REVISTA ELECTRONICA DE DERECHO PUBLICO MINIMO

ENSAYOS JURÍDICOS EN DERECHO PUBLICO

Por
Libardo Orlando Riascos Gómez
Doctor en Derecho
Lriascos@udenar.edu.co
2010

EL DELITO INFORMATICO CONTRA LA INTIMIDAD Y LOS DATOS DE LA PERSONA EN EL DERECHO COLOMBIANO

CONTENIDO

RESUMEN: El presente ensayo jurídico, titulado El delito informático contra la intimidad: una visión constitucional y penal, tiene por objeto el estudio socio jurídico del derecho fundamental a la intimidad en la Constitución y legislación penal colombiana vigentes. Igualmente se hace un

estudio comparado con las legislaciones penales alemana, canadiense y española, a efectos de acercarnos al análisis y tratamiento jurídicos que estas legislaciones le dan al fenómeno informático contra la intimidad. Igualmente, hacemos un análisis detallado de los tipos penales previstos en el Código Penal Colombiano vigente (Ley 599 de 2000) y proponemos a manera de conclusión, un tipo penal complejo para proteger la intimidad de las personas que se ven ante atentados con medios comisivos electrónicos, telemáticos o informáticos o medios (TIC). Finalmente hacemos un relación de los tipos penales creados por la ley 1273 de 2009 que pretenden tutelar el bien jurídico tutelado de la "información y de los datos" personales en Colombia.

Palabras Claves: Intimidad, delito informático, Constitución, medios comisivos penales, medios TIC.

ABSTRACT: The present juridical, titled rehearsal: "The computer crime against the intimacy: the constitutional of vision and penal", this has for object the study juridical partner of the right principle a the intimacy in the Constitution the legislation of and the effective of the penal Colombian. Equally a study is made compared against the German, Canadian penal legislations the Spanish one of and, an effects of the analysis of to the one of coming closer the and juridical treatment that these legislations give to the computer phenomenon against the intimacy. Finally, we make a detailed analysis of the penal types foreseen in the Code the effective of Penal Colombian (Law 599 of 2000) the we propose of and a way of the conclusion, type of the complex to protect the penal intimacy of the people that see each other before attacks against the electronic ones of commisive of means, telematic, the computer ones of or the means (TIC). Finally we make a relationship of the penal types created by the law 1273 of 2009 that seek to guarantee the real juridical one denominated of the "information and of the data" personal in Colombia.

keys Words: Intimacy, computer of the crime, Constitution, penal of commisive of means, TIC of the means.

1. Regulación normativa del fenómeno informático y la intimidad.

A partir de la segunda mitad del siglo XX --lo cual era presumible, después de la barbarie de la II guerra mundial--, la preocupación de las políticas criminológicas de los Estados Democráticos y de Derecho, por la vulneración de los derechos humanos continua e insistentemente tabuladas, evaluadas y analizadas por los criminólogos alemanes, italianos, centroeuropeos y americanos, dejaron de priorizarse, casi única y exclusivamente con base en las convencionales delincuencias de "sangre", las "patrimoniales" o cualquiera otra que atentara contra un bien jurídico protegido y protegible tradicionales, para regular y profundizar en su protección otros bienes jurídicamente tutelados como la dignidad, la honra, el buen nombre, la imagen y la intimidad de las personas, amenazados por medios tradicionales o por medios informáticos o telemáticos, tal y como se puede constatar con la simple lectura de los diversos catálogos punibles de los Estados modernos americanos, los del derecho consuetudinario anglosajón o los del ámbito de la *Common Wealth* en sus "Crimes Act"[1].

En tal virtud, las nuevas preocupaciones; entre muchas otras, pero especialmente las devenidas del fenómeno tecnológico de la información y comunicación por medios electromagnéticos (informáticos y/o telemáticos) , se reflejaron en la doctrina de criminólogos y iuspenalistas, con carácter correctivo, represivo y punitivo y acogido inmediatamente por los Estados en sus diferentes leyes especiales y diversos Codex penales, antes que con carácter preventivo y civilista, en las normas administrativas, las cuales paradójicamente, fueron adoptadas por varios Estados cuando ya se habían expedido estatutos penales que reprimían la actividad humana a través de equipos computacionales o telemáticos, en sus

múltiples formas y pretendían proteger y tutelar derechos fundamentales, como la intimidad, la honra, la imagen, etc. [2], plasmados paulatinamente en las respectivas Constituciones Estatales; o bienes jurídicos específicos, como los patrimoniales y socio-económicos.

Las nuevas actividades humanas transgresoras de derechos fundamentales no patrimoniales (también llamados de la persona o la personalidad) y patrimoniales --se sostiene--, cobraron relevancia con el surgimiento de la tecnología informática [3], el multitratamiento de la información y la comunicación por medios electrónicos, por el avance y gran poder de la teletransmisión de datos sin fronteras [4]; la excesiva libre oferta-demanda de equipos computacionales personales (PC o "personal computer" u "ordenadores"), corporativos o empresariales e incluso industriales ("hardware": unidades de procesamiento y periféricas, como los MODEM); y sobre todo, por el fácil acceso, tratamiento, uso y abuso de programas computacionales o "software", los "ficheros" o bases de datos (de toda clase, fin, servicio y origen público o privado, existentes), por parte de las personas sin distingo de edad o parámetro de distinción alguno, con autorización o sin ella.

2. Los derechos fundamentales de acceso a la información, el habeas data y la intimidad en el ordenamiento jurídico.

2.1. En el ámbito del derecho público.

El proceso de tratamiento informatizado de la información o de los datos de carácter personal, comporta una serie de etapas, fases o ciclos informáticos (recolección, selección, tratamiento, almacenamiento, registro, recuperación y uso de datos [5]). Las diferentes legislaciones del mundo han regulado este procedimiento informático desde el punto de vista del derecho administrativo y civil y para protegerlo como *ultimo ratio*, en todo o en parte, se han añadido mecanismos jurídicos de tipo penal, para tutelar los derechos al acceso a la información, las facultades estructurales del *habeas data* (conocimiento, actualización, rectificación y cancelación de datos); y por supuesto, los derechos fundamentales, tales como la intimidad.

El derecho de acceso a la información que tiene toda persona se encuentra regulado en las diversas constituciones del mundo como un derecho fundamental y personalísimo e indefectiblemente se halla vinculado con otros no menos importantes y de igual rango constitucional, como el derecho a informar y ser informado y el derecho a la intimidad personal y familiar, tal como sucede en Colombia en 1991[6] y en España en 1978 [7].

Hoy por hoy, en la llamada *era de la informática*, el derecho de acceso a la información adquiere relevancia capital que oscila entre el mayor o menor grado de poder de control sobre los datos o informaciones que conciernen a las personas cuando se hallen almacenados, registrados, conservados o transmitidos por medios informáticos, electrónicos o telemáticos por personas naturales, jurídicas, públicas o privadas, según fuere el caso. En dicho marco, se produce el binomio derecho-protegido y derecho-vulnerado y el correspondiente equilibrio ponderado que deviene principalmente de los límites constitucionales y legales de los derechos y libertades fundamentales en éste involucrados y que tanto hemos comentado a lo largo esta investigación.

Los diversos Estados, tras constitucionalizar el derecho de acceso a la información y el habeas data, han optado por la técnica legislativa para cumplir con su papel proteccionista o garantísta del conjunto de derechos y libertades fundamentales.

En efecto, así se ha procedido en el Canadá al emitir leyes que regulan los derechos de acceso a la información y el derecho a la intimidad (Access to information Act, 1980-1983; Privacy Act 1980-83), igual en Australia (Freedom of information Act 1982, complementada por la Privacy and

Data Protection Bill, 1994 -NSW-; Privacy Act, 1988); en Alemania (Ley Federal Alemana de Protección de Datos, Enero 27 de 1977, reformada el 20 de diciembre de 1990); en España (*Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal* o nueva LORTAD, L.O.15/99, Dic. 13. Ley 30/1992, Ley de Régimen Jurídico de las Administraciones públicas y procedimiento administrativo común. LRJPA, arts. 37 y 45, sobre *documentos informáticos, electrónicos y telemáticos* y el R.D. 263/1996, Feb.16.,sobre la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado. Además las normas comunitarias sobre la materia v.gr. Convenio de 1981 y la Directiva 46/95/CE y 97/66/CE, relativas a teletransmisión de datos e intimidad.

En Colombia, los derechos fundamentales del acceso a la información, el habeas data, el buen nombre, la imagen y la intimidad están regulados en el artículo 15 de la Constitución de 1991, la Ley 57 de1985 o Estatuto de la Información, El Código Contencioso-Administrativo (Dec.01/84, Dec.2304/89 y ley 446 de 1998), La Ley 44 de 1993, reformada parcialmente por la Ley 719 de 2001, sobre derechos de autor; la Ley 527 de 1999, sobre el documento electrónico y teletransmisión de datos personales, la Ley 599 y 600 de 2000, Códigos Penal y Procesal Penal Colombiano, el Código de Procedimiento Civil; la Ley 716 de 2001, reglamentada por el Decreto 81 de 2002, sobre caducidad de datos o información histórica negativa en las bases de datos; Ley 795 de 2003, relativa al sistema financiero colombiano y reformatoria del comercio y transmisión electrónica de datos previstos en la Ley 527 de 1999; y finalmente el proyecto refundido de Ley Estatutaria (Número 221/2007, Cámara de Representantes y Número 027/2006, del Senado de la República) y la Ley Estatutaria del procedimiento electrónico de datos financieros públicos y privados en Colombia o Ley de Habeas Data Financiera (Ley 1266 de 2008, Diciembre 26), proyecto que tantas veces presentado al Congreso de la República por diferentes actores parlamentarios, gubernamentales y hasta de la Defensoría del Pueblo y resultaron fallidos unas veces porque ni siquiera hacia tránsito legislativo normal o en una sola oportunidad por el control de constitucionalidad previo de la Corte Constitucional por vicios de forma [7 bis].

2.2. En el ámbito del derecho punitivo canadiense y español.

En el ámbito penal y como *ultima ratio,* los Estados mencionados, han previsto normas específicas en sus códigos penales para reprimir las conductas que se realizan con medios o equipos electromagnéticos, computacionales o telemáticos que atenten contra bienes jurídicos no patrimoniales o derechos fundamentales como el de acceso a la información o *habeas data*, la intimidad personal y familiar, la propia imagen, el honor; entre muchos otros, o también cuando atente contra bienes patrimoniales genéricos o de tratamiento jurídico *sui géneris* como la "propiedad intelectual e industrial".

Los Códigos Penal español y canadiense hacen referencia específica a la intimidad como bien jurídico protegido [8], aunque con diferente visión y cobertura de protección estatal según las fases del tratamiento electromagnético de la información, como en seguida puntualizamos.

Por su parte, el Código Penal Canadiense en el Tít. VI "*Invasion Privacy*" (arts. 183 a 196), extiende la protección penal a la intimidad desde la fase de primaria o "*input*" de datos (recolección), la fase *"in*" o de tratamiento electromagnético propiamente dicho (almacenamiento, registro y conservación de datos) hasta la fase "*output*" de la información (comunicación: emisión/recepción de datos). Los delitos utilizando medios manuales, mecánicos, informáticos o telemáticos o la información misma como objeto material de los estos, son: 1. Interceptación de datos o informaciones de particulares, sin su consentimiento (art.184); 2. Interceptación de datos consentida por una de las partes (art.184.1 y 2) y/o por telecomunicaciones u otros medios tecnológicos (art.184.3); 4. Interceptación judicial de datos en circunstancias excepcionales (art. 184.4); 5. Interceptación de datos o información a través de dispositivos Electro-magnéticos, mecánicos o telemáticos, con fines de lucro (art. 184.5); 6. Interceptaciones autorizadas (art. 185);

7. Interceptación por autorización judicial. Excepciones. (art.186); 8. Interceptación de un dato o información secreta o confidencial. Agravantes (art. 187); 8. Interceptación por autorización judicial en casos especiales (art. 188); 9. Posesión o compraventa de dispositivos electromagnéticos o informáticos utilizados en la interceptación subrepticia de datos. (Art. 191); 10. Descubrimiento o revelación de la información sin consentimiento con medios mecánicos, informáticos o electromagnéticos (art. 193); y, 11. Descubrimiento de datos o informaciones interceptadas, sin consentimiento, a través de medios electromagnéticos, mecánicos e informáticos (art. 193.1).

En España, el profesor *Morales Prats* [9], previa distinción de la fases del ciclo informático (recolección, registro o "programación", y transmisión de la información), confirma que la protección jurídico penal de los derechos fundamentales como el de la intimidad, la imagen e incluso el honor se extiende a partir del registro de los datos de carácter personal, es decir, a partir de la fase que llama de tratamiento o programación. En tal virtud, las fases previas a ésta (como la de recolección y almacenamiento de la información) se protegen o tutelan bien civil y/o administrativamente por las autoridades competentes. El autor citado, al comentar los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio, Título X, del Código Penal de 1995 (arts. 197 a 201), en forma prolija estudia la terminología técnica, jurídica e informática empleada en la regulación de las "infracciones administrativas" previstas en la LORTAD (art. 42 y ss.) y los delitos del artículo 197.2, pues a su juicio, la LORTAD gana en identificación y precisión terminológica, de la que adolece el código penal, a tal punto que causa incertidumbre y "parece que el desconcierto y la precipitación han precedido la creación de éste precepto" (art.197).

En el ámbito jurídico español "extrapenal" ("infracción administrativa") o contravencional del derecho colombiano, la protección jurídica administrativa alude al momento mismo de la recolección y "en forma especial por la salvaguarda de los derechos nucleares del *habeas data*, esto es, los derechos de información, acceso, rectificación y cancelación sobre los datos personales", realizada por la Agencia Protectora de Datos Española, la cual entre otras facultades tiene, las de "preventivas de control, supervisión e inspección que le otorga la LORTAD en el ciclo operativo del banco de datos". *Arroyo Zapatero* [10], en esta misma línea de crítica, manifiesta que "la tutela penal, para ser eficaz debería haberse extendido a todas las fases del ciclo informático, desde la creación de los ficheros informáticos hasta la alteración y transmisión ilícita de los datos registrados". Sin embargo, con fundadas razones un sector de la doctrina española, reconoce que no es fácil para el operador jurídico distinguir, en este punto, los linderos entre infracción administrativa y delito cuando se atenta contra los datos de carácter personal o informaciones personales, a tal punto que se evidencia un cierto solapamiento en algunas acciones de origen aparentemente administrativo que en otras legislaciones han merecido tipificación penal [11], o más aún, cuando infracciones y sanciones administrativas [12] por su contenido son verdaderos delitos y penas [13], correspondientemente suavizados por la mano mágica de la naturaleza ius-administrativa.

2.3. En el ámbito del derecho punitivo Australiano y Alemán

En los Códigos Penal Australiano y Alemán, relacionan las conductas humanas en las que se utilizan medios o equipos computacionales, electromagnéticos y telemáticos que atenta contra el *habeas data,* los datos de carácter particular y los datos o informaciones de valor "económico". En efecto, en el "Crimes Act 1914" Australiano (*Computer related Commonwealth law*) en la Parte VIA y VIB, arts. 76A a 76E y 85ZE, se relacionan los siguientes delitos ("*offence*"): 1. Acceso no autorizado a los datos; 2. Destrucción, modificación e impedimento de acceso a los datos; 3. Acceso no autorizado de los datos utilizando medios informáticos o telemáticos; 4. Destrucción, Modificación o impedimento de acceso a los datos utilizando medios informáticos y telemático; 5. Delito de hostigamiento ("delito conductista" behavorístico) mediante el uso de medios informáticos.

En Alemania, la denominada "Segunda Ley para la lucha contra la Criminalidad Económica (2.WIKG) de 15 de Mayo de 1986., relaciona una variada gama de hechos punibles cometidos con medios electromagnéticos o informáticos o de la información como bien jurídico u objeto material de los mismos, acorde con la realidad tecnológica en la que vivimos. En esta relación punitiva podemos encuadrar los *delitos contra los datos* o las informaciones, a diferencia de la legislación canadiense donde se destacan los *delitos de los datos* contra otro bien jurídico como la intimidad. La legislación española como veremos prevé una y otra clasificación.

Las formas típicas del derecho alemán son: 1. Espionaje de datos (Arts. 202 a StGB); 2. Estafa informática (263 a StGB) ; 3. Utilización abusiva de cheques o tarjetas de crédito (266 b StGB); 4. Falsificación de datos con valor probatorio (269 StGB); 5. Engaño en el tráfico jurídico mediante elaboración de datos (270 StGB); 6. Falsedad ideológica (271 StGB); 7. Uso de documentos falsos (273 StGB); 8.Destrucción de datos (303 a StGB); y, 9. Sabotaje informático (303 StGB).

2.4. EN EL ÁMBITO DEL DERECHO PUNITIVO COLOMBIANO

2.4.1. Regulación del bien jurídico de la intimidad en el Código Penal de 1980 y en el Código de Policía de 1970.

En Colombia, como precisaremos *ut infra*, el Código Penal de 1980 (--C.P. Col--, derogado por la Ley 599 de 2000 o C.P. vigente) no tiene referencia expresa, pero sí tácita al derecho de *Habeas Data* y/o a la intimidad como bienes jurídicos protegibles de cualquier atentado por parte de la informática o telemática dentro del género del bien objeto del Título X, "*De los Delitos contra la Libertad Individual y otras garantías*". En efecto, dos razones convincentes nos llevan a sostener este argumento: por una lado, debemos tener en cuenta que en una etapa de la evolución de los derechos fundamentales, éstos retomaron la configuración, estructura y contenido de las viejas "libertades constitucionales" del liberalismo clásico y post-industrial anglo-francés a la que no escaparon el habeas data y la intimidad; y por otro lado, tanto el derecho de *habeas data* como la intimidad o "privacy", tienen hoy una identidad propia en la Constitución Colombiana de 1991 (art.15), a pesar de que aquél Código Penal todavía mantenía ese origen nominativo y genérico de "Libertades Públicas" como bien jurídico protegible penalmente para referirse a una variopinta gama de derechos hoy considerados fundamentales dentro de los que están los mencionados.

En efecto, la Constitución, en el Titulo II, "De los derechos, las garantías y los deberes", Cap. I. "De los Derechos Fundamentales", art. 15, "Derecho a la intimidad personal y familiar", constitucionaliza los derechos a la intimidad y el *habeas data,* al fusionarlos en un mismo artículo, bajo la fórmula siguiente: "*Todas las personas tienen derecho a su intimidad...Del mismo modo, tiene derecho a conocer, actualizar y rectificar las informaciones...*" entendiendo el constituyente del 91, que éste último es una consecuencia lógica de la estructuración de la intimidad y no otro derecho también fundamental que tiene su sustento en el derecho a la información (art.20 y 73 ibídem), en el desarrollo de la personalidad (art. 16 id.) y en los valores constitucionales de la dignidad, respeto y solidaridad humanos (art. 1 id.) que no sólo a la intimidad puede servir de sustento, afección, restricción o límite o auto-límite constitucional sino al cúmulo de derechos fundamentales previstos en el Título II de la Constitución, pues en un estado social de derecho y democrático no existen derechos absolutos. Por contra, la Corte Constitucional Colombiana estima que la intimidad es un derecho absoluto (Sentencia T-022, Ene. 29/92).

Más aún, el artículo citado en el tercer inciso constitucionaliza el procedimiento o tratamiento automatizado de la información al decir: "*En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución"*, con lo cual no deja duda que el habeas data tiene identidad constitucional en el derecho colombiano y consagra derechos limitados por la propia Constitución y los demás derechos.

El fenecido C.P.Col.,del 80, bajo el concepto genérico de libertades públicas subsume a la intimidad como bien jurídico protegible de cualquier conducta humana que utilice medios electromagnéticos, computacionales o telemáticos en el Título X, Cap.V., del C.P. Col., al referirse a los delitos de "violación de secretos y comunicaciones", y en concreto, a: 1. La violación ilícita de comunicaciones" (art. 288); y, 2. La "violación y empleo de documentos reservados" públicos o privados. Así mismo, por los delitos previstos en la legislación especial Decr. Ext. 2266 de 1991: "utilización ilícita de equipos transmisores o receptores", incluidos los "electrónicos" --informáticos o telemáticos--, (art.16), y "interceptación ilícita de correspondencia oficial" (arts. 18) . La honra prevista en el artículo 21 Constitución Colombiana ("Honor" en el derecho español), también puede ser objeto de atentado de los medios tecnológicos de información y comunicación colectivos, y en tal virtud, se prevén los delitos de injuria y calumnia (arts.313 y ss del C.P. Col.), al estar incorporados en el bien jurídico tutelado de "la Integridad Moral".

Ahora bien, las conductas punibles en Colombia se divide en delitos y contravenciones (art. 12 del C.P.Col del 80 y art.19 del C.P.de 2000.), y éstas a su vez se dividen en ordinarias y especiales (art. 12 del *Código Nacional de Policía*: Decretos 1355-2055 de 1970 y 522 de 1971, modificados parcialmente por la Ley 23 de 1991 y Ley 228 del 93), atendiendo a la gravedad o levedad de la infracción y la sanción, el bien jurídico tutelado y la competencia de las autoridades. En tal virtud, siendo más graves las contravenciones especiales, se ha ubicado después de atribuir competencia a las autoridades administrativas locales y regionales, con funciones cuasi jurisdiccionales [14] y asignarles el conocimiento de las contravenciones "que afectan la integridad personal", la intimidad o la "vida íntima o privada de una persona" (arts.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.

2.4.2. Regulación del bien jurídico de la intimidad en el Código Penal de 2000.

La Ley 599 de 2000, Julio 24 o Código Penal Colombiano vigente, regula en forma expresa la protección jurídico penal del bien no patrimonial denominado la intimidad y su visión-iusinformática (habeas data [15]) cuando hace referencia a los "*Delitos contra la libertad individual y otras garantías", "De la Violación a la intimidad, reserva e interceptación de comunicaciones (Título III, Capítulo 7),* así: 1) *Violación ilícita de comunicaciones* (art. 192), 2) *Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas* (art. 193), 3) *Divulgación y empleo de documentos reservados* (art. 194), 4) *Acceso abusivo a un sistema informático* (art. 195), 5) *Violación ilícita de comunicaciones o correspondencia de carácter oficial* (art.196), 6) *Utilización ilícita de equipos transmisores o receptores* (art.197).

Los anteriores tipos penales pueden ser preparados, realizados, ejecutados o consumados a través de medios tradicionales (aparatos eléctricos o mecánicos de cualquier tipo o forma o documentos escritos) como medios informáticos, electrónicos o telemáticos, también conocidos como medios TIC o de información y comunicación electrónica. A efectos del objeto de este ensayo jurídico, nos referiremos a estos últimos, teniendo en cuenta que hoy por hoy, se acepta universalmente la existencia de los delitos informáticos, vale decir, aquellos que Tiedemann, sostiene:

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...[16]

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 Arrubla., siguiendo a *Tiedemann*, 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 produje 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.

2.5.1. Los tipos punibles informáticos contra la intimidad en nuestro Código Penal.

2.5.1. Intimidad, Datos personales y medios informáticos.

Previo al breve análisis constitucional y penal de los delitos regulados en los artículos 192 a 197 del C.P. de 2000, conviene precisar los siguientes términos, dilucidados ampliamente en el derecho comparado, estos son: a) La intimidad y la visión iusinformática, b) Datos personales contenidos en soportes y/o medios electrónicos o telemáticos; y, c) Los Medios de software y hardware o informáticos.

La intimidad universalmente ha sido considerado como un derecho fundamental del ser humano que hunde sus raíces en valores constitucionales como la dignidad humana, el respeto mutuo, el libre desarrollo de la personalidad y en el conjunto de principios y atribuciones que definen a la persona en nuestra sociedad actual y hacen parte de lo que hoy constituye un Estado Social de Derecho. Así se plasma en nuestra Constitución en al artículo 15, pero recordando que éste como otros derechos fundamentales no son absolutos y que están limitados por otros derechos de igual rango, por el ordenamiento jurídico vigente, por una serie de intereses, valores y principios constituciones y por los derechos de los demás.

Recientemente, por los avances tecnológicos de la información y la comunicación (o medios TIC, acuñados por el profesor Ethain Katsh [17]), unidos a los porosos, penetrantes y complejos desarrollos de la informática, electrónica y telemática, el derecho a la intimidad personal y familiar regulado universalmente por las Constituciones con excelsa protección y tutela jurídica, se ha visto amenazado, vulnerado e incluso desaparecido.

La informática jurídica o ius-informática, hace referencia al tratamiento lógico, con soportes, equipos y medios electrónicos de la información o datos personales generados o transferidos por el ser humano.

Los datos de carácter personal o informaciones de todo tipo de los seres humanos, o *"cualquier información concerniente a personas físicas, identificadas o identificables*", según la Ley Orgánica española de tratamiento sistematizado de datos (L.O. No.15 de 1999). La persona identificada es aquella a quien se puede determinar directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos de su identidad física, fisiológica, psíquica, cultural o social. La persona identificable, según la norma citada, también se le denomina "interesado" o impropiamente "afectado", pues destaca el aspecto negativo del derecho que tiene una persona (v.gr. la vulnerabilidad) y no el positivo de ser titular de los mismos o tener intereses legítimos para ejercitarlos en las condiciones previstas en el ordenamiento jurídico vigente.

En términos ius-informáticos, las expresiones *"cualquier información"* , deben integrarse como una unidad de datos (textual, imagen o sonido) representada en forma binaria (0/I) en el tratamiento computarizado de datos y relativos a una persona natural o física.

En otras latitudes como la Canadiense, por ejemplo han preferido no utilizar el concepto genérico de datos o informaciones personales, sino una relación de los que se consideran como tales, y aunque es una relación *numerus clausus,* la interpretación hermenéutica posibilita la actualización del listado*.* La "*Act Privacy"* canadiense [18], previamente entiende como "*personal information",* la concerniente a una persona, cualquiera sean los mecanismos o tecnologías de las que se obtengan o graben, para luego relatar los siguientes supuestos de información personal:

1) La información relacionada con la raza, origen nacional o étnico, color, religión, edad o estado civil de la persona.
2) la información relacionada con la educación, el historial médico, delictivo, laboral de la persona, o la información relacionada a las transacciones financieras en las que el individuo ha estado involucrado.
3) cualquier número o símbolo que identifique o se le asigne a una persona.
d) la dirección, las huellas digitales o el tipo sanguíneo de la persona.
4) las opiniones o ideas personales, excepto aquellas vertidas sobre otra persona, o sobre una propuesta de subvención, recompensa o un premio otorgado por una institución gubernamental, sección, departamento o Ministerio, según lo estipulen sus reglamentos.
5) la correspondencia enviada a una institución gubernamental por una persona que es implícita o explícitamente de naturaleza privada o confidencial, así como las contestaciones a la misma en la medida que revelen un contenido que corresponda a la envida originalmente.
6) las ideas u opiniones de otra persona sobre él.
7) las ideas u opiniones de otra persona sobre una propuesta de subvención, recompensa o premio otorgado por una institución gubernamental, sección, departamento o Ministerio, según lo estipulen sus reglamentos y referida en el parágrafo (e), pero excluyendo el nombre de la otra persona sobre la cual dedicó sus ideas u opiniones.
8) el nombre de la persona que aparece relacionada con otra información personal y que el sólo descubrimiento del verdadero nombre revelaría información sobre aquél; pero para los propósitos de artículos 7, 8 y 26 de ésta ley y el artículo 19 de la LAIC (Ley de acceso a la información canadiense. *Access to information Act*), la información personal queda excluida.
9) La información de una persona que es, o fue funcionario o empleado de una institución gubernamental y relacionada con la posición o funciones del mismo. Esta información incluye: 1. el hecho de que el individuo es o era funcionario o empleado de la institución gubernamental; 2. el título, dirección comercial y número del teléfono de la persona; 3. la clasificación, rango y monto del sueldo y atribuciones según su cargo; 4. el nombre de la persona que figura en un documento preparado por éste en el ejercicio de su empleo; y, 5. las ideas u opiniones personales expresadas en el curso de su empleo.

10) la información sobre una persona que desempeña o desempeñó los servicios bajo contrato con una institución gubernamental. Esta información incluye: los términos del contrato, el nombre del individuo y las opiniones o ideas expresadas en el transcurso del mismo.
11) información relacionada con cualquier beneficio discrecional de naturaleza financiera, incluida la concesión de una licencia o permiso, así como nominación del mismo, el nombre de quien la confirió y la naturaleza precisa de la misma.; y,
12) la información sobre una persona muerta y hasta por veinte (20) años.

La regla general para la protección de *toda información personal* en el derecho canadiense es el no descubrimiento o divulgación de los datos o las informaciones de carácter personal cuando no haya consentimiento de una persona a quien concierne una información catalogada de personal y siempre que ésta se halle bajo el control o responsabilidad de una institución gubernamental. La excepción, es que se podrá descubrir la información previo un procedimiento administrativo breve y sumario en las doce situaciones previstas en el *Act Privacy*. Estas que se pueden catalogar de excepciones al descubrimiento o divulgación de la información por parte de un organismo del Estado, tienen como fundamento la realización de algunos de los fines de un Estado de derecho, tales como la seguridad, la defensa, la salubridad y la economía públicas, o bien los intereses generales, públicos, de relaciones internacionales, investigativos (judiciales o administrativos), científicos o archivísticos o, en últimas, los del concernido o interesado con la información.

En el derecho de la Comunidad Europeo los datos personales referidos al origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad, tienen un grado de protección jurídica mayor a la de los demás datos de carácter personal. Protección que llega hasta prohibir, restringir o limitar el procesamiento automatizado de los mismos (artículo 8.1 de la Directiva 95/46/CE). Por ello, a estos datos personales se les conoce en la doctrina universal como "*datos sensibles"*, pues sólo pueden ser recolectados, almacenados, tratados o transmitidos por medios informáticos o electrónicos cuando media autorización expresa y escrita del titular ("principio de autodeterminación" de los datos como lo denomina la Ley de Tratamiento de Datos Española de 1999).

Finalmente, el medio informático, es aquel *"mecanismo, la instalación, el equipo o los sistemas de tratamiento de la información que permite, utilizando técnicas electrónicas, informáticas o telemáticas, producir, almacenar o transmitir documentos, datos e informaciones*. (art.3, b), R.D. 263/1996, 16 de Febrero). En esta definición se incorporan *in genere* los medios físicos o materiales, tanto referidos al denominado *Hardware* (el ordenador, propiamente dicho y las unidades periféricas), como a los medios lógicos, logiciales o de *software* (programas de ordenador), utilizados en el procedimiento o tratamiento automatizado de todo tipo de información o datos. Así mismo, a todos aquellos aparatos o sistemas electrónicos que no haciendo parte del hardware o el software, sirven a los fines y objetivos informáticas, al complementar o potenciarlos. Tal es caso del conjunto de aparatos y sistemas de telecomunicaciones unidos a los eléctricos y/o electrónicos que sirven para captar, editar, emitir o transferir imágenes, sonido o texto; o todo a la vez, pues al fin y al cabo todo esto *es información,* bien representada analógica o digitalmente. v.gr. las fotografías en el espacio del Internet, evidencian la vulnerabilidad de la intimidad, a través de la imagen.

La capacidad de estos medios físicos o lógicos para captar, procesar, editar y entregar información o datos por cauces electrónicos, informáticos o telemáticos, es lo que determina que estos medios se les denomine globalmente, a los efectos de éste trabajo investigativo, *medios informáticos*.

2.5.2.1. El delito relativo a los datos personales registrados en forma automatizadas contra la intimidad en el Código Penal Colombiano.

El Código Penal Colombiano ubica los delitos contra la intimidad en el título III, relativo a los "Delitos contra libertad individual y otras garantías" y establece varios tipos penales simples y agravados, según las circunstancias de modo, tiempo y lugar y la cualificación de los medios comisivos utilizados y los sujetos intervinientes en la conducta punible (artículos 192 a 197).

2.5.2.1. Bien Jurídico tutelado: El Derecho Fundamental a la intimidad y la visión ius-informática (habeas data) previstos en los artículos 15 y 20 constitucionales, siempre que estos se vean amenazados, transgredidos o desconocidos en el procesamiento, almacenamiento, registro, utilización o uso o en la tele-transmisión de datos de carácter personal (excluidos los "datos sensibles", cuando no hay autorización expresa y escrita para incluirlos en una base de datos o en fichero sistematizado público o privado) y se realicen por medios informáticos, telemáticos o electrónicos.

2.5.2.2. Medios Comisivos del tipo: Las conductas punibles contra la intimidad se realizan con "*cualquier medio electrónico diseñado o adaptado para emitir o recibir señales*" (art. 197 C.P.); vale decir, con medios informáticos, electrónicos o telemáticos, tanto de hardware (equipos compuntacionales o unidades periféricas: MODEM, Impresoras, Videocámaras, scanners, tableros ópticos, multimedia, cámaras digitales, etc.) como de software [19] (programas de computador utilitarios, educativos, publicitarios, chats room, páginas de WEB, WWW –World Word Web--, hipertexto, correo electrónico, tableros electrónicos, lúdicos, etc.) y sean idóneos para el tratamiento o procesamiento de datos ("Sistema de información", según la Ley 527 de 1999) desde la recolección, almacenamiento, registro, procesamiento, utilización hasta la transmisión de datos personales visuales, de texto o de sonido o todos a la vez (estilo "multimedial" de la información), o el envío y recepción de mensajes de datos o el intercambio electrónico de datos o documentos EDI [20] .

2.5.2.3. El Delito de violación ilícita de Comunicaciones Privadas o Públicas u "Oficiales".

Este delito omnicomprensivo esta previsto en los artículos 192 y 196 del C.P.de 2000, respectivamente, así:

"***Violación ilícita de comunicaciones***. 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 delito sancionado con pena mayor.
Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de dos (2) a cuatro (4) años. "

***Violación ilícita de comunicaciones o correspondencia de carácter oficial*.** El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida comunicación o correspondencia de carácter oficial, incurrirá en prisión de tres (3) a seis (6) años.
La pena descrita en el inciso anterior se aumentará hasta en una tercera parte cuando la comunicación o la correspondencia esté destinada o remitida a la Rama Judicial o a los organismos de control o de seguridad del Estado.

El delito que atenta la Intimidad, comporta dos tipos: unos simples y otros agravados. Los tipos penales simples están contenidos en los primeros incisos de los dos artículos correspondientes y se caracteriza por la apropiación, acceso, almacenamiento, destrucción, utilización indebida e interceptación de las comunicaciones privadas o públicas o de carácter oficial, respectivamente.

Estos tipos se configuran siempre y cuando no haya revelación, descubrimiento o divulgación de una información personal privada o pública o dato confidencial o secreto privado o público.

Los tipos agravados se hallan tipificados en los segundos incisos y se configuran ineludiblemente con la revelación, descubrimiento y posterior divulgación del secreto, información o dato privado o público, respectivamente. En segundo tipo agravado previsto en el inciso 2º del artículo 196, se estructura cuando la información o datos se refieren "*a la Rama Judicial o a los organismos de control o de seguridad del Estado",* bien sea en el proceso electrónico o informático de entrada (input) o de salida (output) de información. Las penas agravadas, para el primero son de 1 a 3 años de prisión, para el primero; y de 3 a 6 años de prisión para el segundo.

Ambos tipos penales se estructuran con los siguientes verbos rectores de sustracción, ocultación, extravío, destrucción, interceptación, control, impedimento o de enterarse de comunicaciones privadas o llegado el caso de descubrir y revelar los secretos que contengan dichas comunicaciones. Las comunicaciones entre personas privadas se entiende pueden realizarse por medios tradicionales escritos o por medios electrónicos, telemáticos o informáticos. En tal virtud, cuando los medios comisivos de la conducta punible contra la intimidad son de esta última clase estamos ante el delito informático relativo a la intimidad, pluricomprensivo en la configuración del verbo rector, pues se regula desde la apropiación, ocultación, extravío, la destrucción hasta la interceptación, control, impedimento, descubrimiento y revelación de cualquier información o dato personal o de un verdadero secreto.

Se entiende que estas conductas delictivas se configuran sin el consentimiento de la parte perjudicada y que resulta decisivo para la agravación punitiva del tipo, que el sujeto que realiza la acción punitiva descubra y divulgue los secretos o informaciones personales o datos confidenciales de la persona, o bien los emplee en provecho propio o ajeno o con perjuicio de otro. Esta conducta punible agravada de capatación y divulgación de las comunicaciones es la que se conoce en el derecho canadiense como *"interceptation of comunications" "Disclosure of information" y la "Invasión Privacy" (*Arts.183 s 196). En idéntico sentido los artículos 197-1 y 197-2 del Código Penal Español de 1995.

2.5.2.4. El Delito de "*Divulgación y empleo de documentos reservados*". Esta figura delictiva es una modalidad del anterior delito, con la particularidad de que el descubrimiento y divulgación de los datos personales, confidenciales o de informaciones personales incluidas los llamados "datos sensibles" de la persona o constitutivos del *"núcleo duro"* de la intimidad (datos sobre la ideología, raza, religión, etnia, sexo, aspectos filosóficos o políticos) estén contenidos en "documentos reservados" según el ordenamiento jurídico vigente. En este caso y a efectos del cumplimiento del delito informático contra la intimidad, los medios comisivos de la conducta punible deben ser informáticos, electrónicos o telemáticos, y por su puesto, los documentos reservados igualmente deben ser informáticos y recolectados, almacenados, procesados, transmitidos o utilizados con medios de hardware o software.

El artículo 194 del C.P. de 2000, sostiene:

"El que en provecho propio o ajeno o con perjuicio de otro divulgue o emplee el contenido de un documento que deba permanecer en reserva, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor".

Esta conducta punible deductible de otra con mayor sanción, contiene una pena débil poco ejemplarizante para el autor y que no se compadece con el atentado hacia la intimidad de las personas.

El documento (escrito o electrónico) reservado goza de protección constitucional (art.74) y legal (Ley 57 de 1985, reformado por la Ley 594 de 2000, art. 28 y Ley 190 de 1995, art.33) y sólo cesará cuando haya transcurrido treinta (30) años de su expedición y podrá ser consultado por cualquier persona o autoridad del Estado. Estos documentos, a título de ejemplo, podrán ser:

"expedientes, informes, estudios, cuentas, estadísticas, directivas, instrucciones, circulares, notas y respuestas provenientes de entidades públicas acerca de la interpretación del derecho o descripción de procedimientos administrativos, pareceres u opiniones, previsiones y decisiones que revistan forma escrita, registros sonoros o visuales, bancos de datos no personales, etc." (C.C., Sent. T-473-92, Julio 28.)

2.5.2.5. Delito de "*Acceso abusivo a un sistema informático*". Esta conducta punitiva constituye una especie de delito de *"intrusión"* a los sistemas informáticos privados o públicos, pues el tipo penal no hace distinción alguna sobre el particular. Intrusión hecha por una persona o usuario que obviamente se hace sin el consentimiento del titular de la información o datos sistematizados o del administrador del banco de datos, fichero o sistema informático .

El procedimiento o tratamiento sistematizado de la información o datos personales [21], esta configurado por diferentes fases o etapas: la recolección, selección, almacenamiento, registro, utilización, transmisión, bloqueo y cancelación de datos. El acceso a la información se presenta en las fases de utilización, transmisión, bloqueo y cancelación de datos. Las personas autorizadas para ellos son los titulares de los bancos de datos o ficheros, los administradores, ejecutores o usuarios del sistema. Cuando no es ninguno de ellos o no están autorizados para hacerlo se dice que el acceso a la información es ilegal o "abusivo". Ahora bien, para que se configure el delito de intrusión informático en el derecho colombiano, se requiere además que el sistema informático esté protegido con "*medida de seguridad"* . Este requisito adicional resulta superfluo, pues se entiende que un sistema informático con o sin medida de seguridad puede ser objeto de vulneración por medios informáticos y para los depredadores ("hackers" o "Crakers") de sistemas informáticos son más atractivos los sistemas con seguridad que los que no la tienen.

El tipo penal de intrusión a sistemas informáticos con medidas de seguridad se tipifica según el artículo 195 del C.P., así:

"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".

2.5.2.6. Delito de "*utilización ilícita de equipos transmisores o receptores*". Este tipo penal se estructura por el uso o utilización fraudulenta de medios informáticos, electrónicos o telemáticos "diseñado o adaptado para emitir o recibir señales" de comunicación, telecomunicación, video, sonido o imagen.

El artículo 197 del C.P. de 2000, sostiene:

***Utilización ilícita de equipos transmisores o receptores*.** El que con fines ilícitos posea o haga uso de aparatos de radiofonía o televisión, o de cualquier medio electrónico diseñado o adaptado para emitir o recibir señales, incurrirá, por esta sola conducta, en prisión de uno (1) a tres (3) años.
La pena se aumentará de una tercera parte a la mitad cuando la conducta descrita en el inciso anterior se realice con fines terroristas.

El delito esta compuesto por dos tipos: uno simple, previsto en el inciso primero que se estructura por el verbo rector “utilizar” medios electrónicos o informáticos o medios de radiofonía o televisión. Y otro, tipo agravado previsto en el inciso *in fine,* constituido si esos medios electrónicos o de radiofonía o televisión se utilizan con “fines terroristas”, con lo cual la pena se aumenta de una tercera parte a la mitad.

Este tipo penal es otra de las modalidades de “*delito intrusivo”* en la fase de uso de los medios electrónicos o telemáticos (bases de datos, ficheros o páginas WEB, WWW –World Wide Web, correos electrónicos o “e-mail”, chats, tableros electrónicos, hipertexto, etc.) públicos o privados. Para que se complete la estructuración del tipo penal, la utilización o el uso de estos medios por el intruso debe ser sin la autorización o consentimiento del titular o administrador de los datos, informaciones o comunicaciones.

2.5.2.7. El Delito de acceso, utilización y alteración de datos o informaciones de carácter personal o familiar registrados en documentos informáticos o de interceptación de datos personales electrónicos o telemáticos.

Para finalizar este breve ensayo, proponemos a la vista de la actual redacción de los delitos informáticos contra la intimidad, el siguiente que subsume los diferentes tipos penales simples y agravados antes vistos, con una mejor técnica jurídico penal y consecuente con el fenómeno informático actual.

En efecto, el delito sería: *El Delito de acceso, utilización y alteración de datos o informaciones de carácter personal o familiar registrados en documentos informáticos o de interceptación de documentos electrónicos o telemáticos.*

Este delito tipifica conductas tendientes a descubrir los secretos o vulnerar la intimidad del titular de los datos o de un tercero, por quien, sin estar autorizado, accede, utilice, modifique o altere datos o informaciones de carácter personal o familiar que se hallen registrados en ficheros o bancos de datos o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

Sin desconocer la autonomía de tipificación ni la redacción gramatical empleada por el actual C.P., de 2000, tanto para el delito de divulgación y empleo de documentos reservados (art. 194), bien sean aquellos realizados por medios tradicionales o escritos (papeles, cartas, etc), o documentos electrónicos (e-mails, hipertexto, WEB, etc.) que la doctrina califica de *delitos sobre secretos documentales* [22], para diferenciarlo del delito de *apoderamiento (por acceso), utilización y alteración de datos registrados en documentos informáticos y/o telemáticos,* que la doctrina iuspenalista española llama de *“Abusos informáticos”* [23], creemos a la vista de las razones antes dadas, que para tratar el fenómeno TIC (medios de información y comunicación electrónicos) y los delitos contra la intimidad, podemos plantear el *Delito de acceso, utilización y alteración de datos o informaciones de carácter particular o familiar registrados en documentos informáticos,* en una primera parte y el *de interceptación de documentos electrónicos o telemáticos ,* en una segunda parte, en atención a una mejor sistematización de los documentos informáticos y/o telemáticos, con la aclaración de que una y otra figuras punitivas, están referidas a la visión ius-informática del derecho a la intimidad personal y familiar, pues de lo contrario, nos estaríamos refiriendo: o, a los delitos *contra los datos informáticos* previstos en el C.P. Español de 1995., para otros bienes jurídicos como el Patrimonio y el orden socioeconómico (Tit.XIII), v.gr. delitos de destrucción, alteración, inutilización de datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos (“Delito de Daños”, art. 264.2), o a cualquier otro tipo o bien jurídico penalmente tutelado.

Ahora bien, por regla general, la tele-transmisión de datos o informaciones se realiza entre máquinas automatizadas a través de medios o equipos electromagnéticos o computacionales con el auxilio de soportes (hardware y/o software) informáticos y/o telemáticos y su producto en consecuencia es de idéntica naturaleza tecnológica (El documento telemático), y por tanto, la transmisión, emisión y la recepción de los datos o informaciones, se presenta en la memoria de los discos electromagnéticos conocidos (fijos o removibles de diferente formato: *disquettes,* CD´s, CD-ROM, CD-RAM, CD-I, DVD) o conocibles en el futuro (p.e. evolución del DVD); en las unidades periféricas computacionales (como impresoras, grabadoras de sonido o audio-visuales, altoparlantes y aparatos audio-visuales, etc) o asimilables. La multimedia (que une telecomunicaciones e informática: datos, imagen y sonido), hace acopio de estas técnicas TIC en la actualidad y una de las formas de transmitir y recepcionar datos, imagen y sonido es a través del llamado documento electrónico de intercambio de datos "*EDI*"[24].

Ahora bien, la interceptación de las telecomunicaciones [25] utilizando a*rtificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o cualquier otra señal de comunicación*", se ha tipificado en la parte *in fine* del artículo propuesto como un *delito mutilado o imperfecto de actos, que no requiere para la consumación el efectivo descubrimiento de la intimidad; basta así para colmar la perfección típica con la interceptación de telecomunicaciones o con la utilización de aparatos de escucha, grabación o reproducción del sonido o de la imagen o cualquier otra señal de comunicación, siempre que alguno de estos sea llevado a cabo con la finalidad de descubrir la intimidad de otro (elemento subjetivo del injusto)...* [26]

En nuestro caso y sin desconocer la amplitud del tipo penal, nos remitimos sólo a la interceptación de los datos o informaciones de carácter personal contenidas en un soporte o documento telemático y con la finalidad de descubrir la intimidad de una persona, tras la denominación de *delito de interceptación de los datos o informaciones de carácter personal o familiar contenidos en documentos electrónicos o telemáticos,* es decir, a aquellos documentos de intercambio de información o (EDI) o "actos satélites" en los cuales A*no se produce papel sino en registros informáticos de los mensajes que se emiten o recepcionan*" [27].

3. **La Ley 1273 de 2009, que crea el bien jurídico tutelado de la "Información y de los datos" de la persona (natural o jurídica, se entiende) en Colombia.**

La reciente ley 1273 de 2009, adiciona el Código Penal con un "Título VII bis" intitulado "De la protección de la Información y de los datos" personales, como nuevo bien jurídico tutelado en el derecho penal Colombiano. En dicho título relaciona tipos penales que nosotros ya en 1999 [28].y luego en 2004 [29], los habíamos estudiado como figuras jurídico-penales que atentaban a los bienes jurídicos de la intimidad, los datos personales y el habeas data.

El singular "Título VII bis" en el C.P. Colombiano, se ubica formalmente después de título referido a los delitos contra el patrimonio económico (Titulo VII) y el título VIII, de los delitos contra los derechos de autor, cuando podrían haber estado mejor ubicados en el Titulo II, relativo a los delitos contra la "libertad individual y otras garantías", Capítulo VII, referente a "LA VIOLACION A LA INTIMIDAD, RESERVA E INTERCEPTACION DE COMUNICACIONES", tal como lo hemos expuesto en los apartes anteriores, pues al fin y al cabo los datos personales o familiares son bienes jurídicos que pueden ser afectados pluriofensivamente, pero relevantemente a la intimidad de las personas que se manifiesta en cualquier tipo de información que sobre las personas se tiene. Vgr. De datos económicos o financieros, de salud, de aspectos tributarios, de datos personalísimos, de vinculación laboral, etc., en fin, en tanto no afecten el "núcleo duro" de la intimidad de las personas o que se trate de datos privilegiados o que afecten la seguridad o defensa estatal.

El Título VII bis, está dividido en capítulos, a saber: 1) De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; y 2) De los atentados informáticos y otras infracciones.

Hacen parte del primer capítulo, los siguiente tipos penales: (i) ART. 269A.—Acceso abusivo a un sistema informático; (ii) ART. 269B.—Obstaculización ilegítima de sistema informático o red de telecomunicación; (iii) ART. 269C.—Interceptación de datos informáticos; (iii) ART. 269D.—Daño informático; (iv) ART. 269E.—Uso de software malicioso; (v) ART. 269F.—Violación de datos personales; (vi) ART. 269G.—Suplantación de sitios web para capturar datos personales. Y Como norma común a las anteriores se establece en el artículo 269H, las "Circunstancias de agravación punitiva", según las cuales, las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere: 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros; 2. Por servidor público en ejercicio de sus funciones; 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este**;** 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro; 5. Obteniendo provecho para sí o para un tercero; 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional**;** 7. Utilizando como instrumento a un tercero de buena fe; y 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

En el segundo Capítulo se relacionan los delitos de: (i) Hurto por medios informáticos y semejantes (artículo 268I); y (ii) Transferencia no consentida de activos (Artículo 269J).

Sin ni siquiera ingresar a su estudio referencial de los anteriores tipos penales, digamos por ahora, que el delito de hurto por medios informáticos y "semejantes" (término que tiene un contenido de ambigüedad y ajenidad que será duramente criticado por los penalistas en su momento), perfectamente pudo haber quedado incluido en una especie del género "Hurto", pues el hurto sigue siendo hurto, sea cual fuere el medio comisivo utilizado. Igual pasa con el tipo de "transferencia no consentida de activos", que sin importar el medio comisivo utilizado (mecánico, manual, informático o telemático", sique siendo un tipo penal especial de defraudación (artículos 251 y 252 del actual Código Penal).

Así mismo, el Capítulo II, adiciona una causal o "Circunstancia de mayor punibilidad, no solo para los anteriores tipos delictivos sino con carácter general para otros delitos, "siempre que no se haya previsto de otra manera": "17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos". Es general y aplicable al contexto de tipos penales, porque adiciona el artículo 58 del Código Penal, que estable los "criterios y reglas para determinación de la punibilidad" regulada en el Código y no solo para los tipos penales antes relacionados.

El Artículo 3, adiciona al artículo 37 del Código de Procedimiento Penal, en cuanto que deja en manos de los jueces penales municipales la competencia para conocer de todos los delitos previstos en el Titulo VII bis. Esta competencia tendrá que revisarse, pues los bienes jurídicos tutelados en el presente título son pluriofensivos y no sólo pueden afectar a las personas particulares públicas o privadas, sino a las personas jurídicas públicas o al mismo Estado en cualquiera de sus niveles cuando se ponga en riesgo la "defensa o seguridad del Estado".

Finalmente, la Ley 1273 de 2009, en el artículo 4º deroga el artículo 195 del actual Código Penal, es decir, el delito de "*ACCESO ABUSIVO A UN SISTEMA INFORMATICO*", el cual consiste en: "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". Este artículo formalmente estaba ubicado en el Título II, Capítulo VII del Código Penal, tutelando entre otros derechos el de la intimidad y la información. La derogación se produce porque el legislador de 2009, reestructura el tipo penal, lo reubica en el bien jurídico tutelado y lo retoca con mayor dureza en las penas privativas de la libertad y pecuniarias, a quien se halle incurso en dichas actividades "abusivas" o de "intrusión informática", telemática o electrónica, así:

"Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (artículo 269ª).

Los tratadistas del derecho penal, tienen mucho que decir sobre la nueva ley que adicionó el Código Penal.

Citas Bibliográficas

(*) Docente Universitario Titular de derecho público. Facultad de Derecho de la Universidad de Nariño (Pasto-Colombia). Abogado de la Universidad de Nariño (1982); Doctor en Derecho de la Universidad de Navarra (1986) y la Universidad de Lleida (1999), España.

(1) Nos referimos a los Estados de *la Commonwealth* que siguen las sugerencias, recomendaciones y aplicaciones de la legislación comunitaria en las variadas actividades humanas objeto de su regulación normativa, en los cuales a falta de una base jurídica rígida de asociación está ampliamente compensada por los vínculos de origen común, historia, tradición jurídica y solidaridad de intereses", como lo sostiene *Oppenheim.* T.I., p.224. Algunos de los muchos países que hacen parte de esta comunidad de Estados son: Inglaterra, Canada, Australia, Irlanda del Norte, Nueva Zelandia, etc. A título de ejemplo: La "Crimes Act 1914" de Australia. Texto de la ley tomado de: AA.VV. ***Base de datos de la Universidad de Australia.*** Legislación y datos vía Internet (WWW.AUSTLII.EDU.AU . En Inglés), p.1.

(2) Nuestra Obra: ***La Constitución de 1991 y la informática jurídica.*** Ed. UNED, Pasto (Col), 1997 pág. 124. Para indicar que el fenómeno de la informática lo invadió todo, tan rápidamente como ninguno otro la había hecho, y en consecuencia, los Estados en la práctica no pudieron hacer lo que en teoría era previsible, es decir, regular normativamente, cuando menos, el acceso, tratamiento y uso de la informática en todas las actividades humanas, sin recurrir a la *ultima ratio* para reprimirla pues los hechos de la vida cotidiana en los que estaba involucrada la informática había desbordado el fenómeno mismo y por supuesto, cualquier tentativa de regulación preventiva, civilista e institucional de carácter administrativo resultó para muchos Estados como Colombia, al menos poco oportuna, eficaz y de verdadera política-estatal contra los nuevos fenómenos tecnológicos, a pesar de que se advertía en la Constitución Política (artículo 15) de los "riesgos" sobrevinientes de la informática contra los derechos fundamentales.

(3) BUENO ARUS, Francisco. ***El Delito Informático***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 11 de Abril, Ed. Aranzadi, Elcano (Navarra.), 1994., pág.1 y ss. MORALES PRATS, Fermín. *El descubrimiento y revelación de Secretos.* En: ***Comentarios a la Parte Especial del Derecho Penal***. Ed. Aranzadi, Pamplona (Esp.), 1996, pág. 297. También: en ***La tutela penal de la intimidad: privacy e informática***. Ed. Barcelona (Esp), 1984, pág.33 DAVARA R. Miguel. *Manual de Derecho Informático.* Ed. Aranzadi, Pamplona (Esp.), 1997, pág.285 y ss. CARBONELL M., J.C. y GONZALEZ CUSSAC., J.L. ***Delitos contra la Intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio***. En:

Comentarios al Código Penal de 1995. Vol. I., Ed. Tirant lo blanch, Valencia (Esp.), 1996, pág. 999 y ss. HEREDERO HIGUERAS, Manuel. ***La protección de los datos personales registrados en soportes informáticos*** .En: Actualidad Informática Aranzadi. A.I.A. Núm. 2, Enero, Ed. Aranzadi, Elcano (Navarra.), 1992. págs. 1 y ss.

(4) Véase, NORA, Simón y MINC, Alain. ***Informe nora-minc. La informatización de la sociedad.*** Trad. Paloma García Pineda y Rodrigo Raza, 1a., reimpresión. Ed. Fondo de Cultura Económica. México-Madrid-Buenos Aires, 1982, págs. 53 a 115. Más Recientemente, ***La Directiva de la Unión Europea 95/46/CE, del Parlamento Europeo*** *y del Consejo, de 24 de Octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos .*AA.VV. ***Base de datos celex".*** Ed. Comunidad Europea, Bruselas, (B), 1997., pág. 20

(5) Nuestra Obra: ***Los Datos personales informatizados en el Derecho Público Colombiano y foráneo.*** Digitocomputarizado, Trabajo para Ascenso al escalafón docente. Evaluado por Universidad Nacional de Colombia, Pasto, 2001, pág. 1 y ss.

(6) Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.
Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.
Art. 20. Se garantiza a toda persona la libertad de expresar su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.
Estos son libres y tienen responsabilidad social. Se garantiza el derecho de rectificación en condiciones de equidad. No habrá censura.

(7) Artículo 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. **Artículo 20**, d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.

(7 bis) RIASCOS GOMEZ, Libardo Orlando. *El Habeas Data: Una visión constitucional, legislativa y en proyectos de leyes estatutarias. Texto mecanografiado, publicado virtualmente en forma parcial en: www.monografias.com , www.informatica-juridica.com y http://akane.udenar.edu.co/derechopublico.*

(8) MORALES PRATS, Fermín. ***Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio***. En: Comentarios a la parte especial del Derecho Penal. Dirigida por Gonzalo Quintero Olivares y Coordinada por José Manuel Valle Muñiz (q.e.p.d.). Ed. Aranzadi, Pamplona (Nav.), 1996. pág. 309 y ss.

(9) MORALES PRATS, Fermín ***Protección penal de la intimidad, frente al uso ilícito de la informática en el código penal de 1995.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No. XI, "Delitos contra la libertad y Seguridad", Madrid, 1996. págs. 146 a 196 y ss

(10) ARROYO Z., Luis. ***La intimidad como bien jurídico protegido*** . En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J, "Estudios del Código Penal de 1995", Madrid, 1995, pág. 306.

(11) MORALES P., Fermín . ***Delitos contra la intimidad...*** Op.cit., pág. 317.

(12) La protección a la Aprivacidad" (por intimidad) es preventiva o cautelar y represiva, ambas de naturaleza administrativa, así mismo el carácter administrativo de las figuras cuasi delictivas previstas en los arts. 42 y 43 de la LORTAD, como "infracciones leves, graves y muy graves", y sostiene que ésta Aparece haberse inspirado más bien en el criterio despenalizador de conductas reprochables a que responde" y por ello, no se ha A tipificado ni una sola figura delictiva", y finaliza "la protección de carácter represivo que otorga la LORTAD es exclusivamente administrativo". GONZALEZ NAVARRO, Francisco. ***Derecho administrativo español.*** Ed. Eunsa, Pamplona (Esp.), 2 ed. 1994, p.179.

(13) Contrariamente a la tesis de González Navarro, el autor sostiene luego de enunciar algunas de las llamadas "infracciones leves, graves y muy graves" previstas en 42 y 43 de la LORTAD, que dentro de "éstas infracciones hay bastantes que, en realidad, por otra vertiente, constituyen delitos. De ahí la extremada gravedad de la actuación que se encomienda a la Agencia" de protección de Datos, creada por la LORTAD, como organismo de conservación, control, vigilancia, investigación y sanción disciplinarias y de infracciones contra datos informáticos públicos y privados. Vid. FAIREN GUILLEN, Víctor. ***El habeas data y su protección actual sugerida en la ley española de informativa de 29 de octubre de 1992 (interdictos, habeas corpus)***. En: Revista de Derecho Procesal. Ed. de derecho reunidas, Madrid, 1996, pág. 542.

(14) Nuestras obras: ***La jurisdicción civil de policía.*** Tesis para optar el título de abogado, Universidad de Nariño, Fac. de Derecho, Pasto, Mayo 27 1983, pág. 12 y ss. ***Constitucionalidad de la jurisdicción de Policía.*** Monografía ganadora del "Concurso Centenario de la Constitución Colombiana de 1886". Banco de la República, Bogotá, 1984, pág. 18 y ss.

(15) Ibidem. Estructurado por el derecho al control de la información de sí mismo, el acceso, actualización, rectificación, bloqueo y cancelación de los datos personales informatizados y el derecho a la oposición y procesamiento informático, electrónico y telemático.

(16) TIEDEMANN, K., citado por Molina A. ***Introducción a la Criminología.***, Ed. Biblioteca Jurídica, Medellín, 1988, pág. 307

(17) KATSH, Ethain. ***Rights, camera, action: Ciberspatial, settings and the firts amendment. En:*** *www.Umontreal.Edu.ca* . Textos en inglés y francés.

(18) Vid. www.umontreal.edu.ca

(19) El Decreto 260 de Febrero 5 de 1988, por vez primera en Colombia introduce la terminología informática y define al Software, como "un conjunto ordenado de instrucciones que facilita la operación y comunicación del hombre con la máquina, o entre máquinas independientemente del medio en que se encuentren almacenados, sea éste magnético, óptico o circuitos integrados". Vid. Mi obra: ***La Constitución de 1991 y ... Ob. Cit.*** Pág.196.

(20) La ley 527 de 1999, define como mensaje de datos "La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax". "Intercambio Electrónico de Datos (EDI). La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto".

(21) ***Acceso a la información***: Es el derecho que tienen los titulares de la información para conocer, actualizar y rectificar los registros administrativos por los operadores de los bancos de datos o centrales de información.
Titular de la información: Es toda persona natural o jurídica, pública o privada a quien se refiere la información que repose en un banco de datos o central de información.
Uso de la información: Es la facultad que tienen los usuarios, en virtud de la autorización del titular, de utilizar para los fines señalados en la misma la información suministrada por los operadores de los bancos de datos o centrales de información.

Usuario: Toda persona a quien se suministra la información contenida en un banco de datos o central de información (art. 3 del Proyecto de Ley Estatutaria de Acceso a la información comercial y financiera en Colombia. Proyecto S075 de 2002)
video, sonido o imagen.

(22) Vid. MUÑOZ CONDE, Francisco. ***Derecho Penal. Parte Especial.*** Undécima ed., Ed. Tirant lo blanch, Valencia, 1996, pág.218. SERRANO GOMEZ, A. Ob. cit., pág. 227.

(23) Cfr. MORALES PRATS, F. *Comentarios a la parte Especial del Derecho Penal* ... Ob. cit. pág. 229. Igual En: ***La protección penal de la intimidad...,*** "La protección penal de la "privavy" informática: "habeas Data" y represión penal de los abusos informáticos. Ob. cit., pág. 165.

(24) AA.VV. *El EDI (Electronic Data Interchange).* En: Actualidad Informática Aranzadi. A.I.A. Núm. 10 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1994.pág.1

(25) En el derecho español, con relación este aspecto estipula: el art 2.2 de la Ley 31 de 1987, estipula que "los servicios de telecomunicación se organizarán de manera que pueda garantizarse eficazmente el secreto de las telecomunicaciones de conformidad con lo dispuesto en el art. 18.3 de la Constitución ". El art 3, de la ley sostiene que se entiende "por telecomunicaciones: Toda transmisión, emisión, o recepción de signos, señales, escritos imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos". Citado por SERRANO GOMEZ, A. Ob. cit. pág.226

(26) MORALES PRATS, F. ***Comentarios a la parte Especial del Derecho Penal***... Ob. Cit., pág. 305.

(27) AA.VV. ***EL EDI (Electronic Data Interchange)...*** Ob. Cit. ,pág. 1 y ss.

(28) RIASCOS GOMEZ, Libardo O. ***El derecho a la intimidad, la visión iusinformatica y el delito de datos personales***. Tesis doctoral, Universidad de Lleida (España), 1999. En: http://www.tesisenxarxa.net/TDX-0128107-195928/index_an.html.

(29) **RIASCOS GOMEZ,** Libardo Orlando. *El Habeas Data: Una visión constitucional, legislativa y en proyectos de leyes estatutarias. Texto mecanografiado, publicado virtualmente en forma parcial en: www.monografias.com , www.informatica-juridica.com y http://akane.udenar.edu.co/derechopublico.*