeditar el *habeas data* a la intimidad, ni menos fusionar el uno al otro, como si fuese uno solo^[56] y como sí el derecho de *habeas data* sólo afectara al derecho de la intimidad y no al cúmulo de derechos y libertades públicas, y además porque, un sector de la doctrina ius-informática ha planteado sus diferencias de contenido, alcance socio-jurídico y carácter proteccionista por parte del Estado^[57].

Esta técnica *sui generis* de codificación constitucional conduce a diversas como erróneas interpretaciones por parte del operador jurídico, por ejemplo, la de entender que el derecho de *habeas data* sólo afecta al derecho de la intimidad y no a ninguno otro derecho personal y/o

patrimonial --como es la tendencia generalizada--, por la exclusión formal de los demás derechos o libertades en los que éste no está incluido.

Por contra, creemos que una recta interpretación de la norma nos debe conducir a entender que dicho texto afecta al cúmulo de derechos y libertades constitucionales que se hallan previstas en la Constitución y no solamente a los previstos en el título II, *De los derechos, las garantías y deberes*, como fundamentales, pues aquellos se reputan no por su mera ubicación formal en la Constitución, ni por ser de aplicación inmediata (artículo 85, constitucional), o ser objeto de “*Acción de Tutela*” (artículo 86 id), sino por su contexto, forma y ámbito de injerencia como derecho en la dignidad y respeto de la persona humana, o por criterios principales y subsidiarios no concurrentes determinados por el juez de tutela ^[58].

Ahora bien, los hechos punibles (delitos y contravenciones) en los que está presente el fenómeno tecnológico de la información y la comunicación: informática y/o telemática, están actualmente ubicados en el Código Penal de 1980 y el Código Nacional de Policía, en las leyes punitivas especiales como la que protege la propiedad intelectual e industrial, bajo diferentes bienes jurídicos, ubicación y dosimetría penal.

I.- *Delitos previstos en el Código Penal de 1980 y en el Código Penal de 2000, a saber:*

A. *Delitos de los datos o informaciones automatizadas contra un bien jurídico tutelado:* En el Título X, “*De los delitos contra la libertad individual y otras garantías*”. Capítulo V, “*Delitos contra la violación de secretos y comunicaciones*”: 1. violación ilícita de comunicaciones (artículo 288); 2. violación y empleo de documentos reservados públicos o privados (artículo 289); 3. utilización ilícita de equipos transmisores o receptores (incluidos los electromagnéticos: informáticos y/o telemáticos); y, 4. interceptación ilícita de correspondencia oficial. Estos dos últimos previstos en el Decreto Extraordinario 2266 de 1991, artículos. 16 y 18, respectivamente que han sido incorporados a la legislación penal especial en forma permanente.

En el Nuevo Código Penal Colombiano de 2000, en el Título III de los Delitos contra la Libertad Individual y otras garantías, en el Capítulo VII, *De la violación a la intimidad, reserva e interceptación de (las) comunicaciones*, se prevé los siguientes tipos delictivos: a) Violación ilícita de comunicaciones (Artículo 192), b) Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas (Artículo 193), c) Divulgación y empleo de documentos reservados (Artículo 194), d) Acceso abusivo a un sistema informático (Artículo 195), e) Violación ilícita de comunicaciones o correspondencia de carácter oficial (Artículo 196), y f) Utilización ilícita de equipos transmisores o receptores (Artículo 197).

B. *Delitos contra los datos o informaciones automatizadas que se hallan bajo diferentes bienes jurídicos:* 1) *La Fe pública.* En el Título VI, *De los delitos contra la fe pública*, extiende el concepto de documento tradicional (escrito) al concepto de “*documento electrónico*”, cuando incluye en la “*asimilación a documentos...los archivos electromagnéticos*” (Artículo 225 del Código Penal Colombiano, concordante con los arts. 274 y 251). Así debe entenderse que éste concepto se aplicará a los delitos: 1. Falsedad material de empleado oficial en documento público (artículo 218); 2. Falsedad ideológica en documento público (artículo 219); 3. Falsedad material de particular en documento público (artículo 220); 4. Falsedad en documento privado (artículo 221); 5. Uso de documento público falso (artículo 222); 6. Destrucción, supresión y ocultamiento de documento público (artículo 223); y, 7. Destrucción, supresión y ocultamiento en documento privado (artículo 224).

En el Código Penal Colombiano de 2000, se establece en parecidos términos, en el Título IX, *De los Delitos contra la Fe Pública*, Capítulo III, *De la Falsedad de documentos* (arts. 286 a 296), quedan involucrados los delitos informáticos cometidos por medios informáticos, telemáticos o informáticos, puesto que en el artículo 294, se retoma la definición de “documento” a los efectos de la ley penal y quedan incluidos aquellos documentos electrónicos en la expresión “por cualquier medio mecánico técnicamente impreso, soporte material que exprese o incorpore datos o hechos, que tengan capacidad probatoria”

2) *El orden económico social.* En el Título VII, *De los delitos contra el Orden Económico Social.* Se hace referencia expresa a los delitos contra la propiedad industrial, Comercial y Financiera. Estos

pueden ser cometidos mediante el uso de elementos informáticos y/o telemáticos. Estos son: 1. Pánico Económico (artículo 232); 2. Usurpación de marcas y patentes (236); 3. Uso ilegítimo de patentes (237); 4. Violación de reserva industrial (238). La ley penal especial, principalmente el Decreto 623 de 1993, conocido como "*Estatuto penal del sistema financiero colombiano*", concede a la Superintendencia Bancaria y de Valores amplias facultades de control, vigilancia, sanción administrativa e información y denuncia ante la Fiscalía General de la Nación sobre actividades delictivas que se presenten en el sector financiero (Bancos, Corporaciones de ahorro y vivienda, corporaciones financieras, sociedades fiduciarias), en todas las gestiones financieras (transferencia, circulación, depósito, ingreso, etc) "*con cualquier forma de dinero u otros bienes*" (artículos. 105 y ss).

La legislación extrapenal amplía la gama de protección: El Código del Comercio, reformado parcialmente por la Ley 256 de 1996, sobre protección a la libertad de competencia económica, prevé un proceso civil abreviado contra actividades que impliquen competencia desleal y *violación de secretos* (artículos. 16 a 33). Igualmente en otras normas sobre marcas y patentes (artículos. 583 y ss C.de Comercio); y, finalmente en la Decisión 344 de 1992, sobre propiedad industrial del Pacto Andino.

En el Código Penal de 2000, en el Título X, De los Delitos contra el Orden Económico Social, se prevé, entre otros delitos, los siguientes: a) Pánico Económico (art. 302), b) Usurpación de marcas y patentes (art.306), c) Uso ilegítimo de patentes (art.307); y, d) Violación de reserva industrial o comercial (art. 308).

Igualmente, el Código Penal de 2000, incorpora en la legislación ordinaria, la extrapenal o especial, sobre los "Delitos contra el Sistema Financiero", y establece las siguientes figuras delictivas donde esta presente la informática: a) Utilización indebida de fondos captados del público (art. 314), b) Operaciones no autorizadas con accionistas o asociados (art. 315), c) Captación masiva y habitual de dineros (art. 316), y d) Manipulación fraudulenta de especies inscritas en el Registro Nacional de Valores e intermediarios (art. 317).

3) *El patrimonio Económico.* En el Título XIV, *De los Delitos contra el Patrimonio Económico*, se relacionan los siguientes: 1. El Hurto Calificado, cuando se comete con "*llave falsa... o superando seguridades electrónicas u otras semejantes*" (artículo350). Entendiendo por llaves falsas, entre otras, "*las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia*", tal como lo prevé la legislación penal española (artículo239 *in fine*). El C. P. Col., amplía los medios comisivos al prevé la obturación o ruptura de claves o "*password*" para acceder a la apropiación de bienes. 2. Estafa "*valiéndose de cualquier medio fraudulento...*" como el informático y/o telemático (artículo256 *in fine*), configura lo que el Código Penal Español denomina "*Estafa informática*" (artículo248), como "*tipo defraudatorio que no comparte la dinámica comisiva de la estafa tradicional y, en consecuencia, ajeno a la elaboración doctrinal y jurisprudencial de los elementos que lo configuran*" ^[59] . 3. Daño agravado cuando se comete en "*archivos*" (se entiende manuales o informatizados), artículo 371.4.

En el Código Penal de 2000, en parecidos términos al Código Penal del 80, establece en el Título VII, De los Delitos contra el Patrimonio Económico, el delito de hurto calificado, cuando se comete "4. Con escalamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes" (art. 240), b) La Estafa, "*valiéndose de cualquier medio fraudulento*", que incluye los medios tecnológicos o informáticos (art. 246), y c) El Daño agravado, cuando se comete en "bienes de interés científico" que incluye a los informatizados o telemáticos (art.266-4).

Como figuras punitivas nuevas, se relacionan las siguientes: a) La defraudación de fluidos. Se apropie de una "señal de comunicaciones" (art. 256); b) Acceso ilegal o prestación ilegal de los servicios de telecomunicaciones (art. 257), c) Utilización indebida de información privilegiada (art.258)

4) *La propiedad intelectual.* Las leyes penales especiales de protección de los programas de computador o "*software*", la legislación de derechos de autor (Ley 23/32, Ley 44 /94 y D.R.1983 de 1991) y el soporte lógico o "*software*" (Dec.1360 de Junio 23 de 1989) prevén una gama variopinta de hechos punibles contra el derecho constitucional de la propiedad intelectual (Artículo61 Cons. Col.)

dentro de los cuales se incluyen los atentados producidos por la informática y/o telemática contra éste derecho fundamental, subjetivo e intangible ^[60] v.gr. accesos, procesamientos y abusos informáticos y la denominada “piratería”: electrónica y material del software. “Se castiga (la fabricación, puesta en circulación y) la tenencia o introducción en el mercado (clandestino) de los medios de inutilización (o neutralización), con independencia de que se hayan usado o no” ^[61], tal es el caso de los programas virus o descryptadores o inutilizadores de password.

El Código Penal de 2000, sobre estas figuras delictivas ^[61A], vuelve a incorporar la legislación extrapenal, y en el Título VIII, De los Delitos contra los Derechos de Autor, estipula: a) *Violación a los derechos morales de autor*, entre otros, la publicación parcial o total (art. 270-1); la Inscripción en el registro de autor con nombre de persona distinta del autor verdadero (art. 270-2); Se compendie, mutile o transforme, sin autorización previa y expresa de su titular (art.270-3) de “programas de ordenador o soporte lógico” ; b) Defraudación a los derechos patrimoniales de autor. Por cualquier medio o procedimiento, sin autorización previa y expresa del titular, reproduzca (art. 271-1); alquile o comercialice (art. 271-3); disponga, realice o utilice (art. 271-4), Recepcione, difunda o distribuya, por cualquier medio, sin autorización previa y expresa (art. 271-7), los programas de ordenador o soporte lógico; c) Violación a los mecanismos de protección de los derechos patrimoniales de autor y otros defraudaciones (art. 272).

II.- *Contravenciones de los datos o informaciones automatizadas contra un bien jurídico tutelado.* En el Código Nacional de Policía, (C.N.P.) se prevé las contravenciones especiales que “afectan la integridad personal”, la intimidad o la “vida íntima o privada de una persona” (artículos.46 a 49), cuando sin facultad legal se la averigüe hechos o datos de la intimidad, se los graba con cualquier medio tecnológico de información o comunicación que llama “subrepticios”, o los “divulga” u obtiene “provecho” de ese descubrimiento de información. Estas modalidades ilícitas se agravan si se hace a sabiendas, con conocimiento previo y sin justa causa.

El Código Nacional de Policía colombiano desde 1970, a diferencia del Código Penal Colombiano de 1980 y el Código Chileno ^[62], expresamente estipula el derecho a la intimidad de las personas como bien jurídico protegido contra agresiones que utilicen cualquier medio subrepticio (incluidos los informáticos) y persigan desvelar furtiva o ilegalmente hechos, actos o datos de la vida privada. Este código de 1970, ya preveía una modalidad de hecho punible (contravención) contra la intimidad, y quizá por ello el Código Penal Col., en 1980, se abstuvo aparentemente de proteger penalmente este bien jurídico específico en forma expresa y prefirió tutelar el descubrimiento de datos, hechos o actos de la vida privada o íntima tácitamente bajo el bien jurídico de *Libertad Individual y otras garantías*, como antes comentábamos ^[63], quizá para ampliar la cobertura al ámbito de datos o informaciones o “secretos” públicos y aumentar la dosimetría punitiva, relegando a la calidad de contravención contra la intimidad los aspectos netamente privados de la persona o la familia. Esta política criminológica del Estado, cuando menos, vulnera derechos fundamentales como el de igualdad (artículo13), el debido proceso (artículo29) y el de favorabilidad (artículo 29 *in fine*), pues “también es cierto que el principio de favorabilidad está esencialmente concebido para resolver conflictos entre leyes que coexisten de manera simultánea en el tiempo” ^[64]. Uno de los fines esenciales del Estado, es la eficacia de los derechos, deberes y principios consagrados en la Constitución (artículo2) y siempre prevalecerá los derechos inalienables de la persona (artículo 5) ^[65].

(44) RIVERA LLANO, Abelardo. *Dimensiones de la informática en el derecho*. Ed. Jurídica Radar, Santa fe de Bogotá, 1995, pág. 89 y ss.

(45) Ibídem pág. 89 y ss.

(46) MOLINA A. Carlos. *Introducción a la criminología*. Ed. Biblioteca Jurídica, Medellín, 1988, pág. 305 y ss.

(47) TIEDEMANN, K., citado por Molina A. ob. ut supra., pág. 307

(48) Ibídem.

(49) Sentencia T-80, Feb. 26/93. Corte Constitucional, Sala II., Rev. M.P. Eduardo Cifuentes. En: AA.VV. *Base de Datos Legis*. Ed. Legis. Santa fe de Bogotá (Col), pág.44-7.

(50) Legislación de Derechos de Autor o propiedad intelectual en Colombia, ha recogido mediante la incorporación legislativa al derecho interno, los diversos Convenio Universales que sobre el asunto se ha suscrito. En efecto, mediante la Ley 46 de 179, los mecanismos de protección al derecho autoral previstos por la OMPI en Estocolmo de 14 de Julio de 1967. Mediante Ley 23 de 1992, el Convenio de Ginebra para la protección de fonogramas contra la reproducción no autorizada; El tratado de Ginebra sobre registro internacional de obras audiovisuales, mediante Ley 26 de 1992; El Convenio de Berna para la protección de obras literarias y artísticas, por Dec. 1042 de 1994 y la

Decisión 351 del Pacto Andino, sobre propiedad intelectual. Las leyes 23 de 1982 y 44 de 1993, constituyen el marco normativo fundamental para la protección civil y penal de la propiedad intelectual en Colombia. Por lo que respecta al hecho punible (Delitos y Contravenciones) contra este derecho fundamental y de contenido omni-compreensivo, se regula en los arts. 30 y ss y arts.232 a 257, de las leyes citadas. En particular, sobre la protección al software, se estableció penas principales y accesorias severas que van desde la prisión y multas por la copia ilegal, la apropiación o el uso indebido de programas de computador hasta la incautación y destrucción de los productos informáticos obtenidos irregularmente por parte de la policía judicial.

- (51) Véase, ut supra, sobre el particular.
- (52) “ Y hoy, cuando casi se cumplen dos décadas del disco compacto, una nueva tecnología ha hecho su aparición, el DVD (Disco Digital Versátil), que supera en siete veces la capacidad de almacenamiento de su predecesor”. Vid. Diario EL MUNDO, Domingo 5 de abril de 1998, págs. 12 y 13 Barcelona España (www.elmundo.es). Igualmente, nuestro trabajo, **La Constitución...** ob. cit. págs.127 a 224. En: <http://akane.udenar.edu.co/derechopublico>
- (53) PEREZ LUÑO, Antonio Enrique. **Derechos humanos, estado de derecho y constitucional.** Ed. Tecnos, Madrid, 1984. págs. 359 y ss.
- (54) Vid. Corte Constitucional: Sent. T-414, Jun. 16 de 1992. M.P. Ciro Angarita; Sent. T-512, Sep.9 de 1992. M.P. José Gregorio Hernández; y, Sent. T-022, Ene. 29 de 1993, M.P. Ciro Angarita. En: AA.VV. **Base de Datos Legis.** Ed. Legis. Santafé de Bogotá (Col), pág.44-6 y ss.
- (55) Vid. Corte Constitucional: Sent. C-114, Marzo 25 de 1993. Sala Plena. Ob.cit. pág. 428.
- (56) Tal como lo analiza Londoño, el iusfilósofo Frosini V. en su obra “ **La protección de la intimidad: De la libertad informática, al bien jurídico informático**”, considera el derecho de habeas data como una extensión del derecho a la intimidad o del “right to privacy”, pero con un contenido actual más acorde con la realidad. La autora se refiere, a la concepción del “habeas data como aquél derecho que surge fruto de la tecnología informática y que pretende solucionar el conflicto generado por la violación de los derechos a la intimidad y a la información y el conflicto que entre ellos se ha ocasionado. Es un derecho moderno, reciente y en inminente evolución”. En ésta última visión se desconoce el concepto de habeas data por procesos diferentes a los automatizados. **Informática jurídica y derecho informático.** Ed. Señal, s/n, Medellín (Col), pág. 33 y ss.
- (57) Por el contenido, se tiene la dificultad para delimitar el verdadero contenido de la intimidad, por el contrario al del habeas data que tiene un carácter objetivo en su definición (“la libertad reside en la habilidad para controlar el uso que de esos datos personales se haga en un programa de computador” y de contenido “muy amplio”, es el derecho al acceso de los bancos de datos, el derecho a verificar su exactitud, el derecho a verificar su exactitud, el derecho a actualizarlos y a corregirlos, el derecho a mantener en secreto a los datos sensibles, el derecho a ningún pronunciamiento acerca de los llamados ‘datos sensibles’ “). “La teoría tradicional de los derechos humanos solo hace referencia a su exigencia frente al Estado, y aunque el derecho a la intimidad generalmente se ha hecho valer por un particular frente a otros particulares, el Habeas Data ha aumentado su alcance... El Habeas Data es un derecho humano que en su moderna tendencia coloca a los particulares con una responsabilidad muy clara frente al respeto de estos derechos. Todo lo anterior no nos autoriza --sostiene-- sin embargo a negar que la garantía de protección del Habeas Data pertenece y se hace exigible a través del Estado”. Ob. cit. pág. 33 y ss.
- (58) Sent. T-002, Mayo 8 de 1992, Corte Constitucional. M.P.: Alejandro Martínez C., En: AA.VV. **Base de Datos Legis.** Ed. Legis. Santa fe de Bogotá (Col), pág. 722.
- (59) VALLE MUÑOZ, José M. Ob. ut cit. pág. 489
- (60) Sent. 1617 de dic. 14 de 1990. Sala Contencioso Administrativo. Sec. I. M. P.: Dr. Rodrigo Viera P.
- (61) QUINTERO OLIVARES, Gonzalo. Ob. ut supra cit. pág. 572. Los paréntesis son nuestros.
- (61A) **TITULO VIII DE LOS DELITOS CONTRA LOS DERECHOS DE AUTOR. CAPITULO UNICO.**
“Artículo 270. *Violación a los derechos morales de autor.* Incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte (20) a doscientos (200) salarios mínimos legales mensuales vigentes quien:
1. Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.
2. Inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.
3. Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.
Parágrafo. Si en el soporte material, carátula o presentación de una obra de carácter literario, artístico, científico, fonograma, videograma, programa de ordenador o soporte lógico, u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho, en los casos de cambio, supresión, alteración, modificación o mutilación del título o del texto de la obra, las penas anteriores se aumentarán hasta en la mitad.
Artículo 271. *Defraudación a los derechos patrimoniales de autor.* Incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte (20) a mil (1.000) salarios mínimos legales mensuales vigentes quien, salvo

las excepciones previstas en la ley:

1. Por cualquier medio o procedimiento, sin autorización previa y expresa del titular, reproduzca obra de carácter literario, científico, artístico o cinematográfico, fonograma, videograma, soporte lógico o programa de ordenador, o transporte, almacene, conserve, distribuya, importe, venda, ofrezca, adquiera para la venta o distribución, o suministre a cualquier título dichas reproducciones.
2. Represente, ejecute o exhiba públicamente obras teatrales, musicales, fonogramas, videogramas, obras cinematográficas, o cualquier otra obra de carácter literario o artístico sin autorización previa y expresa del titular de los derechos correspondientes.
3. Alquile o de cualquier otro modo comercialice fonogramas, videogramas, programas de ordenador o soportes lógicos u obras cinematográficas, sin autorización previa y expresa del titular de los derechos correspondientes.
4. Fije, reproduzca o comercialice las representaciones públicas de obras teatrales o musicales, sin autorización previa y expresa del titular de los derechos correspondientes.
5. Disponga, realice o utilice, por cualquier medio o procedimiento, la comunicación, fijación, ejecución, exhibición, comercialización, difusión o distribución y representación de una obra de las protegidas en este título, sin autorización previa y expresa de su titular.
6. Retransmita, fije, reproduzca o por cualquier medio sonoro o audiovisual divulgue, sin autorización previa y expresa del titular, las emisiones de los organismos de radiodifusión.
7. Recepcione, difunda o distribuya por cualquier medio, sin autorización previa y expresa del titular, las emisiones de la televisión por suscripción.

Parágrafo. Si como consecuencia de las conductas contempladas en los numerales 1, 3 y 4 de este artículo resulta un número no mayor de cien (100) unidades, la pena se rebajará hasta en la mitad.

Artículo 272. *Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.* Incurrirá en multa quien:

1. Supere o eluda las medidas tecnológicas adoptadas para restringir los usos no autorizados.
2. Suprima o altere la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada.

3. Fabrique, importe, venda, arriende o de cualquier forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal, o de cualquier forma de eludir, evadir, inutilizar o suprimir un dispositivo o sistema que permita a los titulares del derecho controlar la utilización de sus obras o producciones, o impedir o restringir cualquier uso no autorizado de éstos.

4. Presente declaraciones o informaciones destinadas directa o indirectamente al pago, recaudación, liquidación o distribución de derechos económicos de autor o derechos conexos, alterando o falseando, por cualquier medio o procedimiento, los datos necesarios para estos efectos”.

- (62) En el Código Penal chileno se estructura un tipo delictivo específico pluri-defensivo con acciones múltiples dirigidas a proteger el derecho de la información. Aunque el tipo adolece de un técnica político-penal, solución de otra parte, los innumerables problemas que se presentan con el proceso automatizado de la información desde la fase de recolección (“input”), pasando por la fase de procesamiento propiamente dicho (“in”), hasta llegar a la fase de recuperación o salida de información (“output”). Este tipo penal subsume por tanto, las figuras delictivas previstas en la clasificación de *Tiedemman y Molina A.*. En efecto, se prevé “el acceso indebido, el apoderamiento, la destrucción, inutilización, transformación o desfiguración de una información con el fin de impedir u obstaculizar su procesamiento automático o de revelarla o transmitirla indebidamente”, además como lo sostiene *Correa*, desde el proyecto de la nueva figura delictiva se propuso agravar la pena de los demás delitos cuando éstos sean cometidos por medios informáticos. Vid. CORREA, C. **Informática y derecho**. Ed. Depalma, Buenos Aires, 1988, pág.24
- (63) Véase, aparte ut supra 4.2.4, punto 1.1. Delitos de los datos o informaciones automatizadas.
- (64) Vid. C. Const., Sent. T-430, Jul. 1/90. M.P. Eduardo Cifuentes .
- (65) Vid. C. Const., Sent. T-490, Ago.13/92. M.P. Eduardo Cifuentes.

Actualización: Pasto, Abril 1 de 2008

[INICIO](#)